

# Cisco IOS Security Command Reference: Commands A to C

**First Published:** 2021-01-11

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



# CONTENTS


CHAPTER 1 **aaa accounting through aaa local authentication attempts max-fail** 1

aaa accounting 3

aaa accounting-list 11

aaa accounting (IKEv2 profile) 12

aaa accounting connection h323 13

aaa accounting delay-start 15

aaa accounting gigawords 18

aaa accounting include auth-profile 19

aaa accounting-list 20

aaa accounting jitter maximum 21

aaa accounting nested 22

aaa accounting redundancy 23

aaa accounting resource start-stop group 25

aaa accounting resource stop-failure group 27

aaa accounting send counters ipv6 29

aaa accounting send stop-record always 30

aaa accounting send stop-record authentication 31

aaa accounting session-duration ntp-adjusted 38

aaa accounting suppress null-username 39

aaa accounting update 40

aaa attribute 42

aaa attribute list 43

aaa authentication (IKEv2 profile) 45

aaa authentication (WebVPN) 47

aaa authentication arap 49

aaa authentication attempts login 51

aaa authentication auto (WebVPN) 52
aaa authentication banner 53
aaa authentication dot1x 55
aaa authentication enable default 57
aaa authentication eou default enable group radius 59
aaa authentication fail-message 60
aaa authentication login 62
aaa authentication nasi 66
aaa authentication password-prompt 69
aaa authentication ppp 71
aaa authentication sgbp 74
aaa authentication suppress null-username 76
aaa authentication token key 77
aaa authentication username-prompt 78
aaa authorization 80
aaa authorization (IKEv2 profile) 85
aaa authorization cache filterserver 88
aaa authorization config-commands 90
aaa authorization console 92
aaa authorization list 93
aaa authorization reverse-access 94
aaa authorization template 97
aaa cache filter 98
aaa cache filterserver 100
aaa cache profile 101
aaa common-criteria policy 103
aaa configuration 105
aaa dnis map accounting network 107
aaa dnis map authentication group 109
aaa dnis map authorization network group 111
aaa group server diameter 113
aaa group server ldap 114
aaa group server radius 115
aaa group server tacacs+ 117

aaa intercept 119
aaa local authentication attempts max-fail 121

CHAPTER 2 **aaa max-sessions through algorithm 123**

aaa max-sessions 125
aaa memory threshold 126
aaa nas cisco-nas-port use-async-info 128
aaa nas port extended 129
aaa nas port option82 130
aaa nas redirected-station 131
aaa new-model 133
aaa password 135
aaa pod server 137
aaa preauth 139
aaa processes 141
aaa route download 143
aaa server radius dynamic-author 145
aaa service-profile 147
aaa session-id 148
aaa session-mib 150
aaa traceback recording 152
aaa user profile 153
access (firewall farm) 154
access (server farm) 156
access (virtual server) 158
access session passthru-access-group 160
access-class 161
access-enable 163
access-group (identity policy) 165
access-group mode 166
access-list (IP extended) 168
access-list (IP standard) 181
access-list (NLSP) 185
access-list compiled 188

access-listcompileddata-linklimitmemory 189
access-listcompiledipv4limitmemory 191
access-list dynamic-extend 193
access-list remark 194
access-profile 195
access-restrict 198
access-session accounting 200
access-template 201
accounting 203
accounting (gatekeeper) 205
accounting (line) 207
accounting (server-group) 209
accounting acknowledge broadcast 213
accounting dhcp source-ip aaa list 214
acl (ISAKMP) 215
acl (WebVPN) 216
acl drop 217
action-type 219
activate 220
add (WebVPN) 221
address 222
address (IKEv2 keyring) 224
address ipv4 226
address ipv4 (config-radius-server) 227
address ipv6 (config-radius-server) 229
address ipv4 (GDOI) 231
address ipv6 (TACACS+) 232
addressed-key 233
administrator authentication list 235
administrator authorization list 237
alert 239
alert (zone-based policy) 240
alert-severity 242
alg sip blacklist 243

alg sip processor 245
alg sip timer 246
algorithm 247

CHAPTER 3 all profile map configuration through browser-proxy 249

all (profile map configuration) 252
allow-mode 253
appfw policy-name 254
appl (webvpn) 256
application (application firewall policy) 257
application-inspect 260
application redundancy 262
arap authentication 263
ase collector 265
ase enable 266
ase group 267
ase signature extraction 268
asymmetric-routing 269
attribute (server-group) 271
attribute map 273
attribute nas-port format 274
attribute type 277
audit filesize 279
audit interval 281
audit-trail 283
audit-trail (zone) 285
authentication 286
authentication (IKE policy) 288
authentication (IKEv2 profile) 290
authentication bind-first 294
authentication command 296
authentication command bounce-port ignore 298
authentication command disable-port ignore 299
authentication compare 300

authentication control-direction 301
authentication critical recovery delay 302
authentication event fail 303
authentication event no-response action 305
authentication event server alive action reinitialize 306
authentication event server dead action authorize 307
authentication fallback 308
authentication host-mode 309
authentication list (tti-registrar) 311
authentication open 313
authentication order 314
authentication periodic 315
authentication port-control 317
authentication priority 319
authentication terminal 320
authentication timer inactivity 321
authentication timer reauthenticate 322
authentication timer restart 324
authentication trustpoint 325
authentication violation 327
authentication url 328
authorization 330
authorization (server-group) 332
authorization (tti-registrar) 334
authorization address ipv4 336
authorization identity 337
authorization list (global) 338
authorization list (tti-registrar) 339
authorization username 341
authorization username (tti-registrar) 343
authorize accept identity 345
auth-type 346
auth-type (ISG) 347
auto-enroll 348

auto-rollover 350
auto-update client 353
automate-tester (config-ldap-server) 355
automate-tester (config-radius-server) 356
auto secure 358
backoff exponential 360
backup-gateway 362
backup group 364
banner 365
banner (parameter-map webauth) 366
banner (WebVPN) 368
base-dn 370
bidirectional 371
binary file 373
bind authenticate 375
block count 377
browser-attribute import 379
browser-proxy 380

CHAPTER 4 **ca trust-point through clear eou** 381

ca trust-point 383
cabundle url 385
cache authentication profile (server group configuration) 387
cache authorization profile (server group configuration) 388
cache clear age 389
cache disable 390
cache expiry (server group configuration) 391
cache max 392
cache refresh 393
call admission limit 394
call guard-timer 395
category (ips) 396
cdp-url 397
certificate 401

chain-validation (ca-trustpool) 403
chain-validation 405
cifs-url-list 407
cipherkey 409
ciphervalue 410
cisco (ips-auto-update) 412
cisp enable 413
citrix enabled 414
class type inspect 415
class type urlfilter 418
class-map type inspect 420
class-map type urlfilter 424
clear aaa cache filterserver acl 427
clear aaa cache filterserver group 428
clear aaa cache group 429
clear aaa counters servers 430
clear aaa local user fail-attempts 431
clear aaa local user lockout 432
clear access-list counters 433
clear access-template 434
clear appfw dns cache 436
clear ase signatures 437
clear authentication sessions 439
clear content-scan 441
clear crypto call admission statistics 442
clear crypto ctcp 443
clear crypto datapath 444
clear crypto engine accelerator counter 445
clear crypto gdoi 448
clear crypto gdoi ks cooperative role 450
clear crypto ikev2 cluster dead-slaves 451
clear crypto ikev2 cluster stats 452
clear crypto ikev2 sa 453
clear crypto ikev2 stats 454

clear crypto ipsec client ezvpn 455
clear crypto isakmp 457
clear crypto sa 459
clear crypto session 462
clear crypto pki benchmarks 464
clear crypto pki crls 465
clear cws 466
clear dmvpn session 467
clear dmvpn statistics 469
clear dot1x 470
clear eap 471
clear eou 472

CHAPTER 5 **clear ip access-list counters through crl-cache none** 475
clear ip access-list counters 477
clear ip access-template 478
clear ip admission cache 480
clear ip audit configuration 481
clear ip audit statistics 482
clear ip auth-proxy cache 483
clear ip auth-proxy watch-list 484
clear ip inspect ha 486
clear ip inspect session 487
clear ip ips configuration 488
clear ip ips statistics 489
clear ip sdee 490
clear ip trigger-authentication 491
clear ip urlfilter cache 492
clear ipv6 access-list 493
clear ipv6 inspect 495
clear ipv6 snooping counters 496
clear kerberos creds 497
clear ldap server 498
clear logging ip access-list cache 499

clear parameter-map type protocol-info 500
clear policy-firewall 501
clear policy-firewall stats global 502
clear policy-firewall stats vrf 503
clear policy-firewall stats vrf global 504
clear policy-firewall stats zone 505
clear port-security 506
clear radius 508
clear radius local-server 509
clear webvpn nbns 511
clear webvpn session 512
clear webvpn stats 513
clear xsm 514
clear zone-pair 516
clid 517
client 519
client authentication list 521
client configuration address 523
client configuration group 524
client inside 525
client pki authorization list 526
client recovery-check interval 527
client connect 528
client rekey encryption 529
client rekey hash 531
client transform-sets 532
commands (view) 533
configuration url 537
configuration version 539
config-exchange 540
config-mode set 541
connect 542
content-length 543
content-scan out 545

content-scan whitelisting 546
content-type-verification 547
control 551
copy (consent-parameter-map) 553
copy idconf 555
copy ips-sdf 557
consent email 560
crl 561
crl (cs-server) 564
crl query 567
crl best-effort 569
crl optional 571
crl-cache delete-after 573
crl-cache none 575

CHAPTER 6 **crypto aaa attribute list through crypto ipsec transform-set 577**

crypto aaa attribute list 579
crypto ca authenticate 582
crypto ca cert validate 584
crypto ca certificate chain 585
crypto ca certificate map 587
crypto ca certificate query (ca-trustpoint) 590
crypto ca certificate query (global) 592
crypto ca crl request 593
crypto ca enroll 595
crypto ca export pem 598
crypto ca export pkcs12 601
crypto ca identity 603
crypto ca import 604
crypto ca import pem 605
crypto ca import pkcs12 607
crypto ca profile enrollment 609
crypto ca trusted-root 611
crypto ca trustpoint 612

crypto call admission limit 614
crypto connect vlan 616
crypto ctcp 618
crypto dynamic-map 620
crypto-engine 623
crypto engine accelerator 624
crypto engine aim 627
crypto engine compliance shield disable 628
crypto engine em 629
crypto engine mode vrf 630
crypto engine nm 632
crypto engine onboard 633
crypto engine slot 634
crypto engine slot (interface) 635
crypto gdoi ks 638
crypto gdoi gm 640
crypto gdoi group 642
crypto identity 643
crypto ikev2 authorization policy 645
crypto ikev2 certificate-cache 647
crypto ikev2 cluster 648
crypto ikev2 cookie-challenge 650
crypto ikev2 cts 651
crypto ikev2 diagnose 656
crypto ikev2 dpd 657
crypto ikev2 fragmentation 659
crypto ikev2 http-url 660
crypto ikev2 keyring 661
crypto ikev2 limit 664
crypto ikev2 name mangler 666
crypto ikev2 nat 668
crypto ikev2 policy 669
crypto ikev2 profile 672
crypto ikev2 proposal 676

crypto ikev2 redirect 679
crypto ikev2 window 680
crypto ipsec client ezvpn (global) 681
crypto ipsec client ezvpn (interface) 686
crypto ipsec client ezvpn connect 689
crypto ipsec client ezvpn xauth 690
crypto ipsec transform-set default 692
crypto ipsec df-bit (global) 694
crypto ipsec df-bit (interface) 695
crypto ipsec fragmentation (global) 697
crypto ipsec fragmentation (interface) 698
crypto ipsec ike sa-strength-enforcement 700
crypto ipsec ipv4-deny 702
crypto ipsec nat-transparency 704
crypto ipsec optional 706
crypto ipsec optional retry 707
crypto ipsec profile 708
crypto ipsec security-association dummy 711
crypto ipsec security-association idle-time 712
crypto ipsec security-association lifetime 714
crypto ipsec security-association multi-sn 717
crypto ipsec security-association replay disable 718
crypto ipsec security-association replay window-size 719
crypto ipsec server send-update 720
crypto ipsec transform-set 721

CHAPTER 7 **crypto isakmp aggressive-mode disable through crypto mib topn 727**

crypto isakmp aggressive-mode disable 729
crypto isakmp client configuration address-pool local 730
crypto isakmp client configuration browser-proxy 731
crypto isakmp client configuration group 732
crypto isakmp client firewall 737
crypto isakmp default policy 739
crypto isakmp enable 742

crypto isakmp fragmentation 744
crypto isakmp identity 745
crypto isakmp invalid-spi-recovery 747
crypto isakmp keepalive 748
crypto isakmp key 751
crypto isakmp nat keepalive 754
crypto isakmp peer 756
crypto isakmp policy 758
crypto isakmp profile 761
crypto key decrypt rsa 764
crypto key encrypt rsa 765
crypto key export ec 767
crypto key export rsa pem 770
crypto key generate ec keysize 773
crypto key generate rsa 775
crypto key import ec 781
crypto key import rsa pem 783
crypto key lock rsa 787
crypto key move rsa 789
crypto key pubkey-chain rsa 791
crypto key storage 793
crypto key unlock rsa 795
crypto key zeroize ec 797
crypto key zeroize pubkey-chain 799
crypto key zeroize rsa 800
crypto keyring 802
crypto logging ezvpn 803
crypto logging ikev2 804
crypto logging session 805
crypto map (global IPsec) 806
crypto map (interface IPsec) 813
crypto map (Xauth) 816
crypto map client configuration address 818
crypto map gdoi fail-close 819

crypto map (isakmp) 821
crypto map isakmp-profile 823
crypto map local-address 824
crypto map redundancy replay-interval 826
crypto mib ipsec flowmib history failure size 828
crypto mib ipsec flowmib history tunnel size 829
crypto mib topn 830

CHAPTER 8 **crypto pki authenticate through cws whitelisting** 833
crypto pki authenticate 836
crypto pki benchmark 838
crypto pki cert validate 840
crypto pki certificate chain 841
crypto pki certificate map 843
crypto pki certificate query (ca-trustpoint) 846
crypto pki certificate storage 848
crypto pki crl cache 850
crypto pki crl request 852
crypto pki enroll 853
crypto pki export pem 856
crypto pki export pkcs12 password 860
crypto pki http max-buffer-size 863
crypto pki import 864
crypto pki import pem 865
crypto pki import pkcs12 password 868
crypto pki profile enrollment 871
crypto pki server 873
crypto pki server grant 877
crypto pki server info crl 878
crypto pki server info requests 879
crypto pki server password generate 881
crypto pki server reject 882
crypto pki server remove 883
crypto pki server request pkcs10 884

crypto pki server revoke 888
crypto pki server start 890
crypto pki server stop 891
crypto pki server trim 892
crypto pki server trim generate expired-list 895
crypto pki server unrevoke 897
crypto pki token change-pin 898
crypto pki token encrypted-user-pin 899
crypto pki token label 901
crypto pki token lock 903
crypto pki token login 905
crypto pki token logout 906
crypto pki token max-retries 907
crypto pki token removal timeout 908
crypto pki token secondary config 910
crypto pki token secondary unconfig 912
crypto pki token unlock 914
crypto pki token user-pin 916
crypto pki trustpoint 917
crypto pki trustpool import 920
crypto pki trustpool policy 924
crypto provisioning petitioner 926
crypto provisioning registrar 928
crypto skip-client 931
crypto vpn 933
crypto wui tti petitioner 935
crypto wui tti registrar 937
crypto xauth 940
csd enable 942
ctcp port 943
ctype 944
cts authorization list network 946
cts credentials 947
cts dot1x 949

cts manual 950
cts role-based enforcement 951
cts role-based sgt-cache 952
cts role-based sgt-caching 954
cts role-based sgt-map (config) 955
cts role-based sgt-map interface 958
cts role-based sgt-map sgt 960
cts sxp connection peer 961
cts sxp default key-chain 965
cts sxp default password 966
cts sxp default source-ip 968
cts sxp enable 970
cts sxp filter-enable 972
cts sxp filter-group 973
cts sxp filter-list 975
cts sxp listener hold-time 977
cts sxp log binding-changes 979
cts sxp mapping network-map 980
cts sxp node-id 981
cts sxp reconciliation period 983
cts sxp retry period 985
cts sxp speaker hold-time 986
custom-page 988
cws out 990
cws whitelisting 991



# aaa accounting through aaa local authentication attempts max-fail


- aaa accounting, on page 3
- aaa accounting-list, on page 11
- aaa accounting (IKEv2 profile), on page 12
- aaa accounting connection h323, on page 13
- aaa accounting delay-start, on page 15
- aaa accounting gigawords, on page 18
- aaa accounting include auth-profile, on page 19
- aaa accounting-list, on page 20
- aaa accounting jitter maximum, on page 21
- aaa accounting nested, on page 22
- aaa accounting redundancy, on page 23
- aaa accounting resource start-stop group, on page 25
- aaa accounting resource stop-failure group, on page 27
- aaa accounting send counters ipv6, on page 29
- aaa accounting send stop-record always, on page 30
- aaa accounting send stop-record authentication, on page 31
- aaa accounting session-duration ntp-adjusted, on page 38
- aaa accounting suppress null-username, on page 39
- aaa accounting update, on page 40
- aaa attribute, on page 42
- aaa attribute list, on page 43
- aaa authentication (IKEv2 profile), on page 45
- aaa authentication (WebVPN), on page 47
- aaa authentication arap, on page 49
- aaa authentication attempts login, on page 51
- aaa authentication auto (WebVPN), on page 52
- aaa authentication banner, on page 53
- aaa authentication dot1x, on page 55
- aaa authentication enable default, on page 57
- aaa authentication eou default enable group radius, on page 59
- aaa authentication fail-message, on page 60

- aaa authentication login, on page 62
- aaa authentication nasi, on page 66
- aaa authentication password-prompt, on page 69
- aaa authentication ppp, on page 71
- aaa authentication sgbp, on page 74
- aaa authentication suppress null-username, on page 76
- aaa authentication token key, on page 77
- aaa authentication username-prompt, on page 78
- aaa authorization, on page 80
- aaa authorization (IKEv2 profile), on page 85
- aaa authorization cache filterserver, on page 88
- aaa authorization config-commands, on page 90
- aaa authorization console, on page 92
- aaa authorization list, on page 93
- aaa authorization reverse-access, on page 94
- aaa authorization template, on page 97
- aaa cache filter, on page 98
- aaa cache filterserver, on page 100
- aaa cache profile, on page 101
- aaa common-criteria policy, on page 103
- aaa configuration, on page 105
- aaa dnis map accounting network, on page 107
- aaa dnis map authentication group, on page 109
- aaa dnis map authorization network group, on page 111
- aaa group server diameter, on page 113
- aaa group server ldap, on page 114
- aaa group server radius, on page 115
- aaa group server tacacs+, on page 117
- aaa intercept, on page 119
- aaa local authentication attempts max-fail, on page 121

# aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode or template configuration mode. To disable AAA accounting, use the **no** form of this command.

**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default***list-name* | **guarantee-first**} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] {**radius** | **group** *group-name*}
**no aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default***list-name* | **guarantee-first**} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] {**radius** | **group** *group-name*}

## Syntax Description

| | |
|---|---|
| **auth-proxy** | Provides information about all authenticated-proxy user events. |
| **system** | Performs accounting for all system-level events not associated with users, such as reloads.<br>**Note**<br>When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes. |
| **network** | Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP). |
| **exec** | Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command. |
| **connection** | Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin. |
| **commands** *level* | Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15. |
| **dot1x** | Provides information about all IEEE 802.1x-related user events. |
| **default** | Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services. |

| | |
|---|---|
| *list-name* | Character string used to name the list of at least one of the following accounting methods:<br>• **group radius** --Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.<br>• **group tacacs +** --Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.<br>• **group** *group-name* --Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*argument. |
| **guarantee-first** | Guarantees system accounting as the first record. |
| **vrf** *vrf-name* | (Optional) Specifies a virtual routing and forwarding (VRF) configuration.<br>VRF is used only with system accounting. |
| **start-stop** | Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server. |
| **stop-only** | Sends a stop accounting record for all cases including authentication failures regardless of whether the **aaa accounting send stop-record authentication failure** command is configured. |
| **none** | Disables accounting services on this line or interface. |
| **broadcast** | (Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |
| **radius** | Runs the accounting service for RADIUS. |

| | |
|---|---|
| **group** *group-name* | Specifies the accounting method list. Enter at least one of the following keywords:<br>• **auth-proxy** --Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service.<br>• **commands** --Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level.<br>• **connection** --Creates a method list to provide accounting information about all outbound connections made from the network access server.<br>• **exec** --Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.<br>• **network** --Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions.<br>• **resource** --Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.<br>• **tunnel** --Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes.<br>• **tunnel-link** --Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes. |
| **delay-start** | Delays PPP network start records until the peer IP address is known. |
| **send** | Sends records to the accounting server. |
| **stop-record** | Generates stop records for a specified event. |
| **authentication** | Generates stop records for authentication failures. |
| **failure** | Generates stop records for authentication failures. |
| **success** | Generates stop records for authenticated users. |
| **remote-server** | Specifies that the users are successfully authenticated through access-accept message, by a remote AAA server. |

## Command Default

AAA accounting is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server support was added. |

| Release | Modification |
|---|---|
| 12.1(1)T | The **broadcast** keyword was added on the Cisco AS5300 and Cisco AS5800 universal access servers. |
| 12.1(5)T | The **auth-proxy** keyword was added. |
| 12.2(1)DX | The vrf keyword and *vrf-name* argument were added on the Cisco 7200 series and Cisco 7401ASR. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(13)T | The vrf keyword and *vrf-name*argument were integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(15)B | The tunnel and tunnel-link accounting methods were introduced. |
| 12.3(4)T | The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | The **dot1x** keyword was integrated into Cisco IOS Release 12.4(11)T. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. The **radius** keyword was added. |
| 15.3(1)S | This command was integrated into Cisco IOS Release 15.3(1)S. |

## Usage Guidelines

### General Information

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

The table below contains descriptions of keywords for AAA accounting methods.

***Table 1: aaa accounting Methods***

| Keyword | Description |
|---|---|
| **group** group-name | Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument. |
| **group radius** | Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. |

| Keyword | Description |
|---|---|
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. |

In the table above, the **group radius** and **group tacacs +** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS--The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+--The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering values for the *list-name*argument where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and method list keywords to identify the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.



**Note** System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a “stop” accounting record for all cases including authentication failures. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a “start” accounting notice at the beginning of the requested process and a “stop” accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the vrf keyword and vrf-name argument. System accounting does not have knowledge of VRF unless VRF is specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, see the appendix “RADIUS Attributes” in the Cisco IOS Security Configuration Guide . For a list of supported TACACS+ accounting AV pairs, see the appendix “TACACS+ Attribute-Value Pairs” in the Cisco IOS Security Configuration Guide .

**Note** This command cannot be used with TACACS or extended TACACS.

**Cisco Service Selection Gateway Broadcast Accounting**

To configure Cisco Service Selection Gateway (SSG) broadcast accounting, use ssg_broadcast_accounting for the *list-name* argument. For more information about configuring SSG, see the chapter "Configuring Accounting for SSG" in the Cisco IOS Service Selection Gateway Configuration Guide , Release 12.4.

**Layer 2 LAN Switch Port**

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of "Update/Watchdog packets from this AAA client" in your RADIUS server Network Configuration tab. Next, enable "CVS RADIUS Accounting" in your RADIUS server System Configuration tab.

You must enable AAA before you can enter the **aaa accounting** command. To enable AAA and 802.1X (port-based authentication), use the following global configuration mode commands:

- **aaa new-model**
- **aaa authentication dot1x default group radius**
- **dot1x system-auth-control**

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

Use the **aaa accounting system default start-stop group radius** command to send "start" and "stop" accounting records after the router reboots. The "start" record is generated while the router is booted and the stop record is generated while the router is reloaded.

The router generates a "start" record to reach the AAA server. If the AAA server is not reachable, the router retries sending the packet four times. The retry mechanism is based on the exponential backoff algorithm. If there is no response from the AAA server, the request will be dropped.

**Establishing a Session with a Router if the AAA Server Is Unreachable**

The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes.

To establish a console or telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first start-stop radius** command.

**Note** Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

## Examples

The following example shows how to define a default command accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example shows how to defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The a**aa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example shows how to define a default system accounting method list, where accounting services are provided by RADIUS security server "server1" with a start-stop restriction. The **aaa accounting**command specifies accounting for vrf "vrf1."

```
aaa accounting system default vrf vrf1 start-stop group server1
```

The following example shows how to define a default IEEE 802.1x accounting method list, where accounting services are provided by a RADIUS server. The **aaa accounting** command activates IEEE 802.1x accounting.

```
aaa new model
aaa authentication dot1x default group radius
aaa authorization dot1x default group radius
aaa accounting dot1x default start-stop group radius
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

The following example shows how to enable IEEE 802.1x accounting:

```
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication dot1x** | Specifies one or more AAA methods for use on interfaces running IEEE 802.1X. |
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa group server tacacs+** | Groups different server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **dot1x system-auth-control** | Enables port-based authentication. |

| Command | Description |
|---|---|
| **radius-server host** | Specifies a RADIUS server host. |
| **show radius statistics** | Displays the RADIUS statistics for accounting and authentication packets. |
| **tacacs-server host** | Specifies a TACACS+ server host. |

# aaa accounting-list

To enable authentication, authorization, and accounting (AAA) accounting when you are using RADIUS for Secure Socket Layer Virtual Private Network (SSL VPN) sessions, use the **aaa accounting-list**command in global configuration mode. To disable the AAA accounting, use the **no** form of this command.

**aaa accounting-list** *aaa-list*
**no aaa accounting-list** *aaa-list*

## Syntax Description

| | |
|---|---|
| *aaa-list* | Name of the AAA accounting list that has been configured under global configuration. |

## Command Default

AAA accounting is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Before configuring this command, ensure that the AAA accounting list has already been configured under global configuration.

## Examples

The following example shows that AAA accounting has been configured for an SSL VPN session:

```
Router (config)# aaa accounting-list aaalist1
```

## Related Commands

| Command | Description |
|---|---|
| aaa accounting network SSLVPN start-stop group radius | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |

# aaa accounting (IKEv2 profile)

To enable AAA accounting for IPsec sessions, use the **aaa accounting** command in IKEv2 profile configuration mode. To disable AAA accounting, use the **no** form of this command.

**aaa accounting** {**psk** | **cert** | **eap**} *list-name*
**no aaa accounting** {**psk** | **cert** | **eap**} *list-name*

## Syntax Description

| | |
|---|---|
| **psk** | Specifies a method list if the authentication method preshared key. |
| **cert** | Specifies a method list if the authentication method is certificate based. |
| **eap** | Specifies a method list if the authentication method is Extensible Authentication Protocol (EAP). |
| *list-name* | Name of the AAA list. |

## Command Default

AAA accounting is disabled.

## Command Modes

IKEv2 profile configuration (config-ikev2-profile)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use the **aaa accounting** command to enable and specify the method list for AAA accounting for IPsec sessions. The **aaa accounting** command can be specific to an authentication method or common to all authentication methods, but not both at the same time. If no method list is specified, the list is common across authentication methods.

## Examples

The following example defines an AAA accounting configuration common to all authentication methods:

```
Router(config-ikev2-profile)# aaa accounting common-list1
```

The following example configures an AAA accounting for each authentication method:

```
Router(config-ikev2-profile)# aaa accounting psk psk-list1
Router(config-ikev2-profile)# aaa accounting cert cert-list1
Router(config-ikev2-profile)# aaa accounting eap eap-list1
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 profile** | Defines an IKEv2 profile. |

# aaa accounting connection h323

To define the accounting method list H.323 using RADIUS as a method with either **stop-only** or **start-stop** accounting options, use the **aaa accounting connection h323** command in global configuration mode. To disable the use of this accounting method list, use the **no** form of this command.

**aaa accounting connection h323** {**stop-only** | **start-stop** | **none**} [**broadcast**] **group groupname**
**no aaa accounting connection h323** {**stop-only** | **start-stop** | **none**} [**broadcast**] **group groupname**

## Syntax Description

| | |
|---|---|
| **stop-only** | Sends a "stop" accounting notice at the end of the requested user process. |
| **start-stop** | Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server. |
| **none** | Disables accounting services on this line or interface. |
| **broadcast** | (Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |
| **group** *groupname* | Specifies the server group to be used for accounting services. The following are valid server group names:<br>• *string* : Character string used to name a server group.<br>• **radius** : Uses list of all RADIUS hosts.<br>• **tacacs+** : Uses list of all TACACS+ hosts. |

## Command Default

No accounting method list is defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(6)NA2 | This command was introduced. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command creates a method list called h323 and is applied by default to all voice interfaces if the **gw-accounting h323** command is also activated.

## Examples

The following example enables authentication, authorization, and accounting (AAA) services, gateway accounting services, and defines a connection accounting method list (h323). The h323 accounting

method lists specifies that RADIUS is the security protocol that will provide the accounting services, and that the RADIUS service will track start-stop records.

```
aaa new model
gw-accounting h323
aaa accounting connection h323 start-stop group radius
```

**Related Commands**

| Command | Description |
|---|---|
| **gw-accounting** | Enables the accounting method for collecting call detail records. |

# aaa accounting delay-start

To delay the generation of accounting start records until the user IP address is established, use the **aaa accounting delay-start** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**aaa accounting delay-start** [**all**] [**vrf** *vrf-name*] [**extended-delay** *delay-value*]
**no aaa accounting delay-start** [**all**] [**vrf** *vrf-name*] [**extended-delay** *delay-value*]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Extends the delay of sending accounting start records to all Virtual Route Forwarding (VRF) and non-VRF users. |
| **vrf** *vrf-name* | (Optional) Extends the delay of sending accounting start records to the specified VRF user. |
| **extended-delay** *delay-value* | (Optional) Delays the sending of accounting start records by a configured delay value (in seconds) when the Internet Protocol Control Protocol Version 6 (IPCPv6) address is initialized before the IPCPv4 address is sent to the RADIUS server. The valid values are 1 and 2. |

## Command Default

Accounting records are not delayed.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1 | This command was introduced. |
| 12.2(1)DX | This command was modified. The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(13)T | This command was modified. The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T. |
| 12.3(1) | This command was modified. The **all** keyword was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

| Release | Modification |
|---|---|
| 15.2(4)S | This command was modified. The **extended-delay** keyword and *delay-value* argument were added. |

## Usage Guidelines

Use the **aaa accounting delay-start** command to delay the generation of accounting start records until the IP address of the user has been established. Use the **vrf** *vrf-name* keyword and argument to delay accounting start records for individual VPN routing and forwarding (VRF) users or use the **all** keyword for all VRF and non-VRF users.



**Note** The **aaa accounting delay-start** command applies only to non-VRF users. If you have a mix of VRF and non-VRF users, configure the **aaa accounting delay-start** (for non-VRF users), **aaa accounting delay-start vrf** *vrf-name* (for VRF users), or **aaa accounting delay-start all** (for all VRF and non-VRF users) command.

Use the **aaa accounting delay-start extended-delay** *delay-value* command in the following two scenarios:

- The user is a dual-stack (IPv4 or IPv6) subscriber.
- The IP address is from a local pool and not from the RADIUS server.



**Note** It is mandatory that you configure the **aaa accounting delay-start** command before you configure the **aaa accounting delay-start extended-delay** command.

In both scenarios, the IPCPv6 address is initialized first and the IPCPv4 address is initialized after a few milliseconds. Use the **aaa accounting delay-start extended-delay** *delay-value* command to delay the accounting start records for the configured time (in seconds) after the IPCPv6 address is sent to the RADIUS server. During this configured delay time, the IPCPv4 address is sent and the Framed-IP-Address attribute is added to the accounting start record. If the IPCPv4 address is not sent in the configured delay time, the accounting start record is sent without the Framed-IP-Address attribute.

## Examples

The following example shows how to delay accounting start records until the IP address of the user is established:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start
radius-server host 192.0.2.1 non-standard
radius-server key rad123
```

The following example shows that accounting start records are to be delayed to all VRF and non-VRF users:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start all
radius-server host 192.0.2.1 non-standard
```

```
radius-server key rad123
```

The following example shows how to delay accounting start records for 2 seconds when the user is a dual-stack subscriber:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start
aaa accounting delay-start extended-delay 2
radius-server host 192.0.2.1 non-standard
radius-server key rad123
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |
| **tacacs-server host** | Specifies a TACACS+ server host. |

# aaa accounting gigawords

To enable authentication, authorization, and accounting (AAA) 64-bit, high-capacity counters, use the **aaa accounting gigawords** command in global configuration mode. To disable the counters, use the **no** form of this command. (Note that gigaword support is automatically configured unless you unconfigure it using the **no** form of the command.)

**aaa accounting gigawords**
**no aaa accounting gigawords**

## Syntax Description

This command has no arguments or keywords.

## Command Default

If this command is not configured, the 64-bit, high-capacity counters that support RADIUS attributes 52 and 53 are automatically enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13.7)T | This command was introduced. |

## Usage Guidelines

The AAA high-capacity counter process takes approximately 8 percent CPU memory for 24,000 (24 K) sessions running under steady state.

If you have entered the **no** form of this command to turn off the 64-bit counters and you want to reenable them, you will need to enter the **aaa accounting gigawords**command. Also, once you have entered the **no form of the command**, it takes a reload of the router to actually disable the use of the 64-bit counters.



**Note** The **aaa accounting gigawords** command does not show up in the running configuration unless the **no** form of the command is used in the configuration.

## Examples

The following example shows that the AAA 64-bit counters have been disabled:

```
no aaa accounting gigawords
```

# aaa accounting include auth-profile

To include authorization profile attributes for the AAA accounting records, use the **aaa accounting include auth-profile**command in global configuration mode. To disable the authorization profile, use the **no** form of this command.

**aaa accounting include auth-profile** {**delegated-ipv6-prefix** | **framed-ip-address** | **framed-ipv6-prefix**}
**no aaa accounting include auth-profile** {**delegated-ipv6-prefix** | **framed-ip-address** | **framed-ipv6-prefix**}

## Syntax Description

| | |
|---|---|
| **delegated-ipv6-prefix** | Includes the delegated-IPv6-Prefix profile in accounting records. |
| framed-ip-address | Includes the Framed-IP-Address profile in accounting records. |
| framed-ipv6-prefix | Includes the Framed-IPv6-Prefix profile in accounting records. |

## Command Default

authorization profile is included in the aaa accounting records.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced in a release earlier than Cisco IOS Release 15.1(1)T. |

## Usage Guidelines

The **aaa accounting include auth-profile**command can also be used for a dual-stack session if the negotiation between IPv4 and IPv6 is successful.

## Examples

The following example shows how to include the delegated-IPv6-Prefix profile in the AAA accounting records:

```
Router(config)# aaa accounting include auth-profile delegated-ipv6-prefix
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |

# aaa accounting-list

To enable authentication, authorization, and accounting (AAA) accounting when you are using RADIUS for Secure Socket Layer Virtual Private Network (SSL VPN) sessions, use the **aaa accounting-list**command in global configuration mode. To disable the AAA accounting, use the **no** form of this command.

**aaa accounting-list** *aaa-list*
**no aaa accounting-list** *aaa-list*

## Syntax Description

| | |
|---|---|
| *aaa-list* | Name of the AAA accounting list that has been configured under global configuration. |

## Command Default

AAA accounting is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Before configuring this command, ensure that the AAA accounting list has already been configured under global configuration.

## Examples

The following example shows that AAA accounting has been configured for an SSL VPN session:

```
Router (config)# aaa accounting-list aaalist1
```

## Related Commands

| Command | Description |
|---|---|
| aaa accounting network SSLVPN start-stop group radius | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |

# aaa accounting jitter maximum

To provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records, use the **aaa accounting jitter maximum**command in global configuration mode. To return to the default interval, use the **no** form of this command.

**aaa accounting jitter maximum max-value**
**no aaa accounting jitter**

## Syntax Description

| | |
|---|---|
| **jitter-value** | Allows the maximum jitter value from 0 to 2147483 seconds to be set in periodic accounting. The value 0 turns off jitter. |

## Command Default

Jitter is set to 300 seconds (5 minutes) by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

If certain applications require that periodic records be sent at exact intervals, disable jitter by setting it to 0.

## Examples

The following example sets the maximum jitter value to 20 seconds:

```
aaa accounting jitter maximum 20
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |

# aaa accounting nested

To specify that NETWORK records be generated, or nested, within EXEC "start" and "stop" records for PPP users who start EXEC terminal sessions, use the **aaa accounting nested** command in global configuration mode. To allow the sending of records for users with a NULL username, use the **no** form of this command.

**aaa accounting nested** [**suppress stop**]
**no aaa accounting nested** [**suppress stop**]

## Syntax Description

| | |
|---|---|
| **suppress stop** | (Optional) Prevents sending a multiple set of records (one from EXEC and one from PPP) for the same client. |

## Command Default

Disabled

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | The **suppress** and **stop** keywords were added. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa accounting nested**command when you want to specify that NETWORK records be nested within EXEC "start" and "stop" records, such as for PPP users who start EXEC terminal sessions. In some cases, such as billing customers for specific services, it can be desirable to keep NETWORK "start" and "stop" records together, essentially nesting them within the framework of the EXEC "start" and "stop" messages. For example, if you dial in using PPP, you can create the following records: EXEC-start, NETWORK-start, EXEC-stop, and NETWORK-stop. By using the **aaa accounting nested command to**generate accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

Use the **aaa accounting nested suppress stop** command to suppress the sending of EXEC-stop accounting records and to send only PPP accounting records.

## Examples

The following example enables nesting of NETWORK accounting records for user sessions:

```
Router(config)# aaa accounting nested
```

The following example disables nesting of EXEC accounting records for user sessions:

```
Router(config)# aaa accounting nested suppress stop
```

# aaa accounting redundancy

To set the Accounting, Authorization, and Authentication (AAA) platform redundancy accounting behavior, use the **aaa accounting redundancy** command in global configuration mode. To disable the accounting behavior, use the **no** form of this command.

**aaa accounting redundancy** {**best-effort-reuse** [**send-interim**] | **new-session** | **suppress system-records**}
**no aaa accounting redundancy** {**best-effort-reuse** [**send-interim**] | **new-session** | **suppress system-records**}

## Syntax Description

| | |
|---|---|
| **best-effort-reuse** | Tracks redundant accounting sessions as existing sessions after switchover. |
| **send-interim** | (Optional) Sends an interim accounting update after switchover. |
| **new-session** | Tracks redundant accounting sessions as new sessions after switchover. |
| **suppress** | Suppresses specific records upon switchover. |
| **system-records** | Suppresses system records upon switchover. |

## Command Default

A redundant session is set as a new session upon switchover.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| Cisco IOS XE Release 3.5S | This command was modified. The **send-interim** keyword was added. |

## Usage Guidelines

Use the **aaa accounting redundancy** command to specify the AAA platform redundancy accounting behavior. This command also enables you to track the redundant sessions or existing sessions upon switchover.

Use the **send-interim** keyword to send the interim accounting record first after a switchover. The router sends the interim update for all sessions that survived the switchover as soon as the standby processor becomes active.

## Examples

The following example shows how to set the AAA platform redundancy accounting behavior to track redundant sessions as existing sessions upon switchover:

```
Router(config)# aaa accounting redundancy best-effort-reuse
```

The following example shows how to enable the router to send the interim accounting record first after a switchover:

```
Router(config)# aaa accounting redundancy best-effort-reuse send-interim
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting delay-start** | Specifies delay generation of accounting “start” records until the user IP address is established. |
| **aaa authentication dot1x** | Specifies one or more AAA methods for use on interfaces running IEEE 802.1X. |

# aaa accounting resource start-stop group

To enable full r esource accounting, which will generate both a “start” record at call setup and a “stop” record at call termination, use the aaa accounting resource start-stop group command in global configuration mode. To disable full resource accounting, use the no form of this command.

**aaa accounting resource** *method-list* **start-stop** [**broadcast**] **group** *groupname*
**no aaa accounting resource** *method-list* **start-stop** [**broadcast**] **group** *groupname*

## Syntax Description

| | |
|---|---|
| *method-list* | Method used for accounting services. Use one of the following options:<br>• **default** : Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.<br>• *string* : Character string used to name the list of accounting methods. |
| **broadcast** | (Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |
| *groupname* | Specifies the server group to be used for accounting services. The following are valid server group names:<br>• *string* : Character string used to name a server group.<br>• **radius** : Uses list of all RADIUS hosts.<br>• **tacacs+** : Uses list of all TACACS+ hosts. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the aaa accounting resource start-stop group command to send a “start” record at each call setup followed with a corresponding “stop” record at the call disconnect. There is a separate “call setup-call disconnect “start-stop” accounting record tracking the progress of the resource connection to the device, and a separate “user authentication start-stop accounting” record tracking the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

You may want to use this command to manage and monitor wholesale customers from one source of data reporting, such as accounting records.



**Note** Sending "start-stop" records for resource allocation along with user "start-stop" records during user authentication can lead to serious performance issues and is discouraged unless absolutely required.

All existing AAA accounting method list and server group options are made available to this command.

## Examples

The following example shows how to configure resource accounting for "start-stop" records:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default start-stop group radius
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting start-stop failure** | Enables resource failure stop accounting support, which will only generate a stop record at any point prior to user authentication if a call is terminated. |

# aaa accounting resource stop-failure group

To enable re source failure stop accounting support, which will generate a “stop” record at any point prior to user authentication only if a call is terminated, use the aaa accounting resource stop-failure group command in global configuration mode. To disable resource failure stop accounting, use the no form of this command.

**aaa accounting resource** *method-list* **stop-failure** [**broadcast**] **group** *groupname*
**no aaa accounting resource** *method-list* **stop-failure** [**broadcast**] **group** *groupname*

## Syntax Description

| | |
|---|---|
| *method-list* | Method used for accounting services. Use one of the following options:<br>• **default** : Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.<br>• *string* : Character string used to name the list of accounting methods. |
| **broadcast** | (Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |
| *groupname* | Group to be used for accounting services. Use one of the following options:<br>• *string* : Character string used to name a server group.<br>• **radius** : Uses list of all RADIUS hosts.<br>• **tacacs+** : Uses list of all TACACS+ hosts. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the aaa accounting resource stop-failure group command to generate a “stop” record for any calls that do not reach user authentication; this function creates “stop” accounting records for the moment of call setup. All calls that pass user authentication will behave as before; that is, no additional accounting records will be seen.

All existing authentication, authorization, and accounting (AAA) accounting method list and server group options are made available to this command.

## Examples

The following example shows how to configure "stop" accounting records from the moment of call setup:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default stop-failure group radius
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting resource start-stop group** | Enables full resource accounting, which will generate both a "start" record at call setup and a "stop" record at call termination. |

# aaa accounting send counters ipv6

To send IPv6 counters in the stop record to the accounting server, use the **aaa accounting send counters ipv6**command in global configuration mode. To stop sending IPv6 counters, use the **no** form of this command.

**aaa accounting send counters ipv6**
**no aaa accounting send counters ipv6**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IPv6 counters in the stop records are not sent to the accounting server.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.6 | This command was introduced. |

## Usage Guidelines

The **aaa accounting send counters ipv6**command sends IPv6 counters in the stop record to the accounting server.

## Examples

The following example shows how enable the router to send IPv6 counters in the stop record to the accounting server:

```
Router(config)# aaa accounting send counters ipv6
```

# aaa accounting send stop-record always

To send a stop record whether or not a start record was sent, use the **aaa accounting send stop-record always** command in global configuration mode. To disable sending a stop record, use the **no** form of this command.

**aaa accounting send stop-record always**
**no aaa accounting send stop-record always**

## Syntax Description

This command has no arguments or keywords.

## Command Default

A stop record is not sent.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2S | This command was introduced. |

## Usage Guidelines

When the **aaa accounting send stop-record always** command is enabled, accounting stop records are sent, even if their corresponding accounting starts were not sent out previously. This command enables stop records to be sent whether local authentication, or other authentication, is configured.

When a session is terminated on a Network Control Protocol (NCP) timeout, a stop record needs to be sent, even if a start record was not sent.

## Examples

The following example shows how to enable stop records to be sent always when an NCP timeout occurs, whether or not a start record was sent:

```
Router(config)# aaa accounting send stop-record always
```

# aaa accounting send stop-record authentication

To refine generation of authentication, authorization, and accounting (AAA) accounting “stop” records, use the **aaa accounting send stop-record authentication** command in global configuration mode. To end generation of accounting stop records, use the **no** form of this command that is appropriate.

**aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*]

**Failed Calls: End Accounting Stop Record Generation**
**no aaa accounting send stop-record authentication failure** [**vrf** *vrf-name*]

**Successful Calls: End Accounting Stop Record Generation**
**no aaa accounting send stop-record authentication success remote-server** [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| **failure** | Used to generate accounting “stop” records for calls that fail to authenticate at login or during session negotiation. |
| **success** | • Used to generate accounting “stop” records for calls that have been authenticated by the remote AAA server. A “stop” record will be sent after the call is terminated.<br>• Used to generate accounting "stop" records for calls that have *not* been authenticated by the remote AAA server. A“stop” record will be sent if one of the following states is true:<br>  • The start record has been sent.<br>  • The call is successfully established and is terminated with the “stop-only” configuration. |
| **remote-server** | Used to specify that the remote server is to be used. |
| **vrf** *vrf-name* | (Optional) Used to enable this feature for a particular Virtual Private Network (VPN) routing and forwarding configuration. |

## Command Default

Accounting “stop” records are sent only if one of the following is true:

- A start record has been sent.
- The call is successfully established with the “stop-only” configuration and is terminated.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(1)DX | The vrf keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |

| Release | Modification |
|---|---|
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(13)T | The vrf keyword and *vrf-name* argument were added. |
| 12.4(2)T | The **success** and **remote-server** keywords were added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

When the **aaa accounting** command is activated, by default the Cisco IOS software does not generate accounting records for system users who fail login authentication or who succeed in login authentication but fail PPP negotiation for some reason. The **aaa accounting** command can be configured to sent a "stop" record using either the **start-stop** keyword or the **stop-only** keyword.

When the **aaa accounting** command is issued with either the **start-stop** keyword or the **stop-only** keyword, the "stop" records can be further configured with the **aaa accounting send stop-record authentication**command. The failure and success keywords are mutually exclusive. If you have the **aaa accounting send stop-record authentication** command enabled with the **failure** keyword and then enable the same command with the **success** keyword, accounting stop records will no longer be generated for failed calls. Accounting stop records are sent for successful calls only until you issue either of the following commands:

- **no aaa accounting send stop-record authentication success remote-server**
- **aaa accounting send stop-record authentication failure**

When using the **failure** keyword, a "stop" record will be sent for calls that are rejected during authentication.

When using the **success** keyword, a "stop" record will be sent for calls that meet one of the following criteria:

- Calls that are authenticated by a remote AAA server when the call is terminated.
- Calls that are not authenticated by a remote AAA server and the start record has been sent.
- Calls that are successfully established and then terminated with the "stop-only" **aaa accounting** configuration.

Use the **vrf**vrf-name keyword and argument to generate accounting "stop" records per VPN routing and forwarding configuration.



**Note** The **success** and **remote-server** keywords are not available in Cisco IOS Release 12.2SX.

## Examples

The following example shows how to generate “stop” records for users who fail to authenticate at login or during session negotiation:

```
aaa accounting send stop-record authentication failure
```

The following example shows “start” and “stop” records being sent for a successful call when the **aaa accounting send stop-record authentication**command is issued with the **failure** keyword:

```
Router# show running-config | include aaa

.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
```

```
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 0.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                    [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "192.168.202.169"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "192.168.202.169"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                    [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@domain.com"
```

```
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 192.168.202.169:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

The following example shows the “stop” record being sent when the call is rejected during authentication when the **aaa accounting send stop-record authentication**command is issued with the **success** keyword.

```
Router# show running-config | include aaa
,
,
,
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius
Router#
*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 0.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 192.168.202.169:2195,
```

```
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=192.168.202.169"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 0.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
192.168.202.169:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
```

```
PPP                        [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                    [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "192.168.202.169"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "192.168.202.169"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                    [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                     [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                   [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                       [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                    [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 192.168.202.169:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |

# aaa accounting session-duration ntp-adjusted

To calculate RADIUS attribute 46, Acct-Sess-Time, on the basis of the Network Time Protocol (NTP) clock time, use the **aaa accounting session-duration ntp-adjusted** command in global configuration mode. To disable the calculation that was configured on the basis of the NTP clock time, use the **no** form of this command.

**aaa accounting session-duration ntp-adjusted**
**no aaa accounting session-duration ntp-adjusted**

## Syntax Description

This command has no arguments or keywords.

## Command Default

If this command is not configured, RADIUS attribute 46 is calculated on the basis of the 64-bit monotonically increasing counter, which is not NTP adjusted.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If this command is not configured, RADIUS attribute 46 can skew the session time by as much as 5 to 7 seconds for calls that have a duration of more than 24 hours. However, you may not want to configure the command for short-lived calls or if your device is up for only a short time because of the convergence time required if the session time is configured on the basis of the NTP clock time.

For RADIUS attribute 46 to reflect the NTP-adjusted time, you must configure the **ntp server** command as well as the **aaa accounting session-duration ntp-adjusted** command.

## Examples

The following example shows that the attribute 46 session time is to be calculated on the basis of the NTP clock time:

```
aaa new-model
aaa authentication ppp default group radius
aaa accounting session-time ntp-adjusted
aaa accounting network default start-stop group radius
```

## Related Commands

| Command | Description |
|---|---|
| **ntp server** | Allows the software clock to be synchronized by a NTP time server. |

# aaa accounting suppress null-username

To prevent the Cisco IOS software from sending accounting records for users whose username string is NULL, use the **aaa accounting suppress null-username**command in global configuration mode. To allow sending records for users with a NULL username, use the **no** form of this command.

**aaa accounting suppress null-username**
**no aaa accounting suppress null-username**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When **aaa accounting** is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. This command prevents accounting records from being generated for those users who do not have usernames associated with them.

## Examples

The following example suppresses accounting records for users who do not have usernames associated with them:

```
aaa accounting suppress null-username
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |

# aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update**command in global configuration mode. To disable interim accounting updates, use the **no** form of this command.

**aaa accounting update** [**newinfo**] [**periodic** *number* [**jitter maximum max-value**]]
**no aaa accounting update**

## Syntax Description

| | |
|---|---|
| **newinfo** | (Optional) An interim accounting record is sent to the accounting server whenever there is new accounting information to report relating to the user in question. |
| **periodic** | (Optional) An interim accounting record is sent to the accounting server periodically, as defined by the *number*. |
| *number* | (Optional) Integer specifying number of minutes. |
| jitter | (Optional) Allows you to set the maximum jitter value in periodic accounting. |
| **maximum max-value** | The number of seconds to set for maximum jitter in periodic accounting. The value 0 turns off jitter. Jitter is set to 300 seconds (5 minutes) by default. |

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(13)T | Introduced support for generation of an additional updated interim accounting record that contains all available attributes when a call leg is connected. |
| 12.2(15)T11 | The jitter keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

- When the **aaa accounting update**commandis activated, the Cisco IOS software issues interim accounting records for all users on the system. If the **newinfo** keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.
- When the **gw-accounting aaa** command and the **aaa accounting update newinfo** command and keyword are activated, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and

backward-call-indicators (BCI)) available at the time of call connection are sent through this interim updated accounting record.

- When used with the **periodic**keyword, interim accounting records are sent periodically as defined by the number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.
- When using both the **newinfo** and **periodic** keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the number. For example, if you configure the **aaa accounting update newinfo periodic** *number*command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the **newinfo** algorithm.
- Vendor-specific attributes (VSAs) such as h323-connect-time and backward-call-indicator (BCI) are transmitted in the interim update RADIUS message when the **aaa accounting update newinfo** command and keyword are enabled.
- Jitter is used to provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records. If certain applications require that periodic records be sent a exact intervals, you should disable jitter by setting it to 0.



**Caution** Using the **aaa accounting update periodic** command and keyword can cause heavy congestion when many users are logged into the network.

## Examples

The following example sends PPP accounting records to a remote RADIUS server. When IPCP completes negotiation, this command sends an interim accounting record to the RADIUS server that includes the negotiated IP address for this user; it also sends periodic interim accounting records to the RADIUS server at 30-minute intervals.

```
aaa accounting network default start-stop group radius
aaa accounting update newinfo periodic 30
```

The following example sends periodic interim accounting records to the RADIUS server at 30-minute intervals and disables jitter:

```
aaa accounting update newinfo periodic 30 jitter maximum 0
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| gw-accounting aaa | Enables VoIP gateway accounting through the AAA system. |

# aaa attribute

To add calling line identification (CLID) and dialed number identification service (DNIS) attribute values to a user profile, use the **aaa attribute**command in AAA-user configuration mode. To remove this command from your configuration, use the **no** form of this command.

**aaa attribute** {**clid** | **dnis**} *attribute-value*
**no aaa attribute** {**clid** | **dnis**} *attribute-value*

## Syntax Description

| | |
|---|---|
| **clid** | Adds CLID attribute values to the user profile. |
| **dnis** | Adds DNIS attribute values to the user profile. |
| *attribute-value* | Specifies a name for CLID or DNIS attribute values. |

## Command Default

If this command is not enabled, you will have an empty user profile.

## Command Modes

AAA-user configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **aaa attribute**command to add CLID or DNIS attribute values to a named user profile, which is created by using the **aaa user profile** command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the **test aaa group**command), thereby providing the RADIUS server with access to CLID or DNIS information when the server receives a RADIUS record.

## Examples

The following example shows how to add CLID and DNIS attribute values to the user profile “cat”:

```
aaa user profile cat
 aaa attribute clid clidval
 aaa attribute dnis dnisval
```

## Related Commands

| Command | Description |
|---|---|
| **aaa user profile** | Creates a AAA user profile. |
| **test aaa group** | Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server. |

# aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list locally on a router, use the **aaa attribute list** command in global configuration mode or IKEv2 authorization policy configuration mode. To remove the AAA attribute list, use the **no** form of this command.

**aaa attribute list** *list-name*
**no aaa attribute list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of the aaa attribute list. |

## Command Default

A local attribute list is not defined.

## Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

## Command History

| Release | Modification |
|---|---|
| 12.3(7)XI1 | This command was introduced. |
| 12.3(14)T | This command was integrated into Cisco IOS Release 12.3(14)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

There is no limit to the number of lists that can be defined (except for NVRAM storage limits).

Use this command to refer to a AAA attribute list. This list must be defined in global configuration mode. Among the AAA attributes, the list can have 'interface-config attribute that is used to apply interface configuration mode commands on the virtual access interface associated with the session.

## Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “cisco.com”:

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
 description vrf blue template1
 rd 1:1
 route-target export 1:1
```

```
 route-target import 1:1
!
subscriber authorization enable
!
subscriber profile cisco.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile cisco.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
!
```

The following examples shows how to configure an AAA attribute list 'attr-list1' which is referred from IKEv2 authorization policy. The AAA attribute list has 'interface-config' attributes.

```
!
aaa attribute list attr-list1
attribute type interface-config "ip mtu 1100"
attribute type interface-config "tunnel key 10"
!
!
crypto ikev2 authorization policy pol1
 aaa attribute list attr-list1
!
```

## Related Commands

| Command | Description |
|---|---|
| **attribute type** | Defines an attribute type that is to be added to an attribute list locally on a router. |
| **crypto ikev2 authorization policy** | Specifies an IKEv2 authorization policy. |

# aaa authentication (IKEv2 profile)

To specify the AAA authentication list for Extensible Authentication Protocol (EAP) authentication, use the **aaa authentication**command in IKEv2 profile configuration mode. To remove the AAA authentication for EAP, use the **no** form of this command.

**aaa authentication eap** *list-name*
**no aaa authentication eap**

## Syntax Description

| | |
|---|---|
| **eap** | Specifies the external EAP server for the authentication list. |
| *list-name* | Name of the AAA authentication list. |

## Command Default

AAA authentication for EAP is not specified.

## Command Modes

IKEv2 profile configuration (config-ikev2-profile)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |

## Usage Guidelines

Use this command to specify the AAA authentication list for EAP authentication. The **crypto ikev2 profile** command must be enabled before this command is executed.

## Examples

The following example shows how to configure the remote access server using the remote EAP authentication method with an external EAP server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-eap-list default group radius
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authentication eap aaa-eap-list
```

The following example shows how to configure the remote access server using the remote EAP authentication method with a local and external EAP server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-eap-list default group radius
Router(config)# aaa authentication login aaa-eap-local-list default group tacacs
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# authentication remote eap-local
Router(config-ikev2-profile)# aaa authentication eap aaa-eap-list
Router(config-ikev2-profile)# aaa authentication eap-local aaa-eap-local-list
```

**Related Commands**

| Command | Description |
|---|---|
| **crypt ikev2 profile** | Defines an IKEv2 profile. |

# aaa authentication (WebVPN)

To configure authentication, authorization, and accounting (AAA) authentication for SSL VPN sessions, use the **aaa authentication** command in webvpn context configuration mode. To remove the AAA configuration from the SSL VPN context configuration, use the **no** form of this command.

**aaa authentication** {**domain** *name* | **list** *name*}
**no aaa authentication** {**domain** | **list**}

## Syntax Description

| | |
|---|---|
| **domain** *name* | Configures authentication using the specified domain name. |
| **list** *name* | Configures authentication using the specified list name. |

## Command Default

If this command is not configured or if the **no** form of this command is entered, the SSL VPN gateway will use global AAA parameters (if configured).

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The **aaa authentication**command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, or the database can be accessed through any RADIUS or TACACS+ AAA server.

We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

## Examples

### Local AAA Example (Default to Global Configuration)

The following example configures local AAA for remote-user connections. Notice that the **aaa authentication** command is not configured in a context configuration.

```
Router (config)# aaa new-model
Router (config)# username USER1 secret 0 PsW2143
Router (config)# aaa authentication login default local
```

### AAA Access Control Server Example

The following example configures a RADIUS server group and associates the AAA configuration under the SSL VPN context configuration.

```
Router (config)# aaa new-model
Router (config)# aaa group server radius myServer
Router (config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646
Router (config-sg-radius)# exit
Router (config)# aaa authentication login default local group myServer
Router (config)# radius-server host 10.1.1.0 auth-port 1645 acct-port 1646
Router (config)# webvpn context context1
Router (config-webvpn-context)# aaa authentication list myServer
Router (config-webvpn-context)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# aaa authentication arap

To enable an authentication, authorization, and accounting (AAA) authentication method for AppleTalk Remote Access (ARA), use the **aaa authentication arap** command in global configuration mode. To disable this authentication, use the **no** form of this command.

**aaa authentication arap** {**default***list-name*} *method1* [*method2* . . .]
**no aaa authentication arap** {**default***list-name*} *method1* [*method2* . . .]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed methods that follow this argument as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the following list of authentication methods tried when a user logs in. |
| *method1* [*method2*...] | At least one of the keywords described in the table below. |

## Command Default

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication arap default local
```

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server and local-case support were added as method keywords for this command. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The list names and default that you set with the **aaa authentication arap**command are used with the **arap authentication** command. Note that ARAP guest logins are disabled by default when you enable AAA. To allow guest logins, you must use either the **guest** or **auth-guest** method listed in the table below. You can only use one of these methods; they are mutually exclusive.

Create a list by entering the **aaa authentication arap** *list-name method*command, where *list-name* is any character string used to name this list (such as *MIS-access* ). The *method*argument identifies the list of methods the authentication algorithm tries in the given sequence. See the table below for descriptions of method keywords.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **more system:running-config**command to view currently configured lists of authentication methods.

**Note** In the table below, the **group radius**, **group tacacs +**, and **group***group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

***Table 2: aaa authentication arap Methods***

| Keyword | Description |
|---|---|
| **guest** | Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed. |
| **auth-guest** | Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed. |
| **line** | Uses the line password for authentication. |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access group tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default group tacacs+ none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

# aaa authentication attempts login

To set the maximum number of login attempts that will be permitted before a session is dropped, use the **aaa authentication attempts login**command in global configuration mode. To reset the number of attempts to the default, use the **no** form of this command.

**aaa authentication attempts login** *number-of-attempts*
**no aaa authentication attempts login**

## Syntax Description

| | |
|---|---|
| *number-of-attempts* | Number of login attempts. Range is from 1 to 25. Default is 3. |

## Command Default

3 attempts

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2 T | This command was introduced. |

## Usage Guidelines

The **aaa authentication attempts login** command configures the number of times a router will prompt for username and password before a session is dropped.

The **aaa authentication attempts login** command can be used only if the **aaa new-model** command is configured.

## Examples

The following example configures a maximum of 5 attempts at authentication for login:

```
aaa authentication attempts login 5
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

# aaa authentication auto (WebVPN)

To allow automatic authentication for Secure Socket Layer virtual private network (SSL VPN) users, use the **aaa authentication auto** command in webvpn context configuration mode. To disable automatic authentication, use the **no** form of this command.

**aaa authentication auto**
**no aaa authentication auto**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Automatic authentication is not allowed.

## Command Modes

Webvpn context (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

Configuring this command allows users to provide their usernames and passwords via the gateway page URL. They do not have to enter the usernames and passwords again from the login page.

A user can embed his or her username and password in the URL using the following format:

```
http://<gateway-address>/<vw_context>/webvpnauth?username:password
```

## Examples

The following example shows that automatic authentication has been configured for users:

```
Router (config)# webvpn context
Router (config-webvpn-context)# aaa authentication auto
```

# aaa authentication banner

To configure a personalized banner that will be displayed at user login, use the **aaa authentication banner** command in global configuration mode.

**aaa authentication banner** *dstringd*
**no aaa authentication banner**

## Syntax Description

| | |
|---|---|
| *d* | Any delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner. |
| *string* | Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996. |

## Command Default

Not enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa authentication banner** command to create a personalized message that appears when a user logs in to the system. This message or banner will replace the default message for user login.

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.



**Note** The AAA authentication banner message is not displayed if TACACS+ is the first method in the method list. With CSCum15057, the AAA authentication banner message is always printed if the user logs into the system using the Secure Shell (SSH) server.

## Examples

The following example shows the default login message if **aaa authentication banner** is not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

The following example configures a login banner (in this case, the phrase "Unauthorized use is prohibited.") that will be displayed when a user logs in to the system. In this case, the asterisk (*) symbol is used as the delimiter. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized use is prohibited.
Username:
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication fail-message** | Configures a personalized banner that will be displayed when a user fails login. |

# aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

**aaa authentication dot1x** {**default***listname*} *method1* [*method2* . . .]
**no aaa authentication dot1x** {**default***listname*} *method1* [*method2* . . .]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. |
| *listname* | Character string used to name the list of authentication methods tried when a user logs in. |
| *method1* [*method2...*] | At least one of these keywords:<br>• **enable** --Uses the enable password for authentication.<br>• **group radius** --Uses the list of all RADIUS servers for authentication.<br>• **line** --Uses the line password for authentication.<br>• **local** --Uses the local username database for authentication.<br>• **local-case** --Uses the case-sensitive local username database for authentication.<br>• **none** --Uses no authentication. The client is automatically authenticated by the switch without using the information supplied by the client. |

## Command Default

No authentication is performed.

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced for the Cisco Ethernet switch network module. |
| 12.2(15)ZJ | This command was implemented on the following platforms for the Cisco Ethernet Switch Module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series. |
| 12.3(2)XA | This command was introduced on the following Cisco router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM - Cisco 2611XM, Cisco 2620XM - Cisco 2621XM, Cisco 2650XM - Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the Cisco IOS configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command. If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

## Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Router(config)# aaa new model
Router(config)# aaa authentication dot1x default group radius none
```

## Related Commands

| Command | Description |
|---|---|
| **debug dot1x** | Displays 802.1X debugging information. |
| **identity profile default** | Creates an identity profile and enters dot1x profile configuration mode. |
| **show dot1x** | Displays details for an identity profile. |
| **show dot1x (EtherSwitch)** | Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface. |

# aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine whether a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

**aaa authentication enable default** *method1* [*method2* . . .]
**no aaa authentication enable default** *method1* [*method2* . . .]

## Syntax Description

| | |
|---|---|
| *method1* [*method2*...] | At least one of the keywords described in the table below. |

## Command Default

If the **default**list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server support was added as various method keywords for this command. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in the table below. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the router to a RADIUS server include the username "$enab15$."

**Note** An enable authentication request for $enab{*x*}$ is sent only for RADIUS servers.

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to view currently configured lists of authentication methods.

**Note** In the table below, the **group radius**, **group tacacs +**, and **group***group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

***Table 3: aaa authentication enable default Methods***

| Keyword | Description |
|---|---|
| **enable** | Uses the enable password for authentication.<br>**Note**<br>An authentication request fails over to the next authentication method only if no enable password is configured on the router. |
| **line** | Uses the line password for authentication. |
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication.<br>**Note**<br>The RADIUS method does not work on a per-username basis. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example shows how to create an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication enable default group tacacs+ enable none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization** | Sets parameters that restrict network access to a user. |
| **aaa new-model** | Enables the AAA access control model. |
| **enable password** | Sets a local password to control access to various privilege levels. |

# aaa authentication eou default enable group radius

To set authentication lists for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **aaa authentication eou default enable group radius**command in global configuration mode. To remove the authentication lists, use the **no** form of this command.

**aaa authentication eou default enable group radius**
**no aaa authentication eou default enable group radius**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Authentication lists for EAPoUDP are not set.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Examples

The following example shows that authentication lists have been set for EAPoUDP:

```
Router (config)# aaa new-model
Router (config)# aaa authentication eou default enable group radius
```

## Related Commands

| Command | Description |
|---|---|
| **eou** | Provides information about EAPoUDP. |
| **ip admission** | Creates a Layer 3 network admission control rule to be applied to the interface. |

# aaa authentication fail-message

To configure a personalized banner that will be displayed when a user fails login, use the **aaa authentication fail-message** command in global configuration mode. To remove the failed login message, use the no form of this command.

**aaa authentication fail-message** *dstringd*
**no aaa authentication fail-message**

## Syntax Description

| | |
|---|---|
| *d* | The delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner. |
| *string* | Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996. |

## Command Default

Not enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa authentication fail-message** command to create a personalized message that appears when a user fails login. This message will replace the default message for failed login.

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

## Examples

The following example shows the default login message and failed login message that is displayed if **aaa authentication banner** and **aaa authentication fail-message** are not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
% Authentication failed.
```

The following example configures both a login banner (“Unauthorized use is prohibited.”) and a login-fail message (“Failed login. Try again.”). The login message will be displayed when a user logs in to the system. The failed-login message will display when a user tries to log in to the system and fails. (RADIUS is specified as the default login authentication method.) In this example, the asterisk (*) is used as the delimiting character.

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized use is prohibited.
Username:
Password:
Failed login. Try again.
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication banner** | Configures a personalized banner that will be displayed at user login. |

# aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

**aaa authentication login** {**default** *list-name*} *method1* [*method2* . . .]
**no aaa authentication login** {**default** *list-name*} *method1* [*method2* . . .]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in. See the "Usage Guidelines" section for more information. |
| *method1* [*method2*...] | The list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below. |

## Command Default

AAA authentication at login is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | This command was modified. The **group radius**, **group tacacs+**, and **local-case** keywords were added as methods for authentication. |
| 12.4(6)T | This command was modified. The **password-expiry** keyword was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. The **cache** *group-name* keyword and argument were added as a method for authentication. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |
| 15.1(1)T | This command was modified. The **group ldap** keyword was added. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |
| 15.0(1)S | This command was integrated into Cisco IOS Release 15.0(1)S. |

## Usage Guidelines

If the **default** keyword is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```



**Note** On the console, login will succeed without any authentication checks if **default** keyword is not set.

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method*command for a particular protocol. The *list-name* argument is the character string used to name the list of authentication methods activated when a user logs in. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The "Authentication Methods That Cannot be used for the list-name Argument" section lists authentication methods that cannot be used for the *list-name* argument and the table below describes the method keywords.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The password is prompted only once to authenticate the user credentials and in case of errors due to connectivity issues, multiple retries are possible through the additional methods of authentication. However, the switchover to the next authentication method happens only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

**Authentication Methods That Cannot Be Used for the list-name Argument**

The authentication methods that cannot be used for the *list-name* argument are as follows:

- **auth-guest**
- **enable**
- **guest**
- **if-authenticated**
- **if-needed**
- **krb5**
- **krb-instance**
- **krb-telnet**
- **line**
- **local**
- **none**
- **radius**

- **rcmd**
- **tacacs**
- **tacacsplus**

**Note** In the table below, the **group radius**, **group tacacs +**, **group ldap**, and **group***group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**,and **aaa group server tacacs+** commands to create a named group of servers.

The table below describes the method keywords.

***Table 4: aaa authentication login Methods Keywords***

| Keyword | Description |
|---|---|
| **cache** *group-name* | Uses a cache server group for authentication. |
| **enable** | Uses the enable password for authentication. This keyword cannot be used. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |
| **group ldap** | Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **krb5** | Uses Kerberos 5 for authentication. |
| **krb5-telnet** | Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router. |
| **line** | Uses the line password for authentication. |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **none** | Uses no authentication. |
| **passwd-expiry** | Enables password aging on a local authentication list.<br>**Note**<br>The **radius-server vsa send authentication** command is required to make the **passwd-expiry** keyword work. |

## Examples

The following example shows how to create an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an

error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access group tacacs+ enable none
```

The following example shows how to create the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ enable none
```

The following example shows how to set authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default krb5
```

The following example shows how to configure password aging by using AAA with a crypto client:

```
aaa authentication login userauthen passwd-expiry group radius
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **login authentication** | Enables AAA authentication for logins. |

# aaa authentication nasi

To specify authentication, authorization, and accounting (AAA) authentication for Netware Asynchronous Services Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** command in global configuration mode. To disable authentication for NASI clients, use the **no** form of this command.

**aaa authentication nasi** {**default***list-name*} *method1* [*method2* **...**]
**no aaa authentication nasi** {**default***list-name*} *method1* [*method2* **...**]

## Syntax Description

| | |
|---|---|
| **default** | Makes the listed authentication methods that follow this argument the default list of methods used when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in. |
| *method1* [*method2...*] | At least one of the methods described in the table below. |

## Command Default

If the **default** list is not set, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication nasi default local
```

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.0(5)T | Group server support and local-case were added as method keywords for this command. |
| 12.2(13)T | This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The default and optional list names that you create with the **aaa authentication nasi** command are used with the **nasi authentication** command.

Create a list by entering the **aaa authentication nasi** command, where *list-name* is any character string that names the list (such as *MIS-access* ). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. Method keywords are described in the table below.

To create a default list that is used if no list is assigned to a line with the **nasi authentication** command, use the default argument followed by the methods that you want to use in default situations.

The remaining methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.



**Note** In the table below, the **group radius**, **group tacacs +**, and **group***group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

***Table 5: aaa authentication nasi Methods***

| Keyword | Description |
|---|---|
| **enable** | Uses the enable password for authentication. |
| **line** | Uses the line password for authentication. |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates an AAA authentication list called *list1* . This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication nasi list1 group tacacs+ enable none
```

The following example creates the same list, but sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication nasi default group tacacs+ enable none
```

## Related Commands

| Command | Description |
|---|---|
| **ip trigger-authentication (global)** | Enables the automated part of double authentication at a device. |

| Command | Description |
|---|---|
| **ipx nasi-server enable** | Enables NASI clients to connect to asynchronous devices attached to a router. |
| **nasi authentication** | Enables AAA authentication for NASI clients connecting to a router. |
| **show ipx nasi connections** | Displays the status of NASI connections. |
| **show ipx spx-protocol** | Displays the status of the SPX protocol stack and related counters. |

# aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

**aaa authentication password-prompt** *text-string*
**no aaa authentication password-prompt** *text-string*

## Syntax Description

| | |
|---|---|
| *text-string* | String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”). |

## Command Default

There is no user-defined *text-string*, and the password prompt appears as “Password.”

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

The aaa authentication password-prompt command works when RADIUS is used as the login method. The password prompt that is defined in the command will be shown even when the RADIUS server is unreachable. The aaa authentication password-prompt command does not work with TACACS+. TACACS+ supplies the network access server (NAS) with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the aaa authentication password-prompt command. If the TACACS+ server is not reachable, the password prompt that is defined in the aaa authentication password-prompt command may be used.

## Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt “Enter your password now:”
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication username-prompt** | Changes the text displayed when users are prompted to enter a username. |
| **aaa new-model** | Enables the AAA access control model. |
| **enable password** | Sets a local password to control access to various privilege levels. |

# aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

**aaa authentication ppp** {**default***list-name*} *method1* [*method2* **...**]
**no aaa authentication ppp** {**default***list-name*} *method1* [*method2* **...**]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods tried when a user logs in. |
| *method1 method2...* | Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below. |

## Command Default

AAA authentication methods on serial interfaces running PPP are not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server support and **local-case** were added as method keywords. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

## Usage Guidelines

If the **default** list is not set, only the local user database is checked. This has the same effect as that created by the following command:

aaa authentication ppp default local

The lists that you create with the **aaa authentication ppp**command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method*command, where *list-name* is any character string used to name this list MIS-access. The *method*argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in the table below.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.



**Note** In the table below, the **group radius**, **group tacacs +**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

***Table 6: aaa authentication ppp Methods***

| Keyword | Description |
|---|---|
| cache *group-name* | Uses a cache server group for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **if-needed** | Does not authenticate if the user has already been authenticated on a tty line. |
| **krb5** | Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication). |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **none** | Uses no authentication. |

**Cisco 10000 Series Router**

The Cisco 10000 series router supports a maximum of 2,000 AAA method lists. If you configure more than 2,000 AAA method lists, traceback messages appear on the console.

## Examples

The following example shows how to create a AAA authentication list calledMIS-access for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa group server tacacs+** | Groups different server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **more system:running-config** | Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information. |
| **ppp authentication** | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |
| **radius-server host** | Specifies a RADIUS server host. |
| **tacacs+-server host** | Specifies a TACACS host. |

# aaa authentication sgbp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for Stack Group Bidding Protocol (SGBP), use the **aaa authentication sgbp** command in global configuration mode. To disable SGBP authentication and return to the default, use the **no** form of this command.

**aaa authentication sgbp** {**default***list-name*} *method1* [*method2* **. . .**]
**no aaa authentication sgbp** {**default***list-name*} *method1* [*method2* **. . .**]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods tried when a user logs in. |
| *method1* [*method2...*] | Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in |

## Command Default

The **aaa authentication ppp default**command. If the **aaa authentication ppp default**command is not enabled, local authentication will be the default functionality.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command introduced. |

## Usage Guidelines

The lists that you create with the **aaa authentication sgbp** command are used with the **sgbp aaa authentication** command.

Create a list by entering the **aaa authentication sgbp**p *list-name method* command, where the *list-name* argument is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in the table below.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

Use the **more system:running-config** command to display currently configured lists of authentication methods.

***Table 7: aaa authentication sgbp Methods***

| Keyword | Description |
|---|---|
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |

| Keyword | Description |
|---|---|
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example shows how to create a AAA authentication list called SGBP. The user first tries to contact a RADIUS server for authentication. If this action returns an error, the user will try to access the local database.

```
Router(config)# aaa authentication sgbp SGBP group radius local
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. |
| **sgbp aaa authentication** | Enables a SGBP authentication list. |

# aaa authentication suppress null-username

To configure Cisco IOS software to prevent an Access Request with a blank username from being sent to the RADIUS server, use the **aaa authentication suppress null-username**command in global configuration mode.

To configure Cisco IOS software to allow an Access Request with a blank username to be sent to the RADIUS server, use the no form of this command:

**aaa authentication suppress null-username**
**no aaa authentication suppress null-username**

## Syntax Description

Enables the prevention of an Access Request with a blank username from being sent to the RADIUS server.

## Command Default

The *command-level defaul* t is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 12.2(33)SRD | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was integrated into Cisco IOS XE Release 2.4 |

## Usage Guidelines

This command ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.

## Examples

The following example shows how the **aaa authentication suppress null-username** is configured:

```
enable
configure terminal
aaa new-model
aaa authentication suppress null-username
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables AAA globally. |

# aaa authentication token key

To create a token authentication key to provide temporary access to the network, use the **aaa authentication token key** command in global configuration mode. To remove the token authentication key, use the **no** form of this command.

**aaa authentication token key** *string*
**no aaa authentication token key** *string*

## Syntax Description

| | |
|---|---|
| *string* | Token authentication key in hexadecimal characters. The maximum number of hexadecimal characters is 16. |

## Command Default

Token authentication key is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.4(1)T | This command was introduced. |

## Usage Guidelines

The **aaa authentication token key** command can be used only if the **aaa new-model** command is configured. You must configure the user account with the **token** keyword before configuring the token authentication.

### Example

The following example shows how to create a token authentication key “abcdefghcisco123” to provide temporary access to the network:

```
Device> enable
Device# configure terminal
Device(config)# username user1 privilege 1 token password 0 cisco123
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authentication token key abcdefghcisco123
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication login** | Sets AAA authentication at login. |
| **aaa new-model** | Enables the AAA access control model. |
| **username** | Establishes a username-based authentication system. |

# aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

**aaa authentication username-prompt** *text-string*
**no aaa authentication username-prompt** *text-string*

## Syntax Description

| | |
|---|---|
| *text-string* | String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”). |

## Command Default

There is no user-defined *text-string*, and the username prompt appears as “Username.”

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.

**Note** The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

## Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt “Enter your name here:”
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication password-prompt** | Changes the text that is displayed when users are prompted for a password. |
| **aaa new-model** | Enables the AAA access control model. |
| **enable password** | Sets a local password to control access to various privilege levels. |

# aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

**aaa authorization** {**auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **exec** | **ipmobile** | **multicast** | **network** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default***list-name*} [*method1* [*method2* . . .]]
**no aaa authorization** {**auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **exec** | **ipmobile** | **multicast** | **network** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default***list-name*} [*method1* [*method2* . . .]]

## Syntax Description

| | |
|---|---|
| **auth-proxy** | Runs authorization for authentication proxy services. |
| **cache** | Configures the authentication, authorization, and accounting (AAA) server. |
| **commands** | Runs authorization for all commands at the specified privilege level. |
| *level* | Specific command level that should be authorized. Valid entries are 0 through 15. |
| **config-commands** | Runs authorization to determine whether commands entered in configuration mode are authorized. |
| **configuration** | Downloads the configuration from the AAA server. |
| **console** | Enables the console authorization for the AAA server. |
| **exec** | Runs authorization to determine if the user is allowed to run an EXEC shell. This facility returns user profile information such as the autocommand information. |
| **ipmobile** | Runs authorization for mobile IP services. |
| **multicast** | Downloads the multicast configuration from the AAA server. |
| **network** | Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA). |
| **policy-if** | Runs authorization for the diameter policy interface application. |
| **prepaid** | Runs authorization for diameter prepaid services. |
| **radius-proxy** | Runs authorization for proxy services. |
| **reverse-access** | Runs authorization for reverse access connections, such as reverse Telnet. |
| **subscriber-service** | Runs authorization for iEdge subscriber services such as virtual private dialup network (VPDN). |
| **template** | Enables template authorization for the AAA server. |
| **default** | Uses the listed authorization methods that follow this keyword as the default list of methods for authorization. |

| | |
|---|---|
| *list-name* | Character string used to name the list of authorization methods. |
| *method1* [*method2...*] | (Optional) Identifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below. |

**Command Default**

Authorization is disabled for all actions (equivalent to the method keyword **none**).

**Command Modes**

Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.0(5)T | This command was modified. The **group radius** and **group tacacs+** keywords were added as methods for authorization. |
| 12.2(28)SB | This command was modified. The **cache** *group-name* keyword and argument were added as a method for authorization. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |
| 15.1(1)T | This command was modified. The **group ldap** keyword was added. |
| Cisco IOS XE Fuji 16.8.1 | Increased supported number of method lists from 8 to 13. |

**Usage Guidelines**

Use the **aaa authorization**command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.



**Note** The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

The **aaa authorization** command supports 13 separate method lists. For example:

```
aaa authorization configuration methodlist1 group radius
aaa authorization configuration methodlist2 group radius
...
aaa authorization configuration methodlist13 group radius
```



**Note** In the table below, the **group** *group-name*, **group ldap, group radius**, and **group tacacs +** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**,and **aaa group server tacacs+** commands to create a named group of servers.

The table below describes the method keywords.

***Table 8: aaa authorization Methods***

| Keyword | Description |
|---|---|
| **cache** *group-name* | Uses a cache server group for authorization. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **aaa group server** *group-name* command. |
| **group ldap** | Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication. |
| **group radius** | Uses the list of all RADIUS servers for authorization as defined by the **aaa group server radius** command. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authorization as defined by the **aaa group server tacacs**+ command. |
| **if-authenticated** | Allows the user to access the requested function if the user is authenticated.<br>**Note**<br>The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated. |
| **local** | Uses the local database for authorization. |
| **none** | Indicates that no authorization is performed. |

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups--The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated --The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local --The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None --The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS --The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+ --The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC --Applies to the attributes associated with a user EXEC terminal session.
- Network --Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.



**Note** You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access --Applies to reverse Telnet sessions.
- Configuration --Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.



**Note** Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

## Examples

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
aaa authorization network mygroup group radius local
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa group server tacacs+** | Groups different TACACS+ server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |
| **tacacs-server host** | Specifies a TACACS+ host. |
| **username** | Establishes a username-based authentication system. |

# aaa authorization (IKEv2 profile)

To specify the authentication, authorization, and accounting (AAA) authorization for a local or external group policy, use the **aaa authorization** command in IKEv2 profile configuration mode. To remove the AAA authorization, use the **no** form of this command.

**aaa authorization** {**group** [**override**] {**cert** | **eap** | **psk**} | **user** {**cert list** | **eap** {**cached** | **list**} | **psk** {**cached** | **list**}} {*aaa-listname* | [*aaa-username* | [**local**] | **name-mangler** *mangler-name*] | [**password** *password*]}}
**no aaa authorization** {**group** [**override**] {**cert** | **eap** | **psk**} | **user** {**cert list** | **eap** {**cached** | **list**} | **psk** {**cached** | **list**}} {*aaa-listname* | [*aaa-username* | [**local**] | **name-mangler** *mangler-name*] | [**password** *password*]}}

## Syntax Description

| | |
|---|---|
| **group** | Specifies the AAA authorization for local or external group policy. |
| **local** | (Optional) Specifies the authorization policy that is used through a local method. |
| **override** | (Optional) Overrides user authorization with group authorization. By default, group authorization is overridden with user authorization. |
| **user** | Specifies the AAA authorization for each user policy. |
| **cert** | Specifies the AAA method list that is used when the remote authentication method is certificate based. |
| **eap** | Specifies the AAA method list that is used when the remote authentication method is Extensible Authentication Protocol (EAP). |
| **psk** | Specifies the AAA method list that is used when the remote authentication method is preshared key. |
| **list** | Specifies the AAA method list for the remote authentication method. |
| **cached** | Uses cached attributes from the EAP authentication or AAA preshared key. |
| *aaa-listname* | The AAA list name. |
| *aaa-username* | The AAA username. |
| **name-mangler** *mangler-name* | Derives the name mangler from the **crypto ikev2 name-mangler** command. |
| **password** *password* | Specifies the AAA password. This *password* argument defines the following values:<br>• **0**—Specifies that the password is unencrypted.<br>• **6**—Specifies that the password is encrypted.<br>• *password*—Specifies an unencrypted user password. |

## Command Default

AAA authorization is not specified.

## Command Modes

IKEv2 profile configuration (config-ikev2-profile)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.3(3)M | This command was modified. The **list** keyword and the **password** *password* keyword-argument pair was added |

## Usage Guidelines

Use this command to specify the AAA authorization for local or external group policy. The **crypto ikev2 profile** command must be enabled before this command is executed.

If no AAA method list is specified, the list is common for all authentication methods. Local AAA is not supported for user authorization.

AAA user policies take precedence over AAA group policies.

The **user** keyword is not required and not recommended when RADIUS is the external AAA server as RADIUS combines authentication and authorization and returns authorization data with successful authentication. The **user** keyword can be used with AAA servers such as TACACS+ where authentication and authorization are decoupled.

If the **cached** keyword is specified, the **name-mangler** *mangler-name* keyword-argument pair cannot be specified.

Use the following variations of the **aaa authorization** command to configure the Internet Key Exchange version 2 (IKEv2) profile for the FlexVPN server:

- To specify the AAA method list and username for user authorization, enter both or one of the following commands:
  - **aaa authorization user** {**eap** | **psk**} {**cached** | **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]}
  - **aaa authorization user cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}
- To specify the AAA method list and username for group authorization, enter both or one of the following commands:
  - **aaa authorization group** [**override**] {**eap** | **psk**} **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]
  - **aaa authorization group** [**override**] **cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

You can simultaneously configure all combinations of user and group authorizations for EAP, preshared key, and certificate-based authentication methods. For EAP and preshared key authentication methods, you can simultaneously configure two variants for user authorization with the **cached** and **list** keywords respectively.

## Examples

The following example shows how to configure the AAA authorization for a local group policy. The **aaa-group-list** keyword specifies that group authorization is local and the AAA username is abc. The authorization list name corresponds to the group policy defined in the **crypto ikev2 client configuration group** command.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-group-list default local
Router(config)# crypto ikev2 client configuration group 123
Router(config-ikev2-client-config-group)# pool addr-pool1
Router(config-ikev2-client-config-group)# dns 198.51.100.1 198.51.100.100
Router(config-ikev2-client-config-group)# wins 203.0.113.1 203.0.113.115
Router(config-ikev2-client-config-group)# exit
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# wins 203.0.113.1 203.0.113.115 authentication remote eap
Router(config-ikev2-profile)# aaa authorization group aaa-group-list abc
```

The following example shows how to configure an external AAA-based group policy. The **aaa-group-list** keyword specifies that the group authorization is RADIUS based. The name mangler derives the group name from the domain part of ID-FQDN, which is abc.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-group-list default group radius
Router(config)# crypto ikev2 name-mangler mangler1
Router(config-ikev2-name-mangler)# fqdn domain
Router(config-ikev2-name-mangler)# exit
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity remote fqdn host1.abc
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authorization group aaa-group-list name-mangler mangler1
```

The following example shows how to configure an external AAA-based group policy. The **aaa-user-list** specifies that user authorization is RADIUS based. The name mangler derives the username from the hostname part of ID-FQDN, which is host1.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-user-list default group radius
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
Router(config-ikev2-name-mangler)# exit
Router(config-ikev2-profile)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# match identity remote fqdn host1.abc
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authorization user aaa-user-list name-mangler mangler2
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 name-mangler** | Defines a name mangler. |
| **crypto ikev2 profile** | Defines an IKEv2 profile. |

# aaa authorization cache filterserver

To enable authentication, authorization, and accounting (AAA) authorization caches and the downloading of access control list (ACL) configurations from a RADIUS filter server, use the **aaa authorization cache filterserver** command in global configuration mode. To disable AAA authorization caches, use the **no** form of this command.

**aaa authorization cache filterserver default** *methodlist* [*methodlist2* **. . .**]
**no aaa authorization cache filterserver default**

## Syntax Description

| | |
|---|---|
| **default** | Default authorization list. |
| *methodlist* [ *methodlist2...* ] | One of the keywords listed in the table below. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **aaa authorization cache filterserver** command to enable the RADIUS ACL filter server.

Method keywords are described in the table below.

***Table 9: aaa authorization cache filterserver Methods***

| Keyword | Description |
|---|---|
| **group** *group-name* | Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. |
| **local** | Uses the local database for authorization caches and ACL configuration downloading. |
| **none** | No authorization is performed. |

This command functions similarly to the **aaa authorization**command with the following exceptions:

- Named method-lists cannot be configured.
- Only one instance of this command can be configured.
- TACACS+ groups cannot be configured.

## Examples

The following example shows how to configure the default RADIUS server group as the desired filter. If the request is rejected or a reply is not returned, local configuration will be consulted. If the local filter does not respond, the call will be accepted but filtering will not occur.

```
aaa authorization cache filterserver group radius local none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |

# aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the aaa authorization config-commands command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

**aaa authorization config-commands**
**no aaa authorization config-commands**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is disabled by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.0(6.02)T | This command was changed from being enabled by default to being disabled by default. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If the **aaa authorization commands** *level method*commandis enabled, all commands, including configuration commands, are authorized by authentication, authorization, and accounting (AAA) using the method specified. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using the **no aaa authorization config-commands** command stops the network access server from attempting configuration command authorization.

After the **no** form of this command has been entered, AAA authorization of configuration commands is completely disabled. Care should be taken before entering the **no** form of this command because it potentially reduces the amount of administrative control on configuration commands.

Use the **aaa authorization config-commands**command if, after using the **no** form of this command, you need to reestablish the default set by the **aaa authorization commands** *level method* command.



**Note** You will get the same result if you (1) do not configure this command, or (2) configure **no aaa authorization config-commands**.

## Examples

The following example specifies that TACACS+ authorization is run for level 15 commands and that AAA authorization of configuration commands is disabled:

```
aaa new-model
```

```
aaa authorization command 15 group tacacs+ none
no aaa authorization config-commands
```

## Related Commands

| Command | Description |
|---|---|
| aaa authorization | Sets parameters that restrict user access to a network. |

# aaa authorization console

To apply authorization to a console, use the **aaa authorization console** command in global configuration mode. To disable the authorization, use the **no** form of this command.

**aaa authorization console**
**no aaa authorization console**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Authentication, authorization, and accounting (AAA) authorization is disabled on the console.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(6)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If the **aaa new-model** command has been configured to enable the AAA access control model, the **no aaa authorization console**command is the default, and the authorization that is configured on the console line will always succeed. If you do not want the default, you need to configure the **aaa authorization console** command.

**Note** This command by itself does not turn on authorization of the console line. It needs to be used in conjunction with the **authorization** command under console line configurations.

If you are trying to enable authorization and the **no aaa authorization console** command is configured by default, you will see the following message:

```
%Authorization without the global command aaa authorization console
 is useless.
```

## Examples

The following example shows that the default authorization that is configured on the console line is being disabled:

```
Router (config)# aaa authorization console
```

## Related Commands

| Command | Description |
|---|---|
| **authorization** | Enables AAA authorization for a specific line or group of lines. |

# aaa authorization list

To allow user attributes to get "pushed" during authentication, use the **aaa authorization list** command in webvpn context configuration mode. To disable the pushing of attributes, use the **no** form of this command.

**aaa authorization list**
**no aaa authorization list**

## Syntax Description

| | |
|---|---|
| *name* | Name of the list to be automatically authorized. |

## Command Default

User attributes are not pushed during authentication.

## Command Modes

Webvpn context (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

If this command is configured, a separate authorization step is no longer needed after authentication.

## Examples

The following example shows that authorization is to be pushed during authentication for List 11:

```
Router (config)# webvpn context
Router (config-webvpn-context)# aaa authorization list 11
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication auto (WebVPN)** | Allows automatic authentication for SSL VPN users. |

# aaa authorization reverse-access

To configure a network access server to request authorization information from a security server before allowing a user to establish a reverse Telnet session, use the **aaa authorization reverse-access**command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

**aaa authorization reverse-access** {**group radius** | **group tacacs**+}
**no aaa authorization reverse-access** {**group radius** | **group tacacs**+}

## Syntax Description

| | |
|---|---|
| **group radius** | Specifies that the network access server will request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session. |
| **group tacacs+** | Specifies that the network access server will request authorization from a TACACS+ security server before allowing a user to establish a reverse Telnet session. |

## Command Default

This command is disabled by default, meaning that authorization for reverse Telnet is not requested.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.0(5)T | Group server support was added as various method keywords for this command. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction--from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to open Telnet sessions to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. This command provides an additional (optional) level of security by requiring authorization in addition to authentication. When this command is enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

## Examples

The following example causes the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs +** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host**command identifies the TACACS+ server.
- The **tacacs-server timeout** command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example configures a generic TACACS+ server to grant a user, “jim,” reverse Telnet access to port tty2 on the network access server named “site1” and to port tty5 on the network access server named site2:

```
user = jim
  login = cleartext lab
  service = raccess {
    port#1 = site1/tty2
    port#2 = site2/tty5
}
```



**Note** In this example, “site1” and “site2” are the configured host names of network access servers, not DNS names or alias.

The following example configures the TACACS+ server (CiscoSecure) to authorize a user named Jim for reverse Telnet:

```
user = jim
 profile_id = 90
 profile_cycle = 1
 member = Tacacs_Users
 service=shell {
 default cmd=permit
 }
 service=raccess {
 allow "c2511e0" "tty1" ".*"
```

```
refuse ".*" ".*" ".*"
password = clear "goaway"
```



**Note** CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(*x*) through version 2.2(1).

An empty "service=raccess {}" clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no "service=raccess" clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the chapter "Configuring TACACS+" in the *CiscoIOS Security Configuration Guide* . For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide* , version 2.1(2) or later.

The following example causes the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key goaway
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key**command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example configures the RADIUS server to grant a user named "jim" reverse Telnet access at port tty2 on network access server site1:

```
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=site1/tty2"
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={*nasname* }/{*tty number* }" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter "Configuring RADIUS" in the *CiscoIOS Security Configuration Guide* .

# aaa authorization template

To enable usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF), use the **aaa authorization template** command in global configuration mode. To disable the new authorization, use the **no** form of this command.

**aaa authorization template**
**no aaa authorization template**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Examples

The following example enables usage of a remote customer template:

```
aaa authorization template
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |
| **tacacs-server host** | Specifies a TACACS+ server host. |
| **template** | Accesses the template configuration mode for configuring a particular customer profile template. |

# aaa cache filter

To enable filter cache configuration, use the **aaa cache filter**command in global configuration mode. To disable this functionality, use the **no** form of this command.

**aaa cache filter**
**no aaa cache filter**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Filter cache configuration is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **aaa cache filter**command to begin filter cache configuration and enter AAA filter configuration mode (config-aaa-filter).

After enabling this command, you can specify filter cache parameters with the following commands:

- **cache clear age** -- Specifies, in minutes, when cache entries expire and the cache is cleared.
- **cache disable** --Disables the cache.
- **cache max** --Refreshes a cache entry when a new sessions begins.
- **cache refresh** --Limits the absolute number of entries the cache can maintain for a particular server.
- **password** --Specifies the optional password that is to be used for filter server authentication requests.



**Note** Each of these commands is optional; thus, the default value will be enabled for any command that is not specified.

## Examples

The following example shows how to enable filter cache configuration and specify cache parameters.

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization cache filterserver** | Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server. |
| **cache clear age** | Specifies when, in minutes, cache entries expire and the cache is cleared. |
| **cache disable** | Disables the cache. |
| **cache max** | Refreshes a cache entry when a new sessions begins. |
| **cache refresh** | Limits the absolute number of entries the cache can maintain for a particular server. |
| **password** | Specifies the optional password that is to be used for filter server authentication requests. |

# aaa cache filterserver

To enable Authentication, Authorization, and Accounting (AAA) filter server definitions, use the **aaa cache filterserver** command in global configuration mode. To disable AAA filter server definitions, use the **no** form of this command.

**aaa cache filterserver**
**no aaa cache filterserver**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.4(11)T | This command was integrated into Cisco IOS Release 12.4(11)T. |

## Usage Guidelines

The **aaa cache filterserver** command is mainly used to define AAA cache filter server requirements for downloading access control lists (ACLs) commands but is also used for cache configurations, domain names, and passwords. To use this command, enable the **aaa authorization cache filterserver** command first.

## Examples

The following example enables the **aaa cache filterserver** command:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router (config)# aaa authorization cache filterserver default group radius
Router(config)# aaa cache filterserver
Router(config-filter)# cache max 100
Router(config-filter)# no cache refresh
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa cache filterserver** | Displays the aaa cache filterserver status. |

# aaa cache profile

To create a named authentication and authorization cache profile group and enter profile map configuration mode, use the **aaa cache profile** command in global configuration mode. To disable a cache profile group, use the **no** form of this command.

**aaa cache profile** *group-name*
**no aaa cache profile** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Text string that specifies an authentication and authorization group. Group names cannot be duplicated. |

## Command Default

No cache profile groups are defined.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use this command to define or modify an authentication or authorization cache group and to specify cache profile parameters using the following commands:

- **all** --Specifies that all authentication and authorization requests are cached. Using the **all** command makes sense for certain service authorization requests, but it should be avoided when dealing with authentication requests.
- **profile** --Specifies an exact profile match to cache. The profile name must be an exact match to the username being queried by the service authentication or authorization request. This is the recommended format to enter profiles that users want to cache.
- **regexp** --Allows entries to match based on regular expressions. Matching on regular expressions is not recommended for most situations.

The **any** keyword, which is available under the **regexp** submenu, allows any unique instance of a AAA server response that matches the regular expression to be saved in the cache. The **only** keyword allows for only one instance of a AAA server response that matches the regular expression to be saved in the cache.

Entering the **no** form of this command deletes the profile definition and all of its command definitions.

## Examples

The following example creates the AAA cache profile group localusers:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
```

## Related Commands

| Command | Description |
|---|---|
| all | Specifies that all authentication and authorization requests be cached. |
| **profile** | Defines or modifies an individual authentication and authorization cache profile. |
| regexp | Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression. |

# aaa common-criteria policy

To configure authentication, authorization, and accounting (AAA) common criteria security policies, use the **aaa common-criteria policy** command in global configuration mode. To disable AAA common criteria policies, use the **no** form of this command.

**aaa common-criteria policy** *policy-name*
**no aaa common-criteria policy** *policy-name*

## Syntax Description

| | |
|---|---|
| *policy-name* | Name of the AAA common criteria security policy. |

## Command Default

The common criteria security policy is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(2)SE | This command was introduced. |

## Usage Guidelines

Use the **aaa common-criteria policy** command to enter the common criteria configuration policy mode. To check the available options in this mode, type **?** after entering into common criteria configuration policy mode (config-cc-policy).

**Note** The **aaa common-criteria policy** command is unavailable when the switch runs on IP Services license or Advanced IP Services license. However, when the switch runs on Advanced Enterprise Services license, the command works as expected. This limitation is applicable to release Cisco IOS XE 15.2(1)SY7 of Cisco Catalyst 6500 Series Switches.

The following options are available:

- **char-change**—Number of changed characters between old and new passwords. The range is from 1 to 64.
- **copy**—Copy the common criteria policy parameters from an existing policy.
- **exit**—Exit from common criteria configuration mode.
- **lifetime**—Configure the maximum lifetime of a password by providing the configurable value in years, months, days, hours, minutes, and seconds. If the lifetime parameter is not configured, the password will never expire.
- **lower-case**—Number of lowercase characters. The range is from 0 to 64.
- **upper-case**—Number of uppercase characters. The range is from 0 to 64.
- **min-length**—Minimum length of the password. The range is from 1 to 64.
- **max-length**—Maximum length of the password. The range is from 1 to 64.

- **numeric-count**—Number of numeric characters. The range is from 0 to 64.
- **special-case**—Number of special characters. The range is from 0 to 64.

## Examples

The following example shows how to create a common criteria security policy:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# end
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables AAA access control model. |
| **debug aaa common-criteria** | Enables debugging for AAA common criteria password security policies. |
| **show aaa common-criteria policy** | Displays common criteria security policy details. |

# aaa configuration

To configure the username and password that are to be used when downloading configuration requests, an IP pool, or static routes through RADIUS, use the **aaa configuration** command in global configuration mode. To disable this configuration, use the **no** form of this command.

**aaa configuration** {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*]}
**no aaa configuration** {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*]}

## Syntax Description

| | |
|---|---|
| **config-username** | Configures the username and password used in configuration requests that can be downloaded. |
| **username** *username* | Defines a username to be used instead of the device's hostname. |
| **password** | Specifies the RADIUS server password. |
| **0** | (Optional) Specifies the unencrypted (cleartext) shared password.<br>**Note**<br>Type 0 passwords are automatically converted to type 7 passwords by enabling the **service password-encryption** command. |
| **6** | (Optional) Specifies a password encrypted with a reversible, symmetric, advanced encryption scheme (AES) encryption algorithm.<br>**Note**<br>Type 6 AES encrypted passwords are configured using the **password encryption aes** command. |
| **7** | (Optional) Specifies a password encrypted using a Cisco-defined encryption algorithm. |
| *password* | The alphanumeric password to be used instead of the default "cisco." |
| **pool** | Configures the username and password used for downloading an IP pool. IP pools are used to define the range of IP addresses that are used for Dynamic Host Configuration Protocol (DHCP) servers and point-to-point servers. |
| **route** | Configures the username and password used when downloading static routes through RADIUS. |

## Command Default

The hostname of the router and the password "cisco" are used during the static route configuration download.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced. |

| Release | Modification |
|---|---|
| 15.4(1)T | This command was modified. The **6** keyword was added. |

## Usage Guidelines

The **aaa configuration** command allows you to specify a username other than the router's hostname and a stronger password than the default "cisco."

You can use the **service password-encryption** command to automatically convert type 0 passwords to type 7 passwords.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

## Examples

The following example shows how to specify the username "MyUsername" and the password "MyPass" when downloading a static route configuration:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# server 10.1.1.1
Device(config-sg-radius)# exit
Device(config)# aaa authorization configuration default group radius
Device(config)# aaa authorization configuration foo group rad1
Device(config)# aaa route download 1 authorization foo
Device(config)# aaa configuration route username MyUsername password 0 MyPass
Device(config)# radius-server host 10.2.2.2
Device(config)# radius-server key 0 RadKey
```

## Related Commands

| Command | Description |
|---|---|
| **aaa route download** | Enables the static route download feature and sets the amount of time between downloads. |
| **password encryption aes** | Enables a type 6 encrypted preshared key. |
| **service password-encryption** | Automatically converts unencrypted passwords to encrypted passwords. |

# aaa dnis map accounting network

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group that will be used for AAA accounting, use the **aaa dnis map accounting network**command in global configuration mode. To remove DNIS mapping from the named server group, use the **no** form of this command.

**aaa dnis map** *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] **group** *groupname*
**no aaa dnis map** *dnis-number* **accounting network**

## Syntax Description

| | |
|---|---|
| *dnis-number* | Number of the DNIS. |
| **start-stop** | (Optional) Indicates that the defined security server group will send a "start accounting" notice at the beginning of a process and a "stop accounting" notice at the end of a process. The "start accounting" record is sent in the background. (The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.) |
| **stop-only** | (Optional) Indicates that the defined security server group will send a "stop accounting" notice at the end of the requested user process. |
| **none** | (Optional) Indicates that the defined security server group will not send accounting notices. |
| **broadcast** | (Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |
| **group** *groupname* | At least one of the keywords described in the table below. |

## Command Default

This command is disabled by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |
| 12.1(1)T | • The optional **broadcast** keyword was added.<br>• The ability to specify multiple server groups was added.<br>• To accommodate multiple server groups, the name of the command was changed from **aaa dnis map accounting network group** to **aaa dnis map accounting network**. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process accounting requests for users dialing in to the network using that particular DNIS. To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

The table below contains descriptions of accounting method keywords.

***Table 10: AAA Accounting Methods***

| Keyword | Description |
|---|---|
| **group radius** | Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius command.** |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. |
| **group** group-name | Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*. |

In the table above, the **group radius**and **group tacacs +** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

## Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for accounting requests for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 acct-port 1646 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 accounting network group group1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa dnis map authentication ppp group** | Maps a DNIS number to a particular authentication server group. |
| **aaa dnis map enable** | Enables AAA server selection based on DNIS. |
| **aaa group server** | Groups different server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |

# aaa dnis map authentication group

To map a dialed number identification service (DNIS) number to a particular authentication server group (this server group will be used for authentication, authorization, and accounting [AAA] authentication), use the **aaa dnis map authentication group** command in AAA-server-group configuration mode. To remove the DNIS number from the defined server group, use the **no** form of this command.

**aaa dnis map** *dnis-number* **authentication** {**ppp** | **login**} **group** *server-group-name*
**no aaa dnis map** *dnis-number* **authentication** {**ppp** | **login**} **group** *server-group-name*

## Syntax Description

| | |
|---|---|
| *dnis-number* | Number of the DNIS. |
| **ppp** | Enables PPP authentication methods. |
| **login** | Enables character-mode authentication. |
| *server-group-name* | Character string used to name a group of security servers associated in a server group. |

## Command Default

A DNIS number is not mapped to a server group.

## Command Modes

AAA-server-group configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |
| 12.1(3)XL1 | This command was modified with the addition of the **login** keyword to include character-mode authentication. |
| 12.2(2)T | Support for the **login** keyword was added into Cisco IOS Release 12.2(2)T and this command was implemented for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 platforms. |
| 12.2(8)T | This command was implemented on the Cisco 806, Cisco 828, Cisco 1710, Cisco SOHO 78, Cisco 3631, Cisco 3725, Cisco 3745, and Cisco URM for IGX8400 platforms. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa dnis map authentication group** command to assign a DNIS number to a particular AAA server group so that the server group can process authentication requests for users that are dialing in to the network using that particular DNIS. To use the **aaa dnis map authentication group** command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

## Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 uses RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS number 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
 aaa dnis map enable
 aaa dnis map 7777 authentication ppp group group1
 aaa dnis map 7777 authentication login group group1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa dnis map accounting network group** | Maps a DNIS number to a particular accounting server group. |
| **aaa dnis map enable** | Enables AAA server selection based on DNIS. |
| **aaa group server** | Groups different server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |

# aaa dnis map authorization network group

To map a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group (the server group that will be used for AAA authorization), use the **aaa dnis map authorization network group**command in global configuration mode. To unmap this DNIS number from the defined server group, use the **no** form of this command.

**aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
**no aaa dnis map** *dnis-number* **authorization network group** *server-group-name*

## Syntax Description

| | |
|---|---|
| *dnis-number* | Number of the DNIS. |
| *server-group-name* | Character string used to name a group of security servers functioning within a server group. |

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process authorization requests for users dialing in to the network using that particular DNIS number. To use this command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

## Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for authorization requests for users dialing in with DNIS 7777:

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authorization network group group1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

| Command | Description |
|---|---|
| **aaa dnis map accounting network group** | Maps a DNIS number to a AAA server group used for accounting services. |
| **aaa dnis map authentication ppp group** | Maps a DNIS number to a AAA server used for authentication services. |
| **aaa dnis map enable** | Enables AAA server selection based on DNIS number. |
| **aaa group server** | Groups different server hosts into distinct lists and methods. |
| **radius-server host** | Specifies and defines the IP address of the RADIUS server host. |

# aaa group server diameter

To group different Diameter server hosts into distinct lists and distinct methods, enter the **aaa group server diameter**command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

**aaa group server diameter** *group-name*
**no aaa group server diameter** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Character string used to name the group of servers. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

The **aaa group server**diameter command introduces a way to group existing server hosts. This command enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are Diameter server hosts, RADIUS server hosts, and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

## Examples

The following example shows the configuration of a Diameter server group named dia_group_1 that comprises two member servers configured as Diameter peers:

```
aaa group server diameter dia_group_1
 server dia_peer_1
 server dia_peer_2
```



**Note** If a peer port is not specified, the default value for the peer port is 3868.

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| **aaa authentication login** | Sets AAA authentication at login. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **server** | Associates a Diameter server with a Diameter server group. |

# aaa group server ldap

To group different Lightweight Directory Access Protocol (LDAP) servers into distinct lists and distinct methods, use the **aaa group server ldap**command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

**aaa group server ldap** *group-name*
**no aaa group server ldap** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the server groups. |

## Command Default

No LDAP servers are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Usage Guidelines

The **aaa group server ldap** command enables you to group existing servers. This command allows you to select a subset of the configured server and use them for a particular service.

A group server is a list of servers of a particular type. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

**Note** LDAP authentication is not supported for interactive (terminal) sessions.

## Examples

The following example shows how to configure an LDAP server group named ldp_group_1:

```
Router> enable
Router(config)# aaa group server ldp_group_1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication login** | Sets AAA authentication at login. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **ldap server** | Defines an LDAP server and enters LDAP server configuration mode. |

# aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius**command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

**aaa group server radius** *group-name*
**no aaa group server radius** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Character string used to name the group of servers. See the table below for a list of words that cannot be used as the *group-name* argument. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.



**Note** When using external interfaces, such as serial or ATM interfaces, to support AAA server configuration over IPv6, you need to reconfigure the **source interface** command or use the Ethernet interface instead.

The table below lists words that cannot be used as the *group-name* argument.

***Table 11: Words That Cannot Be UsedAs the group-nameArgument***

| Word |
|---|
| **auth-guest** |
| **enable** |
| **guest** |

| Word |
|---|
| **if-authenticated** |
| **if-needed** |
| **krb5** |
| **krb-instance** |
| **krb-telnet** |
| **line** |
| **local** |
| **none** |
| **radius** |
| **rcmd** |
| **tacacs** |
| **tacacsplus** |

## Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
aaa group server radius radgroup1
 server 10.1.1.1 auth-port 1700 acct-port 1701
 server 10.2.2.2 auth-port 1702 acct-port 1703
 server 10.3.3.3 auth-port 1705 acct-port 1706
```



**Note** If auth-port and acct-port are not specified, the default value of auth-port is 1645 and the default value of acct-port is 1646.

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| **aaa authentication login** | Set AAA authentication at login. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |
| **source interface** | Specifies the address of an interface to be used as the source address. |

# aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists and distinct methods, use the **aaa group server**tacacs+ command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

**aaa group server tacacs**+ *group-name*
**no aaa group server tacacs**+ *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Character string used to name the group of servers. See the table below for a list of words that cannot be used as the *group-name* argument. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(54)SG | This command was integrated into Cisco IOS Release 12.2(54)SG. |
| Cisco IOS XE Release 3.2S | This command was modified. Support for IPv6 was added. |

## Usage Guidelines

The Authentication, Authorization, and Accounting (AAA) Server-Group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

The table below lists the keywords that cannot be used for the *group-name* argument value.

***Table 12: Words That Cannot Be UsedAs the group-nameArgument***

| Word |
|---|
| **auth-guest** |
| **enable** |
| **guest** |

| Word |
|---|
| **if-authenticated** |
| **if-needed** |
| **krb5** |
| **krb-instance** |
| **krb-telnet** |
| **line** |
| **local** |
| **none** |
| **radius** |
| **rcmd** |
| **tacacs** |
| **tacacsplus** |

## Examples

The following example shows the configuration of an AAA server group named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
server 10.1.1.1
server 10.2.2.2
server 10.3.3.3
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security. |
| **aaa authentication login** | Enables AAA accounting of requested services for billing or security purposes. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **aaa new-model** | Enables the AAA access control model. |
| **tacacs-server host** | Specifies a TACACS+ host. |

# aaa intercept

To enable lawful intercept on a router, use the **aaa intercept**command in global configuration mode. To disable lawful intercept, use the **no** form of this command.

**aaa intercept**
**no aaa intercept**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Lawful intercept is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into CiscoIOS XE Release 2.6. |

## Usage Guidelines

Use the **aaa intercept** command to enable a RADIUS-Based Lawful Intercept solution on your router. Intercept requests are sent (via Access-Accept packets or CoA-Request packets) to the network access server (NAS) or the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) from the RADIUS server. All data traffic going to or from a PPP or L2TP session is passed to a mediation device.

Configure this command with high administrative security so that unauthoried people cannot remove the command.

## Examples

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as NAS device employing a PPP over Ethernet (PPPoEo) link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
virtual-template 1
!
```

```
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface FastEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface FastEthernet5/0/0
description To subscriber
no ip address
!
interface FastEthernet5/0/0.1 point-to-point
pvc 10/808
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

# aaa local authentication attempts max-fail

To specify the maximum number of unsuccessful authentication attempts before a user is locked out, use the **aaa local authentication attempts max-fail**command in global configuration mode. To remove the setting for the number of unsuccessful attempts, use the **no** form of this command.

**aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
**no aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*

## Syntax Description

| | |
|---|---|
| *number-of-unsuccessful-attempts* | Number of unsuccessful authentication attempts. |

## Command Default

The Login Password Retry Lockout feature is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |

## Usage Guidelines

A system message is generated when a user is either locked by the system or unlocked by the system administrator:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

An administrator cannot be locked out.

**Note** No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

**Note** Unconfiguring this command will maintain the status of the user with respect to locked-out or number-of-failed attempts. To clear the existing locked-out or number-of-failed attempts, the system administrator has to explicitly clear the status of the user using **clear** commands.

## Examples

The following **example** illustrates that the maximum number of unsuccessful authentication attempts before a user is locked out has been set for 2:

```
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
```

```
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
ip subnet-zero
```

## Related Commands

| Command | Description |
|---|---|
| clear aaa local user fail-attempts | Clears the unsuccessful login attempts of the user. |
| **clear aaa local user lockout** | Unlocks the locked-out user. |
| show aaa local user locked | Displays a list of all locked-out users. |



# aaa max-sessions through algorithm


- aaa max-sessions, on page 125
- aaa memory threshold, on page 126
- aaa nas cisco-nas-port use-async-info, on page 128
- aaa nas port extended, on page 129
- aaa nas port option82, on page 130
- aaa nas redirected-station, on page 131
- aaa new-model, on page 133
- aaa password, on page 135
- aaa pod server, on page 137
- aaa preauth, on page 139
- aaa processes, on page 141
- aaa route download, on page 143
- aaa server radius dynamic-author, on page 145
- aaa service-profile, on page 147
- aaa session-id, on page 148
- aaa session-mib, on page 150
- aaa traceback recording, on page 152
- aaa user profile, on page 153
- access (firewall farm), on page 154
- access (server farm), on page 156
- access (virtual server), on page 158
- access session passthru-access-group, on page 160
- access-class, on page 161
- access-enable, on page 163
- access-group (identity policy), on page 165
- access-group mode, on page 166
- access-list (IP extended), on page 168
- access-list (IP standard), on page 181
- access-list (NLSP), on page 185
- access-list compiled, on page 188
- access-listcompileddata-linklimitmemory, on page 189
- access-listcompiledipv4limitmemory, on page 191
- access-list dynamic-extend, on page 193

- access-list remark, on page 194
- access-profile, on page 195
- access-restrict, on page 198
- access-session accounting, on page 200
- access-template, on page 201
- accounting, on page 203
- accounting (gatekeeper), on page 205
- accounting (line), on page 207
- accounting (server-group), on page 209
- accounting acknowledge broadcast, on page 213
- accounting dhcp source-ip aaa list, on page 214
- acl (ISAKMP), on page 215
- acl (WebVPN), on page 216
- acl drop, on page 217
- action-type, on page 219
- activate, on page 220
- add (WebVPN), on page 221
- address, on page 222
- address (IKEv2 keyring), on page 224
- address ipv4, on page 226
- address ipv4 (config-radius-server), on page 227
- address ipv6 (config-radius-server), on page 229
- address ipv4 (GDOI), on page 231
- address ipv6 (TACACS+), on page 232
- addressed-key, on page 233
- administrator authentication list, on page 235
- administrator authorization list, on page 237
- alert, on page 239
- alert (zone-based policy), on page 240
- alert-severity, on page 242
- alg sip blacklist, on page 243
- alg sip processor, on page 245
- alg sip timer, on page 246
- algorithm, on page 247

# aaa max-sessions

To set the maximum number of simultaneous authentication, authorization, and accounting (AAA) connections permitted for a user, use the **aaa max-sessions** command in global configuration mode. To disable the maximum number of sessions, use the **no** form of this command.

**aaa max-sessions** *maximum-number-of-sessions*
**no aaa max-sessions**

## Syntax Description

| | |
|---|---|
| *maximum-number-of-sessions* | Number of estimated AAA maximum sessions. The range is from 1024 to 64000. |

## Command Default

The default value for **aaa max-sessions** command is platform dependent.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Usage Guidelines

The **aaa max-sessions** command enables you to set the maximum number of simultaneous connections permitted for a user. The **aaa max-sessions** command can be used only if the **aaa new-model** command is configured.

## Examples

The following example shows how to adjust the initial hash size for the maximum number of simultaneous AAA sessions:

```
Router# configure terminal
Router(config)# aaa max-sessions 1025
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

# aaa memory threshold

To set appropriate threshold values for the authentication, authorization, and accounting (AAA) memory parameters, use the **aaa memory threshold** command in global configuration mode. To remove threshold values for the AAA memory parameters, use the **no** form of this command.

**aaa memory threshold** {**accounting disable** *available-memory* | **authentication reject** *available-memory*}
**no aaa memory threshold** {**accounting disable** | **authentication reject**}

## Syntax Description

| | |
|---|---|
| **accounting** | Sets the AAA accounting low-memory threshold. |
| **disable** | Disables the accounting threshold, if the available memory falls below the specified percentage. |
| *available-memory* | Available memory threshold. The range is from 1 to 15. |
| **authentication** | Sets the AAA authentication low-memory threshold. |
| **reject** | Rejects the AAA authentication request, if the available memory falls below the specified percentage. |
| *available-memory* | Available memory threshold. The range is from 2 to 15. |

## Command Default

The default memory threshold value for authentication is 3, and the default memory threshold value for accounting is 2.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Usage Guidelines

You must use the **aaa new-model** command to enable AAA.

## Examples

The following example shows how to set the threshold values for the AAA accounting low-memory threshold:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa memory threshold accounting disable 2
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa memory** | Displays the output of the AAA data structure memory tracing information. |

# aaa nas cisco-nas-port use-async-info

To display physical interface information and parent interface details as part of the of the cisco-nas-port vendor-specific attribute (VSA) for login calls, use the **aaa nas cisco-nas-port use-async-info**command in global configuration mode. To disable the command, use the **no** form of the command.

**aaa nas cisco-nas-port use-async-info**
**no aaa nas cisco-nas-port use-async-info**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The cisco-nas-port attribute has the format of tty*x*/*y* for login calls. Physical interface information is not included.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(17) | This command was introduced on the Cisco AS5800. |

## Usage Guidelines

This command enables the display of interface and parent interface details for login calls.

When this command is not configured, the cisco-nas-port attribute provides only tty*x*/*y* information for login calls. No physical interface information is included. For example:

```
Oct 14 18:42:53.113: RADIUS:  Vendor, Cisco       [26]  17
Oct 14 18:42:53.113: RADIUS:   cisco-nas-port     [2]   11  "tty1/2/07"
```

Other calls, such as PPP, include the physical interface and parent interface details. For example:

```
Oct 14 18:36:00.692: RADIUS:  Vendor, Cisco       [26]  33
Oct 14 18:36:00.692: RADIUS:   cisco-nas-port     [2]   27  "Async1/2/07*Serial1/1/2:0"
```

When you issue the **aaa nas cisco-nas-port use-async-info**command, the interface and parent interface details are included in the login calls.

## Examples

The following example shows how to enable the display of interface and parent interface details in the login calls :

```
aaa nas cisco-nas-port use-async-info
```

## Related Commands

| Command | Description |
|---|---|
| **aaa nas port extended** | Replaces the NAS-port attribute with RADIUS IETF attribute 26 and displays extended field information. |

# aaa nas port extended

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the **aaa nas port extended**command inglobal configuration mode. To display no extended field information, use the **no** form of this command.

**aaa nas port extended**
**no aaa nas port extended**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF Attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

## Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port extended
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server extended-portnames** | Displays expanded interface information in the NAS-Port attribute. |
| **radius-server vsa send** | Configures the network access server to recognize and use vendor-specific attributes. |

# aaa nas port option82

To send the remote-id and circuit-id as the NAS-Port-Id attribute in the Access-Request and Accounting-Request, use the **aaa nas port option82** command in global configuration mode. To disable this option, use the **no** form of this command.

**aaa nas port option82**
**no aaa nas port option82**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2SB | This command was introduced in Cisco IOS Release 12.2SB. |

## Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation of the RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with the vendor-specific attribute (VSA) RADIUS IETF Attribute 26. The Cisco vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. VSAs can be turned on by entering the **radius-server vsa send** command. The NAS-Port string information in this attribute is provided and configured using the **aaa nas port option82** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

The NAS-Port information is populated in the Intelligent Service Gateway (ISG) interface that has received the DHCP **option82** packet. When the **aaa nas port option82** command is configured, the NAS-Port is populated with the information regarding the remote-id and circuit-id. If this command is not configured, the NAS-Port is populated with the local ISG NAS-Port-Id.

## Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port option82
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server vsa send** | Configures the network access server to recognize and use VSAs. |

# aaa nas redirected-station

To include the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication, use the **aaa nas redirected-station** command in global configuration mode. To leave the original number out of the information sent to the authentication server, use the **no** form of this command.

**aaa nas redirected-station**
**no aaa nas redirected-station**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The original number is not included in the information sent to the authentication server.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If a customer is being authenticated by a RADIUS or TACACS+ server and the number dialed by the cable modem (or other device) is redirected to another number for authentication, the **aaa nas redirected-station** command will enable the original number to be included in the information sent to the authentication server.

This functionality allows the service provider to determine whether the customer dialed a number that requires special billing arrangements, such as a toll-free number.

The original number can be sent as a Cisco Vendor Specific Attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers. The RADIUS Attribute 93 is sent by default; to also send a VSA attribute for TACACS+ servers, use the **radius-server vsa send accounting** and **radius-server vsa send authentication** commands. To configure the RADIUS server to use RADIUS Attribute 93, add the non-standard option to the **radius-server host** command.



**Note** This feature is valid only when using port adapters that are configured for a T1 or E1 ISDN PRI or BRI interface. In addition, the telco switch performing the number redirection must be able to provide the redirected number in the Q.931 Digital Subscriber Signaling System Network Layer.

## Examples

The following example enables the original number to be forwarded to the authentication server:

```
!
aaa authorization config-commands
aaa accounting exec default start-stop group radius
```

```
aaa accounting system default start-stop broadcast group apn23
aaa nas redirected-station
aaa session-id common
ip subnet-zero
!
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server host** | Specifies a RADIUS server host. |
| **radius-server vsa** | Configures the network access server to recognize and use vendor-specific attributes. |

# aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

**aaa new-model**
**no aaa new-model**

## Syntax Description

This command has no arguments or keywords.

## Command Default

AAA is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2(33)SXI | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |
| 15.1(2)SNG | This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

This command enables the AAA access control system.

## Examples

The following example initializes AAA:

```
aaa new-model
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| **aaa authentication arap** | Enables an AAA authentication method for ARAP using TACACS+. |
| **aaa authentication enable default** | Enables AAA authentication to determine if a user can access the privileged command level. |

| Command | Description |
|---|---|
| **aaa authentication login** | Sets AAA authentication at login. |
| **aaa authentication ppp** | Specifies one or more AAA authentication method for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |

# aaa password

To configure restrictions for an authentication, authorization, and accounting (AAA) password, use the **aaa password** command in global configuration mode. To disable the password restriction, use the **no** form of this command.

**aaa password restriction**
**no aaa password restriction**

## Syntax Description

| | |
|---|---|
| **restriction** | Configures restrictions to the password. |

## Command Default

AAA passwords have no restrictions.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)S | This command was introduced. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S. |
| 15.1(4)M | This command was integrated into Cisco IOS Release 15.1(4)M. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

The **aaa password** command can be used only if the **aaa new-model** command is configured. The restrictions are not applied to passwords in the startup configurations. The restrictions are not applied to passwords that are already present in the configurations before the **aaa password** command is enabled.

Passwords are subject to the following restrictions:

- The new password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- The new password should not have a character repeated more than three times consecutively.
- The new password should not be the same as the associated username. The password obtained by capitalization of the username or username reversed is not accepted.
- The new password should not be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1”, “|”, or “!” for i, or by substituting “0” for “o”, or substituting “$” for “s”.

The restrictions can be applied to the passwords configured using the following commands: **aaa pod server**,**enable password**, **enable secret**, **radius-server host key**, **radius-server key**, **server-key**, and the**tacacs-server key**command.

## Examples

The following example shows how to configure restrictions for an AAA password:

```
Router(config)# aaa password restriction
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **aaa pod server** | Enables inbound user sessions to be disconnected when specific session attributes are present. |
| **enable password** | Sets a local password to control access to various privilege levels. |
| **enable secret** | Specifies an additional layer of security over the **enable password** command. |
| **radius-server key** | Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon. |
| **radius-server host** | Specifies a RADIUS server host. |
| **server-key** | Configure the RADIUS key to be shared between a device and RADIUS clients. |
| **tacacs-server host** | Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon. |
| **tacacs-server key** | Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon. |

# aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**aaa pod server** [**clients** *ip-address1 ip-address2 . . . ip-addressn*] [**port** *port-number*] {**auth-type** [**all ignore** | **any ignore**] **session-key server-key** *string* | **ignore** [**session-key**] **server-key** | **server-key** *string*}
**no aaa pod server**

## Syntax Description

| | |
|---|---|
| **clients** *ip-address* | (Optional) Registers the IP address of all the clients who can send POD requests. If this configuration is present and a POD request originates from a device that is not on the list, it is rejected. You can specify only four client IP addresses. |
| **port** *port number* | (Optional) Network access server User Datagram Protocol (UDP) port to use for packet of disconnect (POD) requests. Default value is 1700. |
| **auth-type** | Type of authorization required for disconnecting sessions. If no authentication type is specified, **auth-type** is the default. |
| **all** | (Optional) Only a session that matches all four key attributes is disconnected.T he default is **all**. |
| **any** | (Optional) Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). |
| **ignore** | Ignores the session key or the server key received in the POD packet for session matching. |
| **session-key** | Session with a matching session-key attribute is disconnected. All other attributes are ignored. |
| **server-key** | Configures the shared-secret text string. |
| *string* | Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems. |

## Command Default

The POD server function is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)XH | This command was introduced. |
| 12.1(3)T | This command was integrated into Cisco IOS Release 12.1(3)T. |

| Release | Modification |
|---|---|
| 12.2(2)XB | The encryption-type argument was added, as well as support for the voice applications and the Cisco 3600 series, and Cisco AS5350, and Cisco AS5400 routers. |
| 12.2(2)XB1 | Support for the Cisco AS5800 was added. |
| 12.2(11)T | The *encryption-type* argument and support for the voice applications were added.<br>**Note**<br>Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 is not included in this release. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was modified. The **clients** and **ignore** keywords were added. |

## Usage Guidelines

To disconnect a session, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no **auth-type** attribute is specified, all three values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte Message Digest 5 (MD5) hash value that is carried in the *authentication* field of the POD request.

## Examples

The following example shows how to enable POD and set the secret key to “xyz123”:

```
aaa pod server server-key xyz123
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting delay-start** | Delays generation of the start accounting record until the user IP address is established. |
| **aaa accounting** | Enables accounting records. |
| **debug aaa pod** | Displays debug messages for POD packets. |
| **radius-server host** | Identifies a RADIUS host. |

# aaa preauth

To enter authentication, authorization, and accounting (AAA) preauthentication configuration mode, use the **aaa preauth** command in global configuration mode. To disable preauthentication, use the **no** form of this command.

**aaa preauth**
**no aaa preauth**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Preauthentication is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To enter AAA preauthentication configuration mode, use the **aaa preauth** command. To configure preauthentication, use a combination of the **aaa preauth** commands: **group**, **clid**, **ctype**, **dnis**, and **dnis bypass**. You must configure the **group** command. You must also configure one or more of the **clid**, **ctype**, **dnis**, or **dnis bypass** commands.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

You can use the **clid**, **ctype**, or **dnis** commands to define the list of the preauthentication elements. For each preauthentication element, you can also define options such as password (for all the elements, the default password is cisco). If you specify multiple elements, the preauthentication process will be performed on each element according to the order of the elements that you configure with the preauthentication commands. In this case, more than one RADIUS preauthentication profile is returned, but only the last preauthentication profile will be applied to the authentication and authorization later on, if applicable.

## Examples

The following example enables dialed number identification service (DNIS) preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 dnis password Ascend-DNIS
```

## Related Commands

| Command | Description |
|---|---|
| **dnis (authentication)** | Enables AAA preauthentication using DNIS. |

| Command | Description |
|---|---|
| **group (authentication)** | Selects the security server to use for AAA preauthentication. |
| **isdn guard-timer** | Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request. |

# aaa processes

To allocate a specific number of background processes to be used to process authentication, authorization, and accounting (AAA) authentication and authorization requests for PPP, use the **aaa processes**command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

**aaa processes** *number*
**no aaa processes** *number*

## Syntax Description

| | |
|---|---|
| *number* | Specifies the number of background processes allocated for AAA requests for PPP. Valid entries are 1 to 2147483647. |

## Command Default

The default for this command is one allocated background process.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(2)AA | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **aaa processes** command to allocate a specific number of background processes to simultaneously handle multiple AAA authentication and authorization requests for PPP. Previously, only one background process handled all AAA requests for PPP, so only one new user could be authenticated or authorized at a time. This command configures the number of processes used to handle AAA requests for PPP, increasing the number of users that can be simultaneously authenticated or authorized.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP. This argument also defines the number of new users that can be simultaneously authenticated and can be increased or decreased at any time.

## Examples

The following examples shows the **aaa processes** command within a standard AAA configuration. The authentication method list “dialins” specifies RADIUS as the method of authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP. Ten background processes have been allocated to handle AAA requests for PPP.

```
aaa new-model
aaa authentication ppp dialins group radius local
aaa processes 10
interface 5
encap ppp
ppp authentication pap dialins
```

**Related Commands**

| Command | Description |
|---|---|
| **show ppp queues** | Monitors the number of requests processed by each AAA background process. |

# aaa route download

To enable the static route download feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of this command.

**aaa route download** [*time*] [**authorization** *method-list*]
**no aaa route download**

## Syntax Description

| | |
|---|---|
| *time* | (Optional) Time between downloads, in minutes. The range is from 1 to 1440 minutes. |
| **authorization** *method-list* | (Optional) Specify a named method list to which RADIUS authorization requests for static route downloads are sent. If these attributes are not set, all RADIUS authorization requests will be sent to the servers that are specified by the default method list. |

## Command Default

The default period between downloads (updates) is 720 minutes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.1 | This command was integrated into Cisco IOS Release 12.1. |
| 12.2(8)T | The **authorization** keyword was added; the *method-list* argument was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

This command is used to download static route details from the authorization, authentication, and accounting (AAA) server if the name of the router is *hostname*. The name passed to the AAA server for static routes is *hostname-1*, *hostname-2*... *hostname-n*--the router downloads static routes until it fails an index and no more routes can be downloaded.

## Examples

The following example sets the AAA route update period to 100 minutes:

```
aaa route download 100
```

The following example sets the AAA route update period to 10 minutes and sends static route download requests to the servers specified by the method list name “list1”:

```
aaa route download 10 authorization list1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization configuration default** | Downloads static route configuration information from the AAA server using TACACS+ or RADIUS. |
| **clear ip route download** | Clears static routes downloaded from a AAA server. |
| **show ip route** | Displays all static IP routes, or those installed using the AAA route download function. |

# aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

**aaa server radius dynamic-author**
**no aaa server radius dynamic-author**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The device will not function as a server when interacting with external policy servers.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.4 | This command was integrated into Cisco IOS Release 12.4. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 12.2(5)SXI | This command was integrated into Cisco IOS Release 12.2(5)SXI. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |
| | This command was introduced. |

## Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

**Dynamic Authorization for the Intelligent Services Gateway (ISG)**

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

## Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
```

```
client 10.12.12.12 key cisco
message-authenticator ignore
```

## Related Commands

| Command | Description |
|---|---|
| **auth-type (ISG)** | Specifies the server authorization type. |
| **client** | Specifies a RADIUS client from which a device will accept CoA and disconnect requests. |
| **default** | Sets a RADIUS application command to its default. |
| **domain** | Specifies username domain options. |
| **ignore** | Overrides a behavior to ignore certain paremeters. |
| **port** | Specifies a port on which local RADIUS server listens. |
| **server-key** | Specifies the encryption key shared with RADIUS clients. |

# aaa service-profile

To configure the service profile parameters for an authentication, authorization, and accounting (AAA) session, use the **aaa service-profile** command in global configuration mode. To disable the service profile parameters for AAA sessions, use the **no** form of this command.

**aaa service-profile key username-with-nasport**
**no aaa service-profile key username-with-nasport**

## Syntax Description

| | |
|---|---|
| **key** | Assigns a key to save and search service profiles. |
| **username-with-nasport** | Configures the AAA server to use the username and network access server (NAS) port as the service profile key. |

## Command Default

Service profiles are stored based on the username.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)S | This command was introduced. |

## Examples

The following example shows how to configure the service profile parameters for a AAA session:

```
Router# enable
Router# configure terminal
Router(config)# aaa service-profile key username-with-nasport
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa service-profiles** | Displays the service profiles downloaded and stored by a AAA session. |

# aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

**aaa session-id** [**common** | **unique**]
**no aaa session-id** [**unique**]

## Syntax Description

| | |
|---|---|
| **common** | (Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is **common**. |
| **unique** | (Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID. |

## Command Default

The **common** keyword is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)B | This command was introduced. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| | This command was integrated in Cisco IOS XE 16.12.1. |

## Usage Guidelines

The **common** keyword behavior allows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model** command is configured.



**Note** The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique

keyword must be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req**command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

## Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new model** | Enables AAA. |
| **radius-server attribute 44 include-in-access-req** | Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication). |

# aaa session-mib

To configure MIB options for Simple Network Management Protocol (SNMP) authentication, authorization, and accounting (AAA) sessions, use the aaa session-mib command in global configuration mode. To disable these options, use the **no** form of this command.

**aaa session-mib** {**disconnect** | **populate** {**setup** | **start**}}
**no aaa session-mib** {**disconnect** | **populate** {**setup** | **start**}}

## Syntax Description

| | |
|---|---|
| **disconnect** | Enables an AAA session MIB to disconnect authenticated clients using SNMP. |
| populate setup | Specifies that the AAA session MIB starts to track a session at the setup of the session. |
| populate start | Specifies that the AAA session MIB starts to track a session when accounting starts (when the START record is sent). |

## Command Default

No MIB options for SNMP AAA sessions are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.3(5) | The populate, setup and start keywords were added. |
| 12.3(5a)B | The populate, setup and start keywords were added. |
| 12.3(7)T | The populate, setup and start keywords were added. |
| 12.2(16)BX3 | The populate, setup and start keywords were added. |
| 12.3(7)XI | The populate, setup and start keywords were added. |
| 12.3(12) | The populate, setup and start keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The disconnect keyword enables termination of authenticated client connections via SNMP. Without this keyword, a network management station cannot perform set operations and disconnect users (it can only poll the table).

The populate keyword determines when reporting of a locally terminated sessions begins. Two options are provided: setup (default) and start. The setup keyword begins tracking the session parameters during the setup

of a session while the start keyword begins when the accounting START notification is generated and sent. By default, Cisco AAA session MIB begins reporting sessions generated during setup.

## Examples

The following example shows how to enable the disconnection of authenticated clients using SNMP:

```
Router> enable
Router# configure terminal
Router(config)# aaa session-mib disconnect
```

The following example shows how to start tracking of a session at setup:

```
Router> enable
Router# configure terminal
Router(config)# aaa session-mib populate setup
```

# aaa traceback recording

To enable traceback recording on an authentication, authorization, and accounting (AAA) server, use the **aaa traceback recording** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**aaa traceback recording**
**no aaa traceback recording**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Traceback recording is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Examples

The following example shows how to enable traceback recording on a AAA server:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa traceback recording
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

# aaa user profile

To create an authentication, authorization, and accounting (AAA) named user profile, use the **aaa user profile**command in global configuration mode. To remove a user profile from the configuration, use the **no** form of this command.

**aaa user profile** *profile-name*
**no aaa user profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Character string used to name the user profile. The maximum length of the character string is 63 characters. Longer strings will be truncated. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |
| 12.3(3.8) | The maximum length of the *profile-name* argument is set at 63 characters. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **aaa user profile**command to create a AAA user profile. Used in conjunction with the aaa attribute command, which adds calling line identification (CLID) and dialed number identification service (DNIS) attribute values, the user profile can be associated with the record that is sent to the RADIUS server (via the **test aaa group**command), which provides the RADIUS server with access to CLID or DNIS attribute information when the server receives a RADIUS record.

## Examples

The following example shows how to configure a dnis = dnisvalue user profile named “prfl1”:

```
aaa user profile prfl1
 aaa attribute dnis
 aaa attribute dnis dnisvalue
 no aaa attribute clid
! Attribute not found.
 aaa attribute clid clidvalue
 no aaa attribute clid
```

## Related Commands

| Command | Description |
|---|---|
| **aaa attribute** | Adds DNIS or CLID attribute values to a user profile. |
| **test aaa group** | Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server. |

# access (firewall farm)

To route specific flows to a firewall farm, use the **access**command in firewall farm configuration mode. To restore the default settings, use the **no** form of this command.

**access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]
**no access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]

## Syntax Description

| | |
|---|---|
| **source** | (Optional) Routes flows based on source IP address. |
| *source-ip* | (Optional) Source IP address. The default is 0.0.0.0 (all sources). |
| *netmask* | (Optional) Source IP network mask. The default is 0.0.0.0 (all source subnets). |
| **destination** | (Optional) Routes flows based on destination IP address. |
| *destination-ip* | (Optional) Destination IP address. The default is 0.0.0.0 (all destinations). |
| *netmask* | (Optional) Destination IP network mask. The default is 0.0.0.0 (all destination subnets). |
| **inbound** *inbound-interface* | (Optional) Indicates that the firewall farm is to accept inbound packets only on the specified inbound interface.<br>You can specify a subinterface, such as Gigabitethernet7/3.100, for the *inbound-interface*argument. |
| **inbound datagram connection** | (Optional) Indicates that IOS SLB is to create connections for inbound traffic as well as outbound traffic. |
| **outbound** *outbound-interface* | (Optional) Indicates that the firewall farm is to accept outbound packets only on the specified outbound interface.<br>You can specify a subinterface, such as Gigabitethernet7/3.100, for the *outbound-interface*argument. |

## Command Default

The default source IP address is 0.0.0.0 (routes flows from all sources to this firewall farm). The default source IP network mask is 0.0.0.0 (routes flows from all source subnets to this firewall farm). The default destination IP address is 0.0.0.0 (routes flows from all destinations to this firewall farm). The default destination IP network mask is 0.0.0.0 (routes flows from all destination subnets to this firewall farm). If you do not specify an inbound interface, the firewall farm accepts inbound packets on all inbound interfaces. If you do not specify the **inbound datagram connection** option, IOS SLB creates connections only for outbound traffic. If you do not specify an outbound interface, the firewall farm accepts outbound packets on all outbound interfaces.

## Command Modes

Firewall farm configuration (config-slb-fw)

## Command History

| Release | Modification |
|---|---|
| 12.1(7)E | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXE | The **inbound** and **outbound** keywords and *inbound-interface* and *outbound-interface* arguments were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRE | This command was modified.<br>The **datagram connection** keywords were added.<br>The *inbound-interface*and *outbound-interface*arguments can be subinterfaces. |

## Usage Guidelines

You can specify more than one source or destination for each firewall farm. To do so, configure multiple **access** statements, making sure the network masks do not overlap each other.

You can specify up to two inbound interfaces and two outbound interfaces for each firewall farm. To do so, configure multiple **access** statements, keeping the following considerations in mind:

- All inbound and outbound interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).
- All inbound and outbound interfaces must be different from each other.
- You cannot change inbound or outbound interfaces for a firewall farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the firewall farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

By default, IOS SLB firewall load balancing creates connections only for outbound traffic (that is, traffic that arrives through the real server). Inbound traffic uses those same connections to forward the traffic, which can impact the CPU. To enable IOS SLB to create connections for both inbound traffic and outbound traffic, reducing the impact on the CPU, use the **access inbound datagram connection** command.

## Examples

The following example routes flows with a destination IP address of 10.1.6.0 to firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0
```

## Related Commands

| Command | Description |
|---|---|
| **show ip slb firewallfarm** | Displays information about the firewall farm configuration. |

# access (server farm)

To configure an access interface for a server farm, use the **access** command in server farm configuration mode. To disable the access interface, use the **no** form of this command.

**access** *interface*
**no access** *interface*

## Syntax Description

| | |
|---|---|
| *interface* | Interface to be inspected. The server farm will handle outbound flows from real servers only on the specified interface.<br>You can specify a subinterface, such as Gigabitethernet7/3.100, for the *interface*argument. |

## Command Default

The server farm handles outbound flows from real servers on all interfaces.

## Command Modes

Server farm configuration (config-slb-sfarm)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRE | This command was modified. The *interface*argument can be a subinterface. |

## Usage Guidelines

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two access interfaces for each server farm. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- The access interfaces of primary and backup server farms must be the same.
- You cannot change the interfaces for a server farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the server farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

## Examples

The following example limits the server farm to handling outbound flows from real servers only on access interface Vlan106:

```
Router(config)# ip slb serverfarm SF1
Router(config-slb-sfarm)# access Vlan106
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip slb serverfarms** | Displays information about the server farms. |

# access (virtual server)

To enable framed-IP routing to inspect the ingress interface, use the **access** command in virtual server configuration mode. To disable framed-IP routing, use the **no** form of this command.

**access** *interface* [**route framed-ip**]
**no access** *interface* [**route framed-ip**]

## Syntax Description

| | |
|---|---|
| *interface* | Interface to be inspected.<br>You can specify a subinterface, such as Gigabitethernet7/3.100, for the *interface*argument. |
| **route framed-ip** | (Optional) Routes flows using framed-IP routing. |

## Command Default

Framed-IP routing cannot inspect the ingress interface.

## Command Modes

Virtual server configuration (config-slb-vserver)

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)E | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXE | The command was modified to accept up to two framed-IP access interfaces (specified on separate commands). |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRE | This command was modified. The *interface*argument can be a subinterface. |

## Usage Guidelines

This command enables framed-IP routing to inspect the ingress interface when routing subscriber traffic. All framed-IP sticky database entries created as a result of RADIUS requests to this virtual server will include the interface in the entry. In addition to matching the source IP address of the traffic with the framed-IP address, the ingress interface must also match this interface when this command is configured.

You can use this command to allow subscriber data packets to be routed to multiple service gateway service farms.

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two framed-IP access interfaces for each virtual server. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- You cannot change the interfaces for a virtual server while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the virtual server in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

## Examples

The following example enables framed-IP routing to inspect ingress interface Vlan20:

```
Router(config)# ip slb vserver SSG_AUTH
Router(config-slb-vserver)# access Vlan20 route framed-ip
```

## Related Commands

| Command | Description |
|---|---|
| **show ip slb vservers** | Displays information about the virtual servers defined to IOS SLB. |

# access session passthru-access-group

To map the FQDN ACL with the domain name, use the **access session passthru-access-group** command in global configuration mode. To remove FQDN ACL from the domain name, use the **no** form of the command.

**access session passthru-access-group** *acl_name* **passthru-domain-list** *domain_name*
**no access session passthru-access-group** *acl_name* **passthru-domain-list** *domain_name*

## Syntax Description

| | |
|---|---|
| *acl_name* | Name of the FQDN ACL. |
| **passthru-domain-list** *domain_name* | Configures the domain name list to be mapped to the FQDN ACL. |

## Command Default

No domain is mapped to an FQDN ACL.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.6E | This command was introduced. |

This example shows how to map the FQDN ACL with the domain name:

```
Device(config)# access session passthru-access-group abc passthru-domain-list abc
```

# access-class

To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

**access-class** *access-list-number* {**in** [**vrf-also**] | **out**}
**no access-class** *access-list-number* {**in** | **out**}

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699 . |
| **in** | Restricts incoming connections between a particular Cisco device and the addresses in the access list. |
| **vrf-also** | (Optional) Accepts incoming connections from interfaces that belong to a VRF. |
| **out** | Restricts outgoing connections between a particular Cisco device and the addresses in the access list. |

## Command Default

No access lists are defined.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2 | The **vrf-also** keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Remember to set *identical restrictions* on all the virtual terminal lines because a user can connect to any of them.

To display the access lists for a particular terminal line, use the **show line** EXEC command and specify the line number.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

## Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0 0.0.0.255
```

```
 line 1 5
 access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 10.0.0.0 on terminal lines 1 through 5:

```
access-list 10 permit 10.0.0.0 0.255.255.255
 line 1 5
 access-class 10 out
```

## Related Commands

| Command | Description |
|---|---|
| **show line** | Displays the parameters of a terminal line. |

# access-enable

To e na b le the router to create a temporary access list entry in a dynamic access list, use the **access-enable** command in EXEC mode.

**access-enable** [**host**] [**timeout** *minutes*]

## Syntax Description

| | |
|---|---|
| **host** | (Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network. |
| **timeout** *minutes* | (Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection. |

## Command Default

No default behavior or values.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command enables the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the temporary access list entry will remain, even after the user terminates the session.

Use the **autocommand** command with the **access-enable** command to cause the **access-enable** command to execute when a user opens a Telnet session into the router.

## Examples

The following example causes the software to create a temporary access list entry and tells the software to enable access only for the host from which the Telnet session originated. If the access list entry is not accessed within 2 minutes, it is deleted.

```
autocommand access-enable host timeout 2
```

## Related Commands

| Command | Description |
|---|---|
| **access-list (IP extended)** | Defines an extended IP access list. |

| Command | Description |
|---|---|
| **autocommand** | Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line. |
| **show ip accounting** | Displays the active accounting or checkpointed database or displays access list violations. |

# access-group (identity policy)

To specify an access group to be applied to an identity policy, use the **access-group** command in identity policy configuration mode. To remove the access group, use the **no** form of this command.

**access-group group-name**
**no access-group group-name**

## Syntax Description

| | |
|---|---|
| *group-name* | Access list name. |

## Command Default

An access group is not specified.

## Command Modes

Identity policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

Using this command, you can access only named access lists.

## Examples

The following example shows that access group "exempt-acl" is to be applied to the identity policy "policyname1":

```
Router (config)# identity policy policyname1
Router (config-identity-policy)# access-group exempt-acl
```

## Related Commands

| Command | Description |
|---|---|
| **identity profile** | Creates an identity profile. |

# access-group mode

To specify override and nonoverride modes for an access group, use the **access-group mode** command in interface configuration mode. To return to merge mode, use the **no** form of this command.

**access-group mode** {**prefer** {**port** | **vlan**} | **merge**}
**no access-group mode** {**prefer** {**port** | **vlan**} | **merge**}

## Syntax Description

| | |
|---|---|
| **prefer port** | Specifies that port access control list (ACL) features that are configured on an interface port take precedence over features configured on a VLAN interface. (That is, features configured on the switch virtual interface [SVI] and the port are not merged.) |
| **prefer vlan** | Specifies that the VLAN-based ACL mode takes precedence if VLAN-based ACL features are configured on a VLAN interface. If no VLAN-based ACL features are configured on the VLAN interface, port ACL features are applied on the interface port. |
| **merge** | Merges features configured on the interface port and the interface VLAN. This merged feature is programmed into the hardware. |

## Command Default

The default is merge mode.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXH | This command was introduced. |
| 12.2(33)SXI4 | This command was modified. Support for IPv6 was added. The **prefer vlan** keyword combination is not supported on Cisco IOS Release 12.2(33)SXI4. |
| 12.2(54)SG | This command was integrated into Cisco IOS Release 12.2(54)SG. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |
| Cisco IOS XE Release 3.7S | This command was integrated into Cisco IOS XE Release 3.7S. |

## Usage Guidelines

An SVI is a VLAN of switch ports that are represented by one interface to a routing or bridging system. VLAN ACLs or VLAN maps control the access of all packets (bridged and routed) to an interface.

Port ACLs perform access control on the traffic that enters a Layer 2 interface. Layer 2 interfaces support prefer ports, prefer VLANs, and merge modes. Layer 2 interfaces can have one IP ACL applied in either direction (one at the ingress and one at the egress). Layer 2 interfaces can have only one IPv6 ACL; either in the ingress or egress direction.

In Cisco IOS Release 12.2(33)SXI4, only prefer ports and merge modes are supported on Layer 2 interfaces.

To apply an IPv4 port ACL and a MAC ACL on a trunk port, you must configure the **access-group mode prefer port** command on the trunk port.

## Examples

The following example shows how to configure an interface to use prefer port mode:

```
Device(config-if)# access-group mode prefer port
```

The following example shows how to configure an interface to use merge mode:

```
Device(config-if)# access-group mode merge
```

## Related Commands

| Command | Description |
|---|---|
| **show access-group mode interface** | Displays the ACL configuration on a Layer 2 interface. |

# access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** command in global configuration mode . To remove the access lists, use the **no** form of this command.

**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]
**no access-list** *access-list-number*

**Internet Control Message Protocol (ICMP)**
**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]*icmp-message*] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

**Internet Group Management Protocol (IGMP)**
**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

**Transmission Control Protocol (TCP)**
**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

**User Datagram Protocol (UDP)**
**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence* | **dscp** *dscp* | **tos** *tos* | **time-range** *time-range-name* | **fragments** | **log** [*word*] | | **log-input** [*word*]]

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699. |
| **dynamic** *dynamic-name* | (Optional) Identifies this access list as a dynamic access list. Refer to lock-and- key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide* . |
| **timeout** *minutes* | (Optional) Specifies the absolute length of time, in minutes, that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*. |
| **deny** | Denies access if the conditions are matched. |
| **permit** | Permits access if the conditions are matched. |

| | |
|---|---|
| *protocol* | Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword. Some protocols allow further qualifiers described below. |
| *source* | Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:<br>• Use a 32-bit quantity in four-part dotted decimal format.<br>• Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.<br>• Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0. |
| *source-wildcard* | Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry.<br>There are three alternative ways to specify the source wildcard:<br>• Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore.<br>• Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.<br>• Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.<br>Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0. would be valid. |
| *destination* | Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:<br>• Use a 32-bit quantity in four-part dotted decimal format.<br>• Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.<br>• Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0. |

| | |
|---|---|
| *destination-wildcard* | Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:<br>• Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore.<br>• Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.<br>• Use **host** destination as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0. |
| **precedence** *precedence* | (Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines." |
| **tos** *tos* | (Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines." |
| **dscp** | Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values. |
| **time-range** *time-range-name* | (Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command. |
| *icmp-type* | (Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255. |
| *icmp-code* | (Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255. |
| *icmp-message* | (Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section "Usage Guidelines." |
| *igmp-type* | (Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines." |
| *operator* | (Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).<br>If the operator is positioned after the *source* and *source-wildcard*, it must match the source port.<br>If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port.<br>The **range** operator requires two port numbers. All other operators require one port number. |

| | |
|---|---|
| *port* | (Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines." TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.<br><br>TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP. |
| **established** | (Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST control bits set. The nonmatching case is that of the initial TCP datagram to form a connection. |
| **fragments** | (Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see “Access List Processing of Fragments" and “Fragments and Policy Routing” in the *Usage Guidelines* section. |
| **log** | (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.)<br><br>The log message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and if appropriate, the source and destination addresses and port numbers and the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.<br><br>The logging facility may drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.<br><br>After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command. |
| *word* | (Optional) User-defined cookie appended to the log message. The cookie:<br>• cannot be more than characters<br>• cannot start with hexadecimal notation (such as 0x)<br>• cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range**<br>• must contain alphanumeric characters only<br><br>The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry. |

| | |
|---|---|
| **log-input** | (Optional) Includes the input interface and source MAC address or virtual circuit in the logging output.<br>After you specify the **log-input** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command. |

## Command Default

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 10.3 | The following keywords and arguments were added:<br>• *source*<br>• *source-wildcard*<br>• *destination*<br>• *destination-wildcard*<br>• **precedence** *precedence*<br>• *icmp-type*<br>• *icmp-code*<br>• *icmp-message*<br>• *igmp-type*<br>• *operator*<br>• *port*<br>• **established** |
| 11.1 | The dynamic dynamic-name keyword and argument were added. |
| 11.1 | The timeout minutes keyword and argument were added. |
| 11.2 | The **log-input**keyword was added. |
| 12.0(1)T | The **time-range** *time-range-name* keyword and argument were added. |
| 12.0(11) | The **fragments**keyword was added. |
| 12.2(13)T | The **non500-isakmp** keyword was added to the list of UDP port names. The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software. |
| 12.4 | The **drip** keyword was added to specify the TCP port number used for OER communication. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(22)T | The *word* argument was added to the **log** and **log-input** keywords. |
| 15.1(2)SNG | This command was integrated into the Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

You can use access lists to control the transmission of packets on an interface, control Virtual Terminal Line (VTY) access, and restrict the contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control VTY access or restrict the contents of routing updates must not match against the TCP source port, the type of service (ToS) value, or the precedence of the packet.



**Note** After a numbered access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific numbered access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type and code names:

- **administratively-prohibited**

- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**

- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **drip**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**

- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dnsix**
- **domain**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **non500-isakmp**

- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

### Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

| If the Access-List Entry has... | Then.. |
|---|---|
| ...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches, | For an access-list entry containing only Layer 3 information:<br>• The entry is applied to nonfragmented packets, initial fragments and noninitial fragments.<br><br>For an access list entry containing Layer 3 and Layer 4 information:<br>• The entry is applied to nonfragmented packets and initial fragments.<br>  • If the entry is a **permit**statement, the packet or fragment is permitted.<br>  • If the entry is a **deny**statement, the packet or fragment is denied.<br>• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and<br>  • If the entry is a **permit**statement, the noninitial fragment is permitted.<br>  • If the entry is a **deny** statement, the next access-list entry is processed.<br><br>**Note**<br>The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments. |

| If the Access-List Entry has... | Then.. |
|---|---|
| ...the **fragments** keyword, and assuming all of the access-list entry information matches, | The access-list entry is applied only to noninitial fragments.<br>**Note**<br>The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information. |

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

**Note** The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

**Fragments and Policy Routing**

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

**Permitting Optimized Edge Routing (OER) Communication**

The drip keyword was introduced under the **tcp** keyword to support packet filtering in a network where OER is configured. The drip keyword specifies port 3949 that OER uses for internal communication. This option allows you to build a packet filter that permits communication between an OER primary controller and border router(s). The drip keyword is entered following the TCP source, destination, and the **eq** operator. See the example at the end of this command reference page.

## Examples

In the following example, serial interface 0 is part of a Class B network with the address 10.88.0.0, and the address of the mail host is 10.88.1.2. Th e **established** keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicates that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 10.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 10.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 10.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 10.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. Wildcard bits are similar to the bitmasks that are used with normal access lists. Prefix or mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix or mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.168.0.0 255.255.0.0 but denies any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0   255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example permits 10.108.0/24 but denies 10.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0     255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0   0.0.255.255
```

The following example uses a time range to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
access-list 101 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group 101 in
```

The following example permits communication, from any TCP source and destination, between an OER primary controller and border router:

```
access-list 100 permit tcp any eq drip any eq drip
```

The following example shows how to configure the access list with the **log** keyword. It sets the *word* argument to UserDefinedValue. The word UserDefinedValue is appended to the related syslog entry:

```
Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log UserDefinedValue
```

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

```
Router(config)# access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Router(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

## Related Commands

| Command | Description |
|---|---|
| **access-class** | Restricts incoming and outgoing connections between a particular VTY (into a Cisco device) and the addresses in an access list. |
| **access-list (IP standard)** | Defines a standard IP access list. |
| **access-list remark** | Writes a helpful comment (remark) for an entry in a numbered IP access list. |
| **clear access-template** | Clears a temporary access list entry from a dynamic access list. |
| **delay (tracking)** | Sets conditions under which a packet does not pass a named access list. |
| **distribute-list in (IP)** | Filters networks received in updates. |
| **distribute-list out (IP)** | Suppresses networks from being advertised in updates. |
| **ip access-group** | Controls access to an interface. |
| **ip access-list** | Defines an IP access list by name. |
| **ip access-list logging hash-generation** | Enables hash value generation for ACE syslog entries. |
| **ip accounting** | Enables IP accounting on an interface. |
| **logging console** | Controls which messages are logged to the console, based on severity. |
| **match ip address** | Distributes any routes that have a destination network number address that is permitted by a standard or extended access list. |
| **permit (IP)** | Sets conditions under which a packet passes a named access list. |
| **remark** | Writes a helpful comment (remark) for an entry in a named IP access list. |
| **show access-lists** | Displays the contents of current IP and rate-limit access lists. |
| **show ip access-list** | Displays the contents of all current IP access lists. |
| **time-range** | Specifies when an access list or other feature is in effect. |

# access-list (IP standard)

To define a standard IP access list, use the s tandard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log** [*word*]]
**no access-list** *access-list-number*

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999. |
| **deny** | Denies access if the conditions are matched. |
| **permit** | Permits access if the conditions are matched. |
| *source* | Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source:<br>• Use a 32-bit quantity in four-part, dotted-decimal format.<br>• Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. |
| *source-wildcard* | (Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard:<br>• Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore.<br>• Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. |
| **log** | (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.)<br>The log message includes the access list number, whether the packet was permitted or denied, the source address, the number of packets, and if appropriate, the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.<br>The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. |

| | |
|---|---|
| *word* | (Optional) User-defined cookie appended to the log message. The cookie:<br>• cannot be more than characters<br>• cannot start with hexadecimal notation (such as 0x)<br>• cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range**<br>• must contain alphanumeric characters only<br>The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry. |

## Command Default

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 11.3(3)T | The **log** keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(22)T | The *word* argument was added to the **log** keyword. |

## Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.



**Caution** Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This condition could cause you severe security problems**. Save your old configuration file before booting these images.

## Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 10.88.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 10.48.0.3
access-list 2 permit 10.48.0.3 0.0.0.0
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected. In addition, the logging mechanism is enabled and the word SampleUserValue is appended to each syslog entry.

```
Router(config)# access-list 1 permit 10.29.2.64 0.0.0.63 log SampleUserValue
```

## Related Commands

| Command | Description |
|---|---|
| **access-class** | Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list. |
| **access-list (IP extended)** | Defines an extended IP access list. |
| **access-list remark** | Writes a helpful comment (remark) for an entry in a numbered IP access list. |
| **deny (IP)** | Sets conditions under which a packet does not pass a named access list. |
| **distribute-list in (IP)** | Filters networks received in updates. |
| **distribute-list out (IP)** | Suppresses networks from being advertised in updates. |
| **ip access-group** | Controls access to an interface. |
| **ip access-list logging hash-generation** | Enables hash value generation for ACE syslog entries. |
| **permit (IP)** | Sets conditions under which a packet passes a named access list. |

| Command | Description |
|---|---|
| **remark (IP)** | Writes a helpful comment (remark) for an entry in a named IP access list. |
| **show access-lists** | Displays the contents of current IP and rate-limit access lists. |
| **show ip access-list** | Displays the contents of all current IP access lists. |

# access-list (NLSP)

To define an access list that denies or permits area addresses that summarize routes, use the NetWare Link-Services Protocol (NLSP) route aggregation version of the **access-list** command in global configuration mode. To remove an NLSP route aggregation access list, use the **no**form of this command.

**access-list** *access-list-number* {**deny** | **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]
**no access-list** *access-list-number* {**deny** | **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the access list. This is a number from 1200 to 1299. |
| **deny** | Denies redistribution of explicit routes if the conditions are matched. If you have enabled route summarization with route-aggregation command, the router redistributes an aggregated route instead. |
| **permit** | Permits redistribution of explicit routes if the conditions are matched. |
| *network* | Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks.<br>You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. |
| *network-mask* | Specifies the portion of the network address that is common to all addresses in the route summary. The high-order bits of *network-mask* must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted. |
| *interface* | (Optional) Interface on which the access list should be applied to incoming updates. |
| **ticks** *ticks* | (Optional) Metric assigned to the route summary. The default is 1 tick. |
| **area-count** *area-count* | (Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas. |

## Command Default

No access lists are predefined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.0 | The *interface* argument was added. |

| Release | Modification |
|---|---|
| 12.2(13)T | This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in12.2S-Family releases. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the NLSP route aggregation access list in the following situations:

- When redistributing from an Enhanced IGRP or RIP area into a new NLSP area.

Use the access list to instruct the router to redistribute an aggregated route instead of the explicit route. The access list also contains a "permit all" statement that instructs the router to redistribute explicit routes that are not subsumed by a route summary.

- When redistributing from an NLSP version 1.0 area into an NLSP version 1.1 area, and vice versa.

From an NLSP version 1.0 area into an NLSP version 1.1 area, use the access list to instruct the router to redistribute an aggregated route instead of an explicit route and to redistribute explicit routes that are not subsumed by a route summary.

From an NLSP version 1.1 area into an NLSP version 1.0 area, use the access list to instruct the router to filter aggregated routes from passing into the NLSP version 1.0 areas and to redistribute explicit routes instead.



**Note** NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

## Examples

The following example uses NLSP route aggregation access lists to redistribute routes learned from RIP to NLSP area1. Routes learned via RIP are redistributed into NLSP area1. Any routes learned via RIP that are subsumed by aaaa0000 ffff0000 are not redistributed. An address summary is generated instead.

```
ipx routing
ipx internal-network 2000
interface ethernet 1
 ipx network 1001
 ipx nlsp area1 enable
interface ethernet 2
 ipx network 2001
access-list 1200 deny aaaa0000 ffff0000
access-list 1200 permit -1
ipx router nlsp area
 area-address 1000 fffff000
 route-aggregation
 redistribute rip access-list 1200
```

## Related Commands

| Command | Description |
|---|---|
| **area-address (NLSP)** | Defines a set of network numbers to be part of the current NLSP area. |
| **deny (NLSP)** | Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list. |
| **ipx access-list** | Defines an IPX access list by name. |
| **ipx nlsp enable** | Configures the interval between the transmission of hello packets. |
| **ipx router** | Specifies the routing protocol to use. |
| **permit (NLSP)** | Allows explicit route redistribution in a named NLSP route aggregation access list. |
| **prc-interval** | Controls the hold-down period between partial route calculations. |
| **redistribute (IPX)** | Redistributes from one routing domain into another. |

# access-list compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **a ccess-list compiled**commandinglobal configuration mode. To disable the Turbo ACL feature, use the **no**form of this command.

**access-list compiled**
**no access-list compiled**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Turbo ACL is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(6)S | This command was introduced. |
| 12.1(1)E | This command was introduced for Cisco 7200 series routers. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(4)E | This command was implemented on the Cisco 7100 series. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the access-list compiled command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

## Examples

The following example enables the Turbo ACL feature:

```
access-list compiled
```

# access-listcompileddata-linklimitmemory

To change the amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled data-link limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

**access-list compiled data-link limit memory** *number*
**no access-list compiled data-link limit memory**
**default access-list compiled data-link limit memory**

## Syntax Description

| | |
|---|---|
| *number* | A number between 8 and 4095 that specifies the amount of memory, in megabytes, reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for the Cisco 7304 router using an NSE. |

## Command Default

The default for *number* is 128.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |

## Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled**output, which are found in the "Compiled ACL statistics for Data-Link" section of the output, are especially useful:

- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The "Mb limit" output shows the current memory limit setting.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 3 and Layer 4 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled ipv4 limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 2 ACL processing in the RP path.

To restore a default configuration of this command, which is 128 MB, enter the **default** form of this command.

## Examples

The following example reserves 100 MB of memory for Layer 2 ACL processing in the RP path:

```
access-list compiled data-link limit memory 100
```

The following example allows Layer 2 ACL processing to use as much memory as is needed for Layer 2 ACL processing:

```
no access-list compiled data-link limit memory
```

The following example restores the default amount of memory reserved for Layer 2 ACL processing in the RP path:

```
default access-list compiled data-link limit memory
```

## Related Commands

| Command | Description |
|---|---|
| **access-list compiled ipv4 limit memory** | Configures limits on the amount of memory used for Turbo ACL processing of Layer 3 and Layer 4 traffic. |
| **show access-list compiled** | Displays the status and condition of the Turbo ACL tables associated with each access list. |

# access-listcompiledipv4limitmemory

To change the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled ipv4 limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

**access-list compiled ipv4 limit memory** *number*
**no access-list compiled ipv4 limit memory**
**default access-list compiled ipv4 limit memory**

## Syntax Description

| | |
|---|---|
| *number* | A number between 8 and 4095 that specifies the memory limit in megabytes. |

## Command Default

On an NSE-150, the default for *number* is always 256.

On an NSE-100, the default for *number* is determined by the amount of SDRAM on the NSE-100. If the NSE-100 has 512 MB of DRAM, the default for *number* is 256. If the NSE-100 has less than 512 MB DRAM, the default for *number* is 128.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |

## Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled**output, which are found in the "Compiled ACL statistics for IPv4:" section of the output, are especially useful:

- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The "Mb limit" output shows the current memory limit setting.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 2 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled data-link limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 3 and Layer 4 ACL processing in the RP path.

To restore a default configuration of this command, enter the **default** form of this command.

## Examples

The following example reserves 100 MB of memory for Layer 3 and Layer 4 ACL processing in the RP path:

```
access-list compiled ipv4 limit memory 100
```

The following example allows Layer 3 and Layer 4 ACL processing to use as much memory as is needed for Layer 3 and Layer 4 ACL processing:

```
no access-list compiled ipv4 limit memory
```

The following example restores the default amount of memory reserved for Layer 3 and Layer 4 ACL processing in the RP path:

default access-list compiled ipv4 limit memory

## Related Commands

| Command | Description |
|---|---|
| **access-list compiled data-link limit memory** | Configures memory limits on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic. |
| **show access-list compiled** | Displays the status and condition of the Turbo ACL tables associated with each access list |

# access-list dynamic-extend

To allow the absolute timer of the dynamic acce ss control list (ACL) to be extended an additional six minutes, use the **access-list dynamic-extend** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**access-list dynamic-extend**
**no access-list dynamic-extend**

## Syntax Description

This command has no arguments or keywords.

## Command Default

6 minutes

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you try to create a Telnet session to the router to re-authenticate yourself by using the lock-and-key function, use the **access-list dynamic-extend** command to extend the absolute timer of the dynamic ACL by six minutes.

The router must already be configured with the lock-and-key feature, and you must configure the extension before the ACL expires.

## Examples

The following example shows how to extend the absolute timer of the dynamic ACL:

```
! The router is configured with the lock-and-key feature as follows
access-list 132 dynamic tactik timeout 6 permit ip any any
! The absolute timer will extended another six minutes.
access-list dynamic-extend
```

# access-list remark

To write a helpful comment (remark) for an entry in a numbered IP access list, use the **access-list remark** command in global configuration mode.To remove the remark, use the **no** form of this command.

**access-list** *access-list-number* **remark** [*line*]
**no access-list** *access-list-number* **remark** [*line*]

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of an IP access list. |
| *line* | (Optional) Comment that describes the access list entry, up to 100 characters long. |

## Command Default

The access list entries have no remarks.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

## Examples

The following example shows how to write comments for workstation abc, which is allowed access, and workstation xyz, which is not allowed access:

```
access-list 1 remark Permit only abc workstation comment
access-list 1 permit 192.0.2.0
access-list 1 remark Do not allow xyz workstation comment
access-list 1 deny 192.0.2.13
```

## Related Commands

| Command | Description |
|---|---|
| **access-list (IP extended)** | Defines an extended IP access list. |
| **access-list (IP standard)** | Defines a standard IP access list. |
| **ip access-list** | Defines an IP access list by name. |
| **remark** | Writes a helpful comment (remark) for an entry in a named IP access list. |

# access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile** command in privileged EXEC mode.

**access-profile** [**merge** | **replace**] [**ignore-sanity-checks**]

## Syntax Description

| | |
|---|---|
| **merge** | (Optional) Removes existing access control lists (ACLs) while retaining other existing authorization attributes for the interface.<br>• However, using this option installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all attribute-value (AV) pairs defined in the authentication, authorization, and accounting (AAA) per-user configuration (the user's authorization profile). |
| **replace** | (Optional) Removes existing ACLs and all other existing authorization attributes for the interface.<br>• A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration.<br>• This option is not normally recommended because it initially deletes all existing configurations, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information. |
| **ignore-sanity-checks** | (Optional) Enables you to use any AV pairs, whether or not they are valid. |

## Command Default

By default this command removes existing ACLs while retaining other existing authorization attributes for the interface.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRB | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |

## Usage Guidelines

Remote users can use the **access-profile** command to activate double authentication for a PPP session. Double authentication must be correctly configured for this command to have the desired effect.

You should use this command when remote users establish a PPP link to gain local network access.

The resulting authorization attributes of the interface are a combination of the previous and new configurations.

After you have been authenticated with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), you will have limited authorization. To activate double authentication and gain your appropriate user network authorization, you must open a Telnet session to the network access server and execute the **access-profile** command. (This command could also be set up as an autocommand, which would eliminate the need to enter the command manually.)

This command causes all subsequent network authorizations to be made in your username instead of in the remote host's username.

Any changes to the interface caused by this command will stay in effect for as long as the interface stays up. These changes will be removed when the interface goes down. This command does not affect the normal operation of the router or the interface.

The default form of the command, **access-profile**, causes existing ACLs to be unconfigured (removed), and new ACLs to be installed. The new ACLs come from your per-user configuration on an AAA server (such as a TACACS+ server). The ACL replacement constitutes a reauthorization of your network privileges.

The default form of the command can fail if your per-user configuration contains statements other than ACL AV pairs. Any protocols with non-ACL statements will be deconfigured, and no traffic for that protocol can pass over the PPP link.

The **access-profile merge** form of the command causes existing ACLs to be unconfigured and new authorization information (including new ACLs) to be added to the interface. This new authorization information consists of your complete per-user configuration on an AAA server. If any of the new authorization statements conflict with existing statements, the new statements could override the old statements or be ignored, depending on the statement and applicable parser rules. The resulting interface configuration is a combination of the original configuration and the newly installed per-user configuration.



**Caution** The new user authorization profile (per-user configuration) must *not* contain any invalid mandatory AV pairs, because the command will fail and PPP (containing the invalid pair) will be dropped. If invalid AV pairs are included as *optional* in the user profile, the command will succeed, but the invalid AV pair will be ignored. Invalid AV pair types are listed later in this section.

The **access-profile replace** form of the command causes the entire existing authorization configuration to be removed from the interface, and the complete per-user authorization configuration to be added. This per-user authorization consists of your complete per-user configuration on an AAA server.



**Caution** Use extreme caution when using the **access-profile replac**e form of the command. It might have detrimental and unexpected results, because this option deletes all authorization configuration information (including static routes) before reinstalling the new authorization configuration.

The following are invalid AV pair types:

- addr
- addr-pool
- frame-relay

- ip-addresses
- source-ip
- tunnel-id
- x25-addresses
- zonelist

**Note** These AV pair types are invalid only when used with double authentication in the user-specific authorization profile; they cause the **access-profile**command to fail. However, these AV pair types can be appropriate when used in other contexts.

## Examples

The following example shows how to apply the per-user authorization attributes to an interface during a PPP session:

```
Router# access-profile merge ignore-sanity-checks
```

## Related Commands

| Command | Description |
|---|---|
| **connect** | Logs in to a host that supports Telnet, rlogin, or LAT. |
| telnet | Logs in to a host that supports Telnet. |

# access-restrict

To tie a particular Virtual Private Network (VPN) to a specific interface for access to the Cisco IOS gateway and the services it protects, use the **access-restrict** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the VPN, use the **no** form of this command.

**access-restrict interface-name**
**no access-restrict interface-name**

## Syntax Description

| | |
|---|---|
| *interface-name* | Interface to which the VPN should be tied. |

## Command Default

The VPN is not tied to a specific interface.

## Command Modes

ISAKMP group configuration (config-isakmp-group)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

The Access-Restrict attribute ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it provides.

It may be a requirement that particular customers or groups connect to the VPN gateway via a specific interface that uses a particular policy (as applied by the crypto map on that interface). If this specific interface is required, using the **access-restrict** command will result in validation that a VPN connection is connecting only via that interface (and hence, crypto map) to which it is allowed. If a violation is detected, the connection is terminated.

Multiple restricted interfaces may be defined per group. The Access-Restrict attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

You must enable the **crypto isakmp client configuration group command, which specifies group policy information that has to be defined or changed, before enabling the access-restrict command.**



**Note** The Access-Restrict attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.The attribute can override any similar group attributes.

- The Access-Restrict attribute is not required if ISAKMP profiles are implemented. ISAKMP profiles with specific policies per VPN group (as defined via the **match identity group** command, which is a subcommand of the **crypto isakmp profile** command), will achieve the same result.

An example of an attribute-value (AV) pair for the Access-Restrict attribute is as follows:

```
ipsec:access-restrict=<interface-name>
```

## Examples

The following example shows that the VPN is tied to “ethernet 0”:

```
crypto isakmp client configuration group cisco
 access-restrict ethernet 0
```

## Related Commands

| Command | Description |
|---|---|
| **acl** | Configures split tunneling. |
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |

# access-session accounting

To add access-session protocol data to accounting records, use the **access-session accounting** command in global configuration mode. To exclude the access-session protocol data from accounting records use the **no** form of this command.

**access-session accounting attributes** {**filter-list** | **filter-spec**} **list** *list-name*
**no access-session accounting attributes** {**filter-list** | **filter-spec**} **list** *list-name*

## Syntax Description

| | |
|---|---|
| **attributes** | Defines attributes for information accounting. |
| **filter-list** | Configures a sensor protocol filter list. |
| **filter-spec** | Configures a sensor protocol filter specification. |
| **list** *list-name* | Specifies the name of the protocol TLV filter list. |

## Command Default

The access-session protocol data is not added to the accounting records.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)E | This command was introduced prior to this release. |

## Usage Guidelines

Use the **accession-session accounting** command to add access-session protocol data to accounting records and to generate additional accounting events when new sensor data is detected.

The following example shows how to add access-session protocol data to accounting records.

```
Device# configure terminal
Device(config)# access-session accounting attributes filter-list list mylist
Device(config)# access-session accounting attributes filter-spec list mylist
Device(config-filter-list)# end
```

## Related Commands

| | |
|---|---|
| **access-session control-direction** | Sets the direction of authentication control on a port. |
| **access-session host-mode** | Allows hosts to gain access to a controlled port. |
| **access-session port-control** | Sets the authorization state of a port. |

# access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template** command in privileged EXEC mode.

**access-template** {*access-list-numbername*} *template-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostnamesource-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostnamedestination-address*}} [**timeout** *minutes*]

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the dynamic access list. The ranges are from 100 to 199 and from 2000 to 2699. |
| *name* | Name of an IP access list.<br>• The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |
| *template-name* | Name of a dynamic access list. |
| *source-address* | Source address in a dynamic access list.<br>• All other attributes are inherited from the original access-list entry. |
| *source-wildcard-bit* | Source wildcard bits. |
| **any** | Specifies any source hostname. |
| **host** | Specifies a specific source host. |
| *hostname* | Name of the host. |
| *destination-address* | Destination address in a dynamic access list.<br>• All other attributes are inherited from the original access-list entry. |
| *dest-wildcard-bit* | Destination wildcard bits. |
| **timeout** *minutes* | (Optional) Specifies a maximum time limit, in minutes for each entry within this dynamic list. The range is from 1 to 9999.<br>• This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently. |

## Command Default

Temporary access lists are not placed on the router.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You can use the **access-template** to enable the lock-and-key access feature.

You must always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.

## Examples

The following example shows how to enable IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.

```
Router> enable
Router# access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
```

## Related Commands

| Command | Description |
|---|---|
| **access-list (IP extended)** | Defines an extended IP access list. |
| **autocommand** | Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line. |
| **clear access-template** | Clears a temporary access list entry from a dynamic access list manually. |
| **show ip accounting** | Displays the active accounting or checkpointed database or displays access list violations. |

# accounting

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

**accounting** {**arap** | **commands** *level* | **connection** | **exec**} [**default***list-name*]
**no accounting** {**arap** | **commands** *level* | **connection** | **exec**} [**default***list-name*]

## Syntax Description

| | |
|---|---|
| **arap** | Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP). |
| **commands** *level* | Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15. |
| **connection** | Enables both CHAP and PAP, and performs PAP authentication before CHAP. |
| **exec** | Enables accounting for all system-level events not associated with users, such as reloads on the selected lines. |
| **default** | (Optional) The name of the default method list, created with the **aaa accounting**command. |
| *list-name* | (Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command. |

## Command Default

Accounting is disabled.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

## Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

# accounting (gatekeeper)

To enable and define the gatekeeper-specific accounting method, use the **accounting** command in gatekeeper configuration mode. To disable gatekeeper-specific accounting, use the **no**form of this command.

**accounting** {**username h323id** | **vsa**}
**no accounting**

## Syntax Description

| | |
|---|---|
| **username h323id** | Enables H323ID in the user name field of accounting record. |
| **vsa** | Enables the vendor specific attribute accounting format. |

## Command Default

Accounting is disabled.

## Command Modes

Gatekeeper configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(2)NA | This command was introduced. |
| 12.0(3)T | This command was integrated into Cisco IOS Release 12.0(3)T. |
| 12.1(5)XM | The **vsa** keyword was added. |
| 12.2(2)T | The **vsa** keyword was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(2)XB1 | This command was implemented on the Cisco AS5850 universal gateway. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.3(9)T | This **username h323id**keyword was added. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To collect basic start-stop connection accounting data, the gatekeeper must be configured to support gatekeeper-specific H.323 accounting functionality. The **accounting** command enables you to send accounting data to the RADIUS server via IETF RADIUS or VSA attriibutes.

Specify a RADIUS server before using the **accounting** command.

There are three different methods of accounting. The H.323 method sends the call detail record (CDR) to the RADIUS server, the syslog method uses the system logging facility to record the CDRs, and the VSA method collects VSAs.

## Examples

The following example enables the gateway to report user activity to the RADIUS server in the form of connection accounting records:

```
aaa accounting connection start-stop group radius
```

```
gatekeeper
 accounting
```

The following example shows how to enable VSA accounting:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting exec vsa
```

The following example configures H.323 accounting using IETF RADIUS attributes:

```
Router(config-gk)# accounting
username
 h323id
```

The following example configures H.323 accounting using VSA RADIUS attributes:

Router(config-gk)# **accounting vsa**

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| **gatekeeper** | Enters gatekeeper configuration mode. |

# accounting (line)

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

**accounting** {**arap** | **commands** *level* | **connection** | **exec**} [**default***list-name*]
**no accounting** {**arap** | **commands** *level* | **connection** | **exec**} [**default***list-name*]

## Syntax Description

| | |
|---|---|
| **arap** | Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP). |
| **commands** *level* | Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15. |
| **connection** | Enables both CHAP and PAP, and performs PAP authentication before CHAP. |
| **exec** | Enables accounting for all system-level events not associated with users, such as reloads on the selected lines. |
| **default** | (Optional) The name of the default method list, created with the **aaa accounting**command. |
| *list-name* | (Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command. |

## Command Default

Accounting is disabled.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

## Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |

# accounting (server-group)

To specify RADIUS accounting filters for attributes that are to be sent to the RADIUS server in accounting requests, use the **accounting** command in server-group configuration mode. To disable specific RADIUS accounting filters for attributes that are to be sent to the RADIUS server, use the **no** form of this command.

**accounting** {**accept** *list-name* | **reject** *list-name* | **acknowledge broadcast** | **reply** {**accept** *list-name* | **reject** *list-name*} | **request** {**accept** *list-name* | **reject** *list-name*} | **system host-config**}
**no accounting** {**accept** *list-name* | **reject** *list-name* | **acknowledge broadcast** | **reply** {**accept** *list-name* | **reject** *list-name*} | **request** {**accept** *list-name* | **reject** *list-name*} | **system host-config**}

## Syntax Description

| | |
|---|---|
| **accept** | All attributes are rejected except for required attributes and the attributes specified by the list-name argument. |
| reject | All attributes are accepted except for the attributes listed in the specified list-name argument . |
| *list-name* | The name of a specific configured RADIUS attribute list. |
| **acknowledge** | Sends the specified accounting response. |
| broadcast | Specifies broadcast accounting. |
| **reply** | Reply attributes are accepted or rejected as specified by the *list-name* argument. |
| **request** | Request attributes are accepted or rejected as specified by the *list-name* argument. |
| **system** | Enables system accounting generation. |
| **host-config** | Generates system accounting records when private servers are added or deleted. |

## Command Default

If specific attributes are not accepted or rejected, all attributes will be accepted.

## Command Modes

Server-group configuration (config-sg-radius)#

## Command History

| Release | Modification |
|---|---|
| 12.2(1)DX | This command was introduced. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(13)T | Platform support was added for the Cisco 7401ASR. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | The following new keywords were added: **system and host-config** |

## Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS accounting allows users to send only the accounting attributes their business requires, thereby reducing unnecessary traffic and allowing users to customize their own accounting data.

Only one filter may be used for RADIUS accounting per server group.



**Note** The listname must be the same as the listname defined in the **radius-server attribute list**command, which is used with the **attribute**(server-group configuration) command to add to an accept or reject list.

## Examples

The following example shows how to specify accept list "usage-only" for RADIUS accounting:

```
Router> enable
Router# configure terminal
Router(config
)# aaa new-model
Router(config
)# aaa authentication ppp default group radius-sg
Router(config
)# aaa authorization network default group radius-sg
Router(config
)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

The following examples show how Accounting-On records or Accounting-Off records are generated when the **system host-config** keywords are configured using the **accounting** command in server-group configuration mode:

### Accounting-On

In this example, Accounting-On records are generated when private server (server-private 10.10.1.1) is added to a server-group.

```
Router> enable
Router# configure terminal
Router(config
)# aaa new-model
Router(config
)# aaa group server radius g2
Router#(config-sg-radius)# accounting system host-config
Router#(config-sg-radius)# server-private 10.10.1.1
```

```
 --> Debugs when adding a private server.
*May  6 05:23:25.530: RADIUS/ENCODE(00000011):Orig. component type = AAA
*May  6 05:23:25.530: RADIUS(00000011): Config NAS IP: 0.0.0.0
*May  6 05:23:25.530: RADIUS(00000011): sending
*May  6 05:23:25.530: RADIUS/ENCODE: Best Local IP-Address 10.10.55.9 for Radius-Server
10.64.67.15
*May  6 05:23:25.530: RADIUS(00000011): Send Accounting-Request to 10.10.67.15:1646 id
1646/1, len 48
*May  6 05:23:25.530: RADIUS:  authenticator 9A 10 D2 10 10 10 10 9D - 75 EE D4 AF 5D CC
8F 6A
*May  6 05:23:25.530: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*May  6 05:23:25.530: RADIUS:  Acct-Status-Type    [40]  6   Accounting-On            [7]
*May  6 05:23:25.530: RADIUS:  NAS-IP-Address      [4]   6   10.10.55.9
*May  6 05:23:25.530: RADIUS:  Acct-Delay-Time     [41]  6   0
*May  6 05:23:25.550: RADIUS: Received from id 1646/10 10.10.67.15:1646, Accounting-response,
 len 20
*May  6 05:23:25.550: RADIUS: authenticator 10 A1 10 10 1A 3F E5 C9 - D1 D1 D6 92 4D 0A F9
 04
```

### Accounting-Off

In this example, Accounting-Off records are generated when private server (server-private 10.10.10.10) is deleted from a server-group.

```
Router> enable
Router# configure terminal
Router(config
)# aaa new-model
Router(config
)# aaa group server radius g2
Router#(config-sg-radius)# accounting system host-config
Router#(config-sg-radius)# no
 server-private 10.10.10.10
 --> Debugs when a private server is deleted.
*May  6 05:23:34.162: RADIUS/ENCODE(00000011):Orig. component type = AAA
*May  6 05:23:34.162: RADIUS(00000011): Config NAS IP: 0.0.0.0
*May  6 05:23:34.162: RADIUS(00000011): sending
*May  6 05:23:34.166: RADIUS/ENCODE: Best Local IP-Address 10.10.55.9 for Radius-Server
10.64.67.15
*May  6 05:23:34.166: RADIUS(00000011): Send Accounting-Request to 10.10.67.15:1646 id
1646/2, len 48
*May  6 05:23:34.166: RADIUS:  authenticator 0A 1E D6 A9 4C 5A 4B 5B - 2A F4 E1 28 3A CF
87 03
*May  6 05:23:34.166: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*May  6 05:23:34.166: RADIUS:  Acct-Status-Type    [40]  6   Accounting-Off           [8]
*May  6 05:23:34.166: RADIUS:  NAS-IP-Address      [4]   6   10.10.55.9
*May  6 05:23:34.166: RADIUS:  Acct-Delay-Time     [41]  6   0
*May  6 05:23:34.166: RADIUS: Received from id 1646/10 10.10.67.15:1646, Accounting-response,
 len 20
*May  6 05:23:34.166: RADIUS:  authenticator 79 ED 10 55 84 5A 08 8D - 74 03 CE 05 12 A5
DE 75
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict network access to the user. |

| Command | Description |
|---|---|
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **attribute (server-group configuration)** | Adds attributes to an accept or reject list. |
| **authorization (server-group configuration)** | Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server. |
| **radius-server attribute list** | Defines an accept or reject list name. |

# accounting acknowledge broadcast

To define a designated broadcast accounting server group, use the **accounting acknowledge broadcast**command in server group RADIUS configuration mode. To disable the broadcast functionality, use the no form of this command.

**accounting acknowledge broadcast**
**no accounting acknowledge broadcast**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Accounting broadcast functionality is disabled for the RADIUS server group.

## Command Modes

Server group RADIUS configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Examples

The following example enables accounting broadcast functionality on RADIUS server group abcgroup:

```
Router(config)# aaa group server radius abcgroup
Router(config-sg-radius)# accounting acknowledge broadcast
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting update** | Enables periodic interim accounting records to be sent to the accounting server. |
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **gw-accounting aaa** | Enables VoIP gateway accounting through the AAA system. |

# accounting dhcp source-ip aaa list

To enable Per IP Subscriber DHCP Triggered RADIUS Accounting for billing or security purposes, use the **accounting dhcp source-ip aaa list** command in access interface configuration mode. To disable Per IP Subscriber DHCP Triggered RADIUS Accounting, use the **no** form of this command.

**accounting dhcp source-ip aaa list** *method-list-name*
**no accounting**

## Syntax Description

| | |
|---|---|
| *method-list-name* | Character string used to name at least one of the accounting methods, tried in a given sequence. Valid values are **default** or a named method list as defined by the **aaa accounting**command. |

## Command Default

This command is disabled by default. If the **accounting dhcp source-ip aaa list**command for RADIUS accounting is issued without a named method list specified, the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list. If no default method list is defined, then no accounting takes place.

## Command Modes

Access interface

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |

## Usage Guidelines

Enter the **accounting dhcp source-ip aaa list** *command to enable accounting.*Use the **aaa accounting** command to create a named method list.

## Examples

The following example shows how to define a command accounting method list named “default”.

```
accounting dhcp source-ip aaa list default
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |
| **ip dhcp limit lease per interface** | Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface. |

# acl (ISAKMP)

To configure split tunneling, use the **acl** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

**acl** *number*
**no acl** *number*

## Syntax Description

| | |
|---|---|
| *number* | Specifies a group of access control lists (ACLs) that represent protected subnets for split tunneling purposes. |

## Command Default

Split tunneling is not enabled; all data is sent via the Virtual Private Network (VPN) tunnel.

## Command Modes

ISAKMP group configuration (config-isakmp-group)

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **acl** command to specify which groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

You must enable the **crypto isakmp client configuration group command, which specifies group policy information that has to be defined or changed, before enabling the acl command.**

## Examples

The following example shows how to correctly apply split tunneling for the group name “cisco.” In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent via the VPN tunnel.

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp client configuration group** | Specifies the policy profile of the group that will be defined. |

# acl (WebVPN)

To define an access control list (ACL) using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway at the Application Layer level and to associate an ACL with a policy group, use the **acl** command in webvpn context configuration and webvpn group policy configuration modes. To remove the ACL definition, use the **no** form of this command.

**acl** *acl-name*
**no acl** *acl-name*

## Syntax Description

| | |
|---|---|
| *acl-name* | Name of the ACL. |

## Command Default

If a user session has no ACL attributes configured, all application requests are permitted.

## Command Modes

Web context configuration
Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

The ACL can be defined for an individual user or for a policy group.

A defined ACL can be overridden by an individual user when the user logs on to the gateway (using AAA policy attributes).

## Examples

The following example shows that "acl1" has been defined as the ACL and that it has been associated with policy group "default."

```
webvpn context context1
 acl acl1
  permit url "http://www.example.com"
 policy group default
  acl acl1
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Configures a policy group and enters group policy configuration mode. |
| **webvpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# acl drop

To configure an access control list (ACL) drop enforcement action in a Transitory Messaging Services (TMS) Rules Engine configuration, use the **acl drop** command in policy-map class configuration mode. To remove the enforcement action from the Rules Engine configuration, use the **no** form of this command.



**Note** Effective with Cisco IOS Release 12.4(20)T, the **acl drop** command is not available in Cisco IOS software.

**acl drop**
**no acl drop**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(15)XZ | This command was integrated into Cisco IOS Release 12.4(15)XZ. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

The **acl drop** command is entered in a mitigation type policy map. This command configures the TMS Rules Engine to drop packets that match a predefined extended access list. The **ip access-group** command is configured to attach the access list to the interface. The **tms-class** command is configured to associate the interface with the ACL drop enforcement action.

A mitigation service policy (TMS Rules Engine configuration) is configured on a consumer to customize or override a Threat Information Message (TIM) enforcement action sent by the controller. The TMS Rules Engine can be configured to perform an ACL drop, an ignore, or a redirect enforcement action. Only one action can configured for each mitigation type class of traffic.

## Examples

The following example configures an ACL drop enforcement action. Traffic that matches the extended access list (172.16.1/24) is dropped.

```
Router(config)# ip access-list extended 100

Router(config-ipacl)# permit ip 172.16.1.0 0.0.0.255 any
Router(config-ipacl)# exit

Router(config)# interface Ethernet 0/0

Router(config-if)# ip access-group 100 in
Router(config-if)# tms-class
```

```
Router(config-if)# exit
Router(config)# class-map type control mitigation match-all MIT_CLASS_1

Router(config-cmap)# match priority 3

Router(config-cmap)# match primitive block

Router(config-cmap)# exit

Router(config)# policy-map type control mitigation MIT_POL_1
Router(config-pmap)# class MIT_CLASS_1

Router(config-pmap-c)# acl drop

Router(config-pmap-c)# end
```

## Related Commands

| Command | Description |
|---|---|
| **class-map type control mitigation** | Configures a mitigation type class map. |
| ignore (TMS) | Configures the TMS Rules Engine to ignore a mitigation enforcement action. |
| **match primitive** | Configures a primitive match in a mitigation type class map. |
| **match priority** | Configures the match priority level for a mitigation enforcement action. |
| **parameter-map type mitigation** | Configures a mitigation type parameter map. |
| **policy-map type control mitigation** | Configures a mitigation type policy map. |
| **redirect route** | Configures a redirect enforcement action in a mitigation type policy map. |
| **tms-class** | Associates an interface with an ACL drop enforcement action. |
| **variable** | Defines the next-hop variable in a mitigation type parameter map. |

# action-type

To enable the type of action to be performed on accounting records, use the **action-type** command in accounting method list configuration mode. To disable the action for the accounting records, use the **no** form this command.

**action-type** {**none** | **start-stop** | **stop-only**}
**no action-type** {**none** | **start-stop** | **stop-only**}

**Cisco 1000 Series Router**
**action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}
**no action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}

## Syntax Description

| | |
|---|---|
| **none** | Sets the action-type of the accounting records to none. |
| **start-stop** | Sets the start and stop action for the accounting records. |
| **stop-only** | Sets the stop action for the accounting records when service terminates. |
| **periodic** | (Optional) Specifies the periodic accounting action. |
| **disable** | Disables periodic accounting action. |
| **interval** | Sets the periodic accounting interval. |
| *minutes* | Periodic interval, in minutes, for accounting update records. |

## Command Default

If the periodic interval is not specified, information of all periodic accounting records is displayed.

## Command Modes

accounting method list configuration (cfg-acct-mlist)

## Command History

| Release | Modification |
|---|---|
| 15.0 (1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use the **action-type** command to enable the type of action to be performed on accounting records.

## Examples

The following is sample output from the **action-type**command:

```
Router(config)# aaa accounting network default
Router(cfg-acct-mlist)# action-type start-stop periodic interval 1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |

# activate

To activate fail-close mode so that unencrypted traffic cannot pass through a group member before that member is registered with a key server, use the **activate** command in crypto map fail-close configuration mode. To disable fail-close mode, use the **no** form of this command.

**activate**
**no activate**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Fail-close mode is not activated.

## Command Modes

Crypto map fail-close configuration (crypto-map-fail-close)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |
| Cisco IOS XE Release 2.3 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

The **crypto map** command and **gdoi fail-clos**e keywords must precede this command. However, fail-close mode is not activated until the **activate** command is also configured.

## Examples

The following example shows that fail-close mode has been activated, and unencrypted traffic from access list 102 is allowed before the group member is registered:

```
crypto map map1 gdoi fail-close
 match address 102
 activate crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

## Related Commands

| Command | Description |
|---|---|
| show crypto map gdoi fail-close | Displays information about the status of the fail-close mode. |

# add (WebVPN)

To add an ACL entry at a specified position, use the **add** command in webvpn acl configuration mode. To remove an entry from the position specified, use the **no** form of this command.

**add** *position acl-entry*
**no add** *position acl-entry*

## Syntax Description

| | |
|---|---|
| *position* | Position in the entry list to which the ACL rule is to be added. |
| *acl-entry* | Permit or deny command string. |

## Command Default

The ACL entry is appended to the end of the entry list.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Examples

The following example shows that the ACL rule should be added to the third position of the ACL list:

```
webvpn context context1
 acl acl1
  add 3 permit url any
```

## Related Commands

| Command | Description |
|---|---|
| **acl** | Defines an ACL using a SSL VPN gateway at the Application Layer level. |
| **wevpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command inrsa-pubkey configuration mode. To remove the IP address, use the **no** form of this command.

**address** *ip-address*
**no address** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the remote peer. |

## Command Default

No default behavior or values

## Command Modes

Rsa-pubkey configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

## Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **crypto keyring** | Defines a crypto keyring to be used during IKE authentication. |

| Command | Description |
|---|---|
| **key-string** | Specifies the RSA public key of a remote peer. |
| **rsa-pubkey** | Defines the RSA manual key to be used for encryption or signatures during IKE authentication. |

# address (IKEv2 keyring)

To specify an IPv4 or IPv6 address or the range of the peer in an Internet Key Exchange Version 2 (IKEv2) keyring, use the **address** command inIKEv2 keyring peer configuration mode. To remove the IP address, use the **no** form of this command.

**address**
{*ipv4-address*[*mask*] | *ipv6-address prefix*}
**no address**

## Syntax Description

| | |
|---|---|
| *ipv4-address* | IPv4 address of the remote peer. |
| *mask* | (Optional) Subnet mask. |
| *ipv6-address* | IPv6 address of the remote peer. |
| *prefix* | Prefix length |

## Command Default

The IP address is not specified.

## Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| 15.1(4)M | This command was modified. Support was added for IPv6 addresses. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to specify the peer's IP address, which is the IKE endpoint address and independent of the identity address.

## Examples

The following examples show how to specify the preshared key of an IP Security (IPsec) peer:

```
Router(config)# crypto ikev2 keyring keyring1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0
Router(config)# crypto ikev2 keyring keyring2
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# address 2001:DB8:0:ABCD::1/2
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 keyring** | Defines an IKEv2 keyring. |

| Command | Description |
|---|---|
| **description (ikev2 keyring)** | Describes an IKEv2 peer or a peer group for the IKEv2 keyring. |
| **hostname (ikev2 keyring)** | Specifies or modifies the hostname for the network server or peer. |
| **peer** | Defines a peer or a peer group for the keyring. |
| **identity (ikev2 keyring)** | Identifies the peer with IKEv2 types of identity. |
| **pre-shared-key (ikev2 keyring)** | Defines a preshared key for the IKEv2 peer. |

# address ipv4

To configure the IP address of a Diameter peer, use the **address ipv4** command in Diameter peer configuration submode. To disable the configured address, use the **no** form of this command.

**address ipv4** *ip-address*
**no address ipv4** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip address* | The IP address of the host. |

## Command Default

No IP address is configured.

## Command Modes

Diameter peer configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Examples

The following example shows how to configure the IP address of a Diameter peer:

```
Router (config-dia-peer)# address ipv4
 192.0.2.0
```

## Related Commands

| Command | Description |
|---|---|
| **diameter peer** | Defines a Diameter peer and enters Diameter peer configuration mode. |

# address ipv4 (config-radius-server)

To configure the IPv4 address for the RADIUS server accounting and authentication parameters, use the **address ipv4** command in RADIUS server configuration mode. To remove the specified RADIUS server accounting and authentication parameters, use the **no** form of this command.

**address ipv4** {*hostnameipv4address*} [**acct-port** *port* | **alias** {*hostnameipv4address*} | **auth-port** *port* [**acct-port** *port*]]
**no address ipv4** {*hostnameipv4address*} [**acct-port** *port* | **alias** {*hostnameipv4address*} | **auth-port** *port* [**acct-port** *port*]]

## Syntax Description

| | |
|---|---|
| *hostname* | Domain Name System (DNS) name of the RADIUS server host. |
| *ipv4address* | RADIUS server IPv4 address. |
| **acct-port** *port* | (Optional) Specifies the User Datagram Protocol (UDP) port for the RADIUS accounting server for accounting requests. The default port is 1646. |
| **alias** {*hostname* \| *ipv4address*} | (Optional) Specifies an alias for this server. The alias can be an IPv4 address or hostname. Up to eight aliases can be configured for this server. |
| **auth-port** *port* | (Optional) Specifies the UDP port for the RADIUS authentication server. The default port is 1645. |

## Command Default

The RADIUS server accounting and authentication parameters are not configured.

## Command Modes

RADIUS server configuration (config-radius-server)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

The **aaa new-model** command must be configured before issuing this command.

The Cisco TrustSec (CTS) feature uses Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering.

Before an alias can be configured for the RADIUS server, the server's IPv4 address or DNS name must be configured. This is accomplished by using the **address ipv4** command and the *hostname* argument. An alias can then be configured by using the **address ipv4** command, **alias** keyword, and the *hostname* argument.

## Examples

The following example shows how to configure the RADIUS server accounting and authentication parameters:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2 acct-port 1813 auth-port 1812
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **address ipv6** | Configures the IPv6 address for the RADIUS server accounting and authentication parameters. |
| **radius server** | Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode. |

# address ipv6 (config-radius-server)

To configure the IPv6 address for the RADIUS server accounting and authentication parameters, use the **address ipv6** command in RADIUS server configuration mode. To remove the specified RADIUS server accounting and authentication parameters, use the **no** form of this command.

**address ipv6** {*hostnameipv6address*} [**acct-port** *port* | **alias** {*hostnameipv6address*} | **auth-port** *port* [**acct-port** *port*]]
**no address ipv6** {*hostnameipv6address*} [**acct-port** *port* | **alias** {*hostnameipv6address*} | **auth-port** *port* [**acct-port** *port*]]

## Syntax Description

| | |
|---|---|
| *hostname* | Domain Name System (DNS) name of the RADIUS server host. |
| *ipv6address* | RADIUS server IPv6 address. |
| **acct-port** *port* | (Optional) Specifies the User Datagram Protocol (UDP) port for the RADIUS accounting server for accounting requests. The default port is 1646. |
| **alias** {*hostname* \| *ipv6address*} | (Optional) Specifies an alias for this server. The alias can be an IPv6 address or hostname. Up to eight aliases can be configured for this server. |
| **auth-port** *port* | (Optional) Specifies the UDP port for the RADIUS authentication server. The default port is 1645. |

## Command Default

The RADIUS server accounting and authentication parameters are not configured.

## Command Modes

RADIUS server configuration (config-radius-server)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

The **aaa new-model** command must be configured before accessing this command.

The Cisco TrustSec (CTS) feature uses Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering.

Before an alias can be configured for the RADIUS server, the server's IPv6 address or DNS name must be configured. This is accomplished by using the **address ipv6** command and the *hostname* argument. An alias can then be configured by using the **address ipv6** command, the **alias** keyword, and the *hostname* argument.

## Examples

The following example shows how to configure the RADIUS server accounting and authentication parameters:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv6 2001:DB8:1::1 acct-port 1813 auth-port 1812
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **address ipv4** | Configures the IPv4 address for the RADIUS server accounting and authentication parameters. |
| **radius server** | Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode. |

# address ipv4 (GDOI)

To set the source address, which is used as the source for packets originated by the local key server, use the **address ipv4**command in GDOI local server configuration mode. To remove the source address, use the **no** form of this command.

**address ipv4** *ip-address*
**no address ipv4** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | Source address of the local key server. |

## Command Default

A source address is not configured.

## Command Modes

GDOI local server configuration (config-local-server)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |
| Cisco IOS XE Release 2.3 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

When this command is used with unicast rekeys, the address is used as the source of the outgoing rekey message. When this command is used with redundancy, the address is used as the source of the outgoing announcement message. If both unicast rekeying and redundancy are configured, the same address is the source of both types of packets.

If multicast rekeying is configured and the **address ipv4** command is configured, the address (*ip-address)*is the source of the outgoing multicast packet. If multicast is configured but the **address ipv4** command is not configured, the access control list (ACL) specified in the **rekey address ipv4** command identifies the source of the outgoing multicast packet.

## Examples

The following example shows the local server IP address is 10.1.1.0:

```
server local
 rekey algorithm aes 192
 rekey address ipv4 121
 rekey lifetime seconds 300
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa mykeys
 address ipv4 10.1.1.0
 sa ipsec 1
```

## Related Commands

| Command | Description |
|---|---|
| rekey address ipv4 | Sends a rekey to a destination multicast address. |
| **server local** | Designates a device as a GDOI key server and enters GDOI local server configuration mode. |

# address ipv6 (TACACS+)

To configure the IPv6 address of the TACACS+ server, use the **address ipv6** command in TACACS+ server configuration mode. To remove the IPv6 address, use the **no** form of this command.

**address ipv6** *ipv6-address*
**no address ipv6** *ipv6-address*

## Syntax Description

| | |
|---|---|
| ipv6-address | The private TACACS+ server host. |

## Command Default

No TACACS+ server is configured.

## Command Modes

TACACS+ server configuration (config-server-tacacs)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2S | This command was introduced. |

## Usage Guidelines

Use the address ipv6 (TACACS+) command after you have enabled the TACACS+ server using the **tacacs server** command.

## Examples

The following example shows how to specify the IPv6 address on a TACACS+ server named server1:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

## Related Commands

| Command | Description |
|---|---|
| **tacacs server** | Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode. |

# addressed-key

To specify which peer's RSA public key you will manually configure, use the **addressed-key**command in public key chain configuration mode .

**addressed-key** *key-address* [**encryption** | **signature**]

## Syntax Description

| | |
|---|---|
| *key-address* | Specifies the IP address of the remote peer's RSA keys. |
| **encryption** | (Optional) Indicates that the RSA public key to be specified will be an encryption special usage key. |
| **signature** | (Optional) Indicates that the RSA public key to be specified will be a signature special usage key. |

## Command Default

If neither the **encryption** nor **signature** keywords are used, general purpose keys will be specified.

## Command Modes

Public key chain configuration. This command invokes public key configuration mode.

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command or the **named-key** com mand to specify which IP Security peer's RSA public key you will manually configure next.

Follow this command with the **key string** command to specify the key.

If the IPSec remote peer generated general-purpose RSA keys, do not use the **encryption** or **signature** keywords.

If the IPSec remote peer generated special-usage keys, you must manually specify both keys: use this command and the **key-string** command twice and use the **encryption** and **signature** keywords respectively.

## Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key otherpeer.example.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 005C300D 06092A86 4886F70D 01010105
Router(config-pubkey)# 00034B00 30480241 00C5E23B 55D6AB22
Router(config-pubkey)# 04AEF1BA A54028A6 9ACC01C5 129D99E4
Router(config-pubkey)# 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
```

```
Router(config-pubkey)# BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
Router(config-pubkey)# D58AD221 B583D7A4 71020301 0001
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 signature
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key pubkey-chain rsa** | Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices). |
| **key-string (IKE)** | Specifies the RSA public key of a remote peer. |
| **named-key** | Specifies which peer RSA public key you will manually configure. |
| **show crypto key pubkey-chain rsa** | Displays peer RSA public keys stored on your router. |

# administrator authentication list

To authenticate an administrative introducer for a Secure Device Provisioning (SDP) transaction, use the **administrator authentication list** command in tti-registrar configuration mode. To disable administrative introducer authentication, use the **no** form of this command.

**administrator authentication list** *list-name*
**no administrator authentication list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of list. |

## Command Default

All introducers are authenticated as users; their username is used directly to build the device name.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

When you use the **administrator authentication list** command in SDP transactions, the RADIUS or TACACS+ authentication, authorization, and accounting (AAA) server checks for a valid account by looking at the username and password.

The authentication list and the authorization list usually both point to the same AAA list. It is possible that the lists can be on different databases, but it is generally not recommended.

## Examples

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator
 authentication list authen-rad
Router(tti-registrar)# administrator
 authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

## Related Commands

| Command | Description |
|---|---|
| **administrator authorization list** | Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for an administrative introducer in an SDP transaction. |
| **authentication list (tti-registrar)** | Authenticates an introducer in an SDP transaction. |
| authorization list (tti-registrar) | Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction. |

# administrator authorization list

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner for an administrative introducer in a Secure Device Provisioning (SDP) transaction, use the **administrator authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

**administrator authorization list** *list-name*
**no administrator authorization list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of list. |

## Command Default

There is no authorization information requested from the authentication, authorization, and accounting (AAA) server for the administrator.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use the **administrator authorization list** command in SDP transactions, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```



**Note** The existence of a valid AAA username record is enough to pass the authentication check. The cisco-avpair=tti information is necessary only for the authorization check.

If a subject name were received in the authorization response, the registrar stores it in the enrollment database, and that subject name overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered tti:iosconfig values are expanded into the Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.



**Note** The template configuration location may include a variable $n, which is expanded to the name that the administrator enters in the additional SDP dialog.

## Examples

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator
 authentication list authen-rad
Router(tti-registrar)# administrator
 authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

## Related Commands

| Command | Description |
|---|---|
| **administrator authentication list** | Authenticates an administrative introducer for an SDP transaction. |
| **authentication list (tti-registrar)** | Authenticates a user introducer for an SDP transaction. |
| authorization list (tti-registrar) | Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP operation. |

# alert

To enable message logging when events, such as a text-chat, begin, use the **alert** command in the appropriate configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

**alert** {**on** | **off**}
**no alert**

## Syntax Description

| | |
|---|---|
| **on** | Enables message logging for instant messenger application policy events. |
| **off** | Disables message logging for instant messenger application policy events. |

## Command Default

If this command is not configured, the global setting for the **ip inspect alert-off** command will take effect.

## Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Examples

The following example shows to enable audit trail messages for all AOL instant messenger traffic:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im aol
  server deny name login.user1.aol.com
  audit trail on
  alert on
```

## Related Commands

| Command | Description |
|---|---|
| **ip inspect alert-off** | Disables Cisco IOS firewall alert messages. |

# alert (zone-based policy)

To turn on or off console display of Cisco IOS stateful packet inspection alert messages, use the **alert** command in parameter-map type inspect configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

**alert** {**on** | **off**}
**no alert** {**on** | **off**}

## Syntax Description

| | |
|---|---|
| **on** | Alert messages are generated. |
| **off** | Alert messages are not generated. |

## Command Default

Alert messages are not issued.

## Command Modes

Parameter-map type inspect configuration (config-profile)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| Cisco IOS XE Release 3.4S | This command was modified to enable its use only after configuration of the **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, or **parameter-map type inspect global** commands. |

## Usage Guidelines

You can use the **alert** command when you are creating a parameter map.

You must configure the **parameter-map type inspect**, **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, **parameter-map type inspect global**, or **parameter-map type urlfilter** command before you can configure the **alert** command.

You must configure the **alert on** command for the alert messages to be logged. You can configure the **log** command to log the alert messages to either the syslog or the high-speed logger (HSL).

You must configure the **alert on** command for the parameter map for which the alert messages are to be logged. For example, to log zone-related alert messages, you must configure the **alert on** command after you configure the **parameter-map type inspect-zone** command.

## Examples

The following example shows a sample inspect parameter map with the Cisco IOS stateful packet inspection alert messages enabled:

```
Router(config)# parameter-map type inspect insp-params
Router(config-profile)# alert on
```

## Related Commands

| Command | Description |
|---|---|
| **ip inspect alert-off** | Disables the Cisco IOS firewall alert messages. |

| Command | Description |
|---|---|
| **log** | Logs the firewall activity for an inspect parameter map. |
| **parameter-map type inspect** | Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action. |
| **parameter-map type inspect-vrf** | Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode. |
| **parameter-map type inspect-zone** | Configures an inspect zone-type parameter map and enters parameter-map type inspect configuration mode. |
| **parameter-map type inspect global** | Configures a global parameter map and enters parameter-map type inspect configuration mode. |
| **parameter-map type urlfilter** | Creates or modifies a parameter map for URL filtering parameters. |

# alert-severity

To change the alert severity rating for a given signature or signature category, use the **alert-severity** command in signature-definition-action (config-sigdef-action) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

**alert-severity** {**high** | **medium** | **low** | **informational**}
**no alert-severity**

## Syntax Description

| | |
|---|---|
| **high medium** \| **low** \| **informational** | Alert severity action for a given signature or signature category. |

## Command Default

No default behavior or values

## Command Modes

Signature-definition-action configuration (config-sigdef-action)
IPS-category-action configuration (config-ips-category-action)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Before issuing the **alert-severity** command, you must specify either a signature via the **signature** command or a signature category (such as attack-type) via the **category** command.

## Examples

The following example shows how to set the alert severity value to low for signature 5760:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition

Router(config-sigdef)# signature 5726 0

Router(config-sigdef-sig)# alert-severity low

Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11 engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

## Related Commands

| Command | Description |
|---|---|
| category | Specifies a signature category that is to be used for multiple signature actions or conditions. |
| **signature** | Specifies a signature for which the CLI user tunings will be changed. |

# alg sip blacklist

To configure a dynamic Session Initiation Protocol (SIP) application layer gateway (ALG) blocked list for destinations, use the **alg sip blacklist** command in global configuration mode. To remove a blocked list, use the **no** form of this command.

**alg sip blacklist trigger-period** *seconds* **trigger-size** *number-of-events* [**block-time** *block-time*] [**destination** *ipv4-address*]
**no alg sip blacklist trigger-period** *seconds* **trigger-size** *number-of-events* [**block-time** *block-time*] [**destination** *ipv4-address*]

## Syntax Description

| | |
|---|---|
| **trigger-period** *seconds* | Specifies the time period, in seconds, during which events are monitored before a blocked list is triggered. Valid values are from 10 to 60000. |
| **trigger-size** *number-of-events* | Specifies the number of events that are allowed from a source before the blocked list is triggered and all packets from that source are blocked. Valid values are from 1 to 65535. |
| **block-time** *block-time* | (Optional) Specifies the time period, in seconds, when packets from a source are blocked if the configured limit is exceeded. Valid values are from 0 to 2000000. The default is 30. |
| **destination** *ipv4-address* | (Optional) Specifies the destination IP address to be monitored. |

## Command Default

A blocked list is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.11S | This command was introduced. |

## Usage Guidelines

If the configured block time is zero, it means that a blocked list is not configured for the source. If no destination is specified, all destinations are monitored for denial of service (DoS) attacks.

The following events trigger a blocked list:

- In the configured period of time if a source sends multiple requests to a destination and receives non-2xx (as per RFC 3261, any response with a status code between 200 and 299 is a "2xx response") final responses from the destination.
- In the configured period of time if a source sends multiple requests to a destination and does not receive any response from the destination.

## Examples

The following example shows how to configure a blocked list for the destination IP address 10.2.2.23:

```
Device(config)# alg sip blacklist trigger-period 100 trigger-size 10 destination 10.2.2.23
```

**Related Commands**

| | |
|---|---|
| **show alg sip** | Displays all SIP ALG information. |

# alg sip processor

To configure the maximum number of backlog messages that wait for shared processor resources, use the **alg sip processor** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**alg sip processor** {**global** | **session**} **max-backlog** *concurrent-usage*
**no alg sip processor** {**global** | **session**} **max-backlog** *concurrent-usage*

## Syntax Description

| | |
|---|---|
| **global** | Sets the maximum number of backlog messages that are waiting for shared resources for all Session Initiation Protocol (SIP) sessions. The default is 100. |
| **session** | Sets a per session limit for the number of backlog messages waiting for shared resources. The default is 10. |
| **max-backlog** | Specifies the maximum backlog for all sessions or for a single session. |
| *concurrent-usage* | Maximum number of backlog messages waiting for concurrent processor usage. Valid values are from 1 to 200 for the **global** keyword and from 1 to 20 for the **session** keyword. |

## Command Default

Blocked list messages are enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.11S | This command was introduced. |

## Usage Guidelines

Use this command to configure parameters against distributed denial of service (DoS) attacks.

## Examples

The following example shows set the per session limit for the number of backlog messages:

```
Device(config)# alg sip processor session max-backlog 5
```

## Related Commands

| | |
|---|---|
| **show alg sip** | Displays all SIP ALG information. |

# alg sip timer

To configure a timer that the Session Initiation Protocol (SIP) application layer gateway (ALG) uses to manage SIP calls, use the **alg sip timer** command in global configuration mode. To remove the configured timer, use the **no** form of this command.

**alg sip timer** {**call-proceeding-timeout** *call-proceeding-time* | **max-call-duration** *call-duration*}
**no alg sip timer** {**call-proceeding-timeout** *call-proceeding-time* | **max-call-duration** *call-duration*}

## Syntax Description

| | |
|---|---|
| **call-proceeding-timeout** *call-proceeding-time* | Sets the call proceeding time interval, in seconds, for SIP calls that do not receive a response. The range is from 30 to 1800. The default is 180. |
| **max-call-duration** *call-duration* | Sets the maximum call duration, in seconds, for a successful SIP call. The range is from 0 to 65535. The default is 3600. |

## Command Default

A timer is not configured for SIP ALG calls.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.11S | This command was introduced. |

## Usage Guidelines

The timer that you configure with the **alg sip timer call-proceeding-timeout** command is similar to the number of times a phone rings for a call; the SIP ALG releases the SIP call if the call is not connected after the final ring.

When you configure the **alg sip timer max-call-duration** command, all SIP calls whose duration exceeds the configured value is released. The SIP ALG only releases resources that are used by the calls; and the SIP ALG is not torn down.

## Examples

The following example shows how to configure a maximum time interval after which an unsuccessful SIP call is released:

```
Device(config)# alg sip timer call-proceeding-timeout 200
```

The following example shows how to configure a call duration time for a successful SIP call:

```
Device(config)# alg sip timer max-call-duration 180
```

## Related Commands

| | |
|---|---|
| **show alg sip** | Displays all SIP ALG information. |

# algorithm



**Note** Effective with Cisco IOS Release 15.2(4)M, the **algorithm** command is not available in Cisco IOS software.

To specify the algorithm to be used for decrypting the filters, use the **algorithm** command in FPM match encryption filter configuration mode.

**algorithm** *algorithm*

## Syntax Description

| | |
|---|---|
| *algorithm* | The algorithm to be used for decrypting. Currently, aes256cbc is the only algorithm supported. |

## Command Default

No algorithm is specified.

## Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 15.2(4)M | This command was removed from the Cisco IOS software. |

## Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **algorithm** command to specify the algorithm used for decrypting the filters.

## Examples

The following example shows how to specify the algorithm for decrypting the filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# algorithm aes256cbc
```

Router(c-map-match-enc-config)#

## Related Commands

| Command | Description |
|---|---|
| **class-map type** | Creates a class map to be used for matching packets to a specified class. |

| Command | Description |
| --- | --- |
| **match encrypted** | Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode. |



# all profile map configuration through browser-proxy


- all (profile map configuration), on page 252
- allow-mode, on page 253
- appfw policy-name, on page 254
- appl (webvpn), on page 256
- application (application firewall policy), on page 257
- application-inspect, on page 260
- application redundancy, on page 262
- arap authentication, on page 263
- ase collector, on page 265
- ase enable, on page 266
- ase group, on page 267
- ase signature extraction, on page 268
- asymmetric-routing, on page 269
- attribute (server-group), on page 271
- attribute map, on page 273
- attribute nas-port format, on page 274
- attribute type, on page 277
- audit filesize, on page 279
- audit interval, on page 281
- audit-trail, on page 283
- audit-trail (zone), on page 285
- authentication, on page 286
- authentication (IKE policy), on page 288
- authentication (IKEv2 profile), on page 290
- authentication bind-first, on page 294
- authentication command, on page 296
- authentication command bounce-port ignore, on page 298
- authentication command disable-port ignore, on page 299
- authentication compare, on page 300
- authentication control-direction, on page 301
- authentication critical recovery delay, on page 302

- authentication event fail, on page 303
- authentication event no-response action, on page 305
- authentication event server alive action reinitialize, on page 306
- authentication event server dead action authorize, on page 307
- authentication fallback, on page 308
- authentication host-mode, on page 309
- authentication list (tti-registrar), on page 311
- authentication open, on page 313
- authentication order, on page 314
- authentication periodic, on page 315
- authentication port-control, on page 317
- authentication priority, on page 319
- authentication terminal, on page 320
- authentication timer inactivity, on page 321
- authentication timer reauthenticate, on page 322
- authentication timer restart, on page 324
- authentication trustpoint, on page 325
- authentication violation, on page 327
- authentication url, on page 328
- authorization, on page 330
- authorization (server-group), on page 332
- authorization (tti-registrar), on page 334
- authorization address ipv4, on page 336
- authorization identity, on page 337
- authorization list (global), on page 338
- authorization list (tti-registrar), on page 339
- authorization username, on page 341
- authorization username (tti-registrar), on page 343
- authorize accept identity, on page 345
- auth-type, on page 346
- auth-type (ISG), on page 347
- auto-enroll, on page 348
- auto-rollover, on page 350
- auto-update client, on page 353
- automate-tester (config-ldap-server), on page 355
- automate-tester (config-radius-server), on page 356
- auto secure, on page 358
- backoff exponential, on page 360
- backup-gateway, on page 362
- backup group, on page 364
- banner, on page 365
- banner (parameter-map webauth), on page 366
- banner (WebVPN), on page 368
- base-dn, on page 370
- bidirectional, on page 371
- binary file, on page 373

- bind authenticate, on page 375
- block count, on page 377
- browser-attribute import, on page 379
- browser-proxy, on page 380

# all (profile map configuration)

To specify that all authentication and authorization requests be cached, use the **all**command in profile map configuration mode. To disable the caching of all requests, use the **no** form of this command.

**all** [**no-auth**]
**no all**

## Syntax Description

| | |
|---|---|
| **no-auth** | (Optional) Specifies that authentication is bypassed for this user. |

## Command Default

No requests are cached.

## Command Modes

Profile map configuration (config-profile-map)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use the **all** command to cache all authentication and authorization requests.

Use the **all** command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

## Examples

The following example caches all authorization requests in the localusers cache profile group. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# all no-auth
```

## Related Commands

| Command | Description |
|---|---|
| **profile** | Defines or modifies an individual authentication and authorization cache profile based on an exact username match. |
| **regexp** | Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression. |

# allow-mode

To turn the default mode of the filtering algorithm on or off, use the **allow-mode**command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

**allow-mode** {**on** | **off**}
**no allow-mode** {**on** | **off**}

## Syntax Description

| | |
|---|---|
| **on** | Turns on the default mode of the filtering algorithm. The default is on. |
| **off** | Turns off the default mode of the filtering algorithm. |

## Command Default

The filtering algorithm is turned on.

## Command Modes

URL parameter-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **allow-mode**subcommand after you enter the **parameter-map type urlfilter** command.

For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

## Examples

The following example turns on the filtering algorithm:

```
parameter-map type urlfilter eng-filter-profile
 allow-mode on
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type urlfilter** | Creates or modifies a parameter map for URL filtering parameters. |

# appfw policy-name

To define an application firewall policy and put the router in application firewall policy configuration mode, use the **appfw policy-name**command in global configuration mode. To remove a policy from the router configuration, use the **no** form of this command.

**appfw policy-name** *policy-name*
**no appfw policy-name** *policy-name*

## Syntax Description

| | |
|---|---|
| *policy-name* | Name of application policy. |

## Command Default

If this command is not issued, an application firewall policy cannot be created.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

This command puts the router in application firewall policy (appfw-policy-*protocol)*configuration mode, which allows you to begin defining the application firewall policy that will later be applied to the Cisco IOS Firewall via the **ip inspect name** command.

**What Is an Application Firewall Policy?**

The application firewall uses static signatures to detect security violations. A static signature is a collection of parameters that specifies which protocol conditions must be met before an action is taken. (For example, a signature may specify that an HTTP data stream containing the POST method must reset the connection.) These protocol conditions and reactions are defined by the end user via a command-line interface (CLI) to form an application firewall policy (also known as a security policy).

## Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
```

```
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

## Related Commands

| Command | Description |
|---|---|
| **application** | Puts the router in appfw-policy-*protocol*configuration mode and begin configuring inspection parameters for a given protocol. |
| ip inspect name | Defines a set of inspection rules. |

# appl (webvpn)

To configure an application to access a smart tunnel, use the **appl** command in WebVPN smart tunnel configuration mode. To disable an application from accessing the smart tunnel, use the **no** form of this command.

**appl** *display-name appl-name* **windows**
**no appl** *display-name appl-name* **windows**

## Syntax Description

| | |
|---|---|
| *display-name* | Name of the application to be displayed in the smart tunnel application access list on the web browser. |
| *appl-name* | Application name or path. |
| **windows** | Specifies the Windows platform. |

## Command Default

No applications have access to a smart tunnel.

## Command Modes

WebVPN smart tunnel configuration mode (config-webvpn-smart-tunnel)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

## Usage Guidelines

You must configure the correct path and application name to allow the smart tunnel to provide access to applications.

## Examples

The following example shows how to configure applications to access the smart tunnel:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# smart-tunnel list st1
Router(config-webvpn-smart-tunnel)# appl ie ieexplore.exe windows
Router(config-webvpn-smart-tunnel)# appl telnet telnet.exe windows
```

## Related Commands

| Command | Description |
|---|---|
| **smart-tunnel list** | Configures the smart tunnel list and enables it within a policy group. |
| **webvpn context** | Configures the SSL VPN context. |

# application (application firewall policy)

To put the router in appfw-policy-*protocol*configuration mode and begin configuring inspection parameters for a given protocol, use the **application**command in application firewall policy configuration mode. To remove protocol-specific rules, use the **no** form of this command.

**application** *protocol*
**no application** *protocol*

## Syntax Description

| | |
|---|---|
| *protocol* | Protocol-specific traffic will be inspected.<br>One of the following protocols (keywords) can be specified:<br>• **http** (HTTP traffic will be inspected.)<br>• **im** {**aol** \| **yahoo** \| **msn**} (Traffic for the specified instant messenger application will be inspected.) |

## Command Default

You cannot set up protocol-specific inspection parameters.

## Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(4)T | The **im**, **aol yahoo**, and **msn** keywords were introduced to support instant message traffic detection and prohibition. |

## Examples

This command puts the router in appfw-policy-*protocol*configuration mode, where "*protocol*" is dependent upon the specified protocol.

### HTTP-Specific Inspection Commands

After you issue the **application http** command and enter the appfw-policy-http configuration mod e, begin configuring inspection parameters for HTTP traffic by issuing any of the following commands:

- **audit-trail**
- **content-length**
- **content-type-verification**

- **max-header-length**
- **max-uri-length**
- **port-misuse**
- **request-method**
- **strict-http**
- **timeout**
- **transfer-encoding**

### Instant Messenger-Specific Inspection Commands

After you issue the **application im**command and specify an instant messenger application (AOL, Yahoo, or MSN), you can begin configuring inspection parameters for IM traffic by issuing any of the following commands:

- **alert**
- **audit trail**
- **server**
- **service**
- **timeout**

## Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
```

```
!
!
```

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.user1.aol.com
!
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy
interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

## Related Commands

| Command | Description |
|---|---|
| **appfw policy-name** | Defines an application firewall policy and puts the router in application firewall policy configuration mode. |

# application-inspect

To enable Layer 7 application protocol inspection in zone-based policy firewalls, use the **application-inspect** command in parameter-map type inspect configuration mode. To disable Layer 7 inspection, use the **no** form of this command.

**application-inspect** {**all** *protocol-name*}
**no application-inspect** {**all** *protocol-name*}

## Syntax Description

| | |
|---|---|
| **all** | Specifies all supported Layer 7 protocols. |
| *protocol-name* | Name of the protocol to be inspected or not. Valid values for the *protocol-name* argument are the following:<br>• **dns**—Domain Name Server<br>• **exec**—Remote process execution<br>• **ftp**—File Transfer Protocol<br>• **gtp**—GPRS Tunneling Protocol<br>• **h323**—H.323 Protocol<br>• **http**—HTTP<br>• **imap**—Internet Message Access Protocol<br>• **login**—Remote login<br>• **msrpc**—Microsoft Remote Procedure Call<br>• **netbios**—NETBIOS<br>• **pop3**—Post Office Protocol Version 3<br>• **rtsp**—Real Time Streaming Protocol<br>• **shell**—Shell<br>• **sip**—Session Initiation Protocol<br>• **skinny**—Skinny Client Control Protocol<br>• **smtp**—Simple Mail Transfer Protocol<br>• **sunrpc**—SUN Remote Procedure Call<br>• **tftp**—Trivial File Transfer Protocol |

## Command Default

Layer 7 application protocol inspection is enabled.

## Command Modes

Parameter-map type inspect configuration (config-profile)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.11S | This command was introduced. |

## Usage Guidelines

Zone-based policy firewalls supports Layer 7 application protocol inspection along with application layer gateways (ALGs) and application inspection and controls (AICs). Layer 7 application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic that passes through a security module.

Before configuring the **application-inspect** command, you must configure either the **parameter-map type inspect** *parameter-map-name* or the **parameter-map type inspect-global** command.



**Note** You can only configure either the **parameter-map type inspect** *parameter-map-name* or the **parameter-map type inspect-global** command at any time. You cannot configure these command simultaneously.

## Examples

The following example shows how to disable Layer 7 application protocol inspection for FTP in a user-defined parameter map:

```
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# no application-inspect ftp
```

The following example shows how to enable Layer 7 application protocol inspection for all supported protocols at a global firewall level:

```
Device(config)# parameter-map type inspect-global
Device (config-profile)# application-inspect all
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type inspect** | Enables an inspect-type parameter map for the firewall to connect thresholds, timeouts, and other parameters that pertain to the inspect action, and enters parameter-map type inspect configuration mode. |
| **parameter-map type inspect-global** | Enables a global parameter map and enters parameter-map type inspect configuration mode. |

# application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode.

**application redundancy**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Redundancy configuration (config-red)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.1S | This command was introduced. |

## Examples

The following example shows how to enter redundancy application configuration mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)#
```

## Related Commands

| Command | Description |
|---|---|
| **group (firewall)** | Enters redundancy application group configuration mode. |

# arap authentication

To enable authentication, authorization, and accounting (AAA) authentication for AppleTalk Remote Access Protocol (ARAP) on a line, use the **arap authentication** command in line configuration mode. To disable authentication for an ARAP line, use the **no** form of this command.

**Caution** If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARAP will be disabled on this line.

**arap authentication** {**default***list-name*} [**one-time**]
**no arap authentication** {**default***list-name*}

## Syntax Description

| | |
|---|---|
| **default** | Default list created with the **aaa authentication arap** command. |
| *list-name* | Indicated list created with the **aaa authentication arap** command. |
| **one-time** | (Optional) Accepts the username and password in the username field. |

## Command Default

ARAP authentication uses the default set with **aaa authentication arap** command. If no default is set, the local user database is checked.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 11.0 | The **one-time** keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** keyword. Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

## Examples

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARAP line 7:

```
line 7
 arap authentication MIS-access
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa authentication arap** | Enables an AAA authentication method for ARAP using TACACS+. |

# ase collector

**Note** Effective with Cisco IOS Release 12.4(24), the **ase collector** command is not available in Cisco IOS software.

To enter the destination IP address of the Automatic Signature Extraction (ASE) collector server, use the **ase collector** command in global configuration mode. To remove this IP address, use the **no** form of this command.

**ase collector** *ip-address*
**no ase collector** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | Provides IP connectivity between the ASE sensor and ASE collector. |

## Command Default

No ASE collector IP address is specified.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| 12.4(24) | This command was removed. |

## Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

## Examples

The following example shows how to configure an ASE collector IP address:

```
Router(config)# ase collector 10.10.10.3
```

## Related Commands

| Command | Description |
|---|---|
| **ase enable** | Enables the ASE feature on a specified interface. |
| **ase group** | Identifies the TIDP group number for the ASE feature. |
| **ase signature extraction** | Enables the ASE feature globally on the router. |
| **clear ase signature** | Clears ASE signatures that were detected on the router. |
| **debug ase** | Provides error, log, messaging, reporting, status, and timer information. |
| **show ase** | Shows the ASE run-time status, which includes the TIDP group number. |

# ase enable

**Note** Effective with Cisco IOS Release 12.4(24), the **ase enable** command is not available in Cisco IOS software.

To enable the Automatic Signature Extraction (ASE) feature on a specified interface, use the **ase enable** command in interface configuration mode. To disable the ASE feature on a specified interface, use the **no** form of this command.

**ase enable**
**no ase enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The ASE feature is disabled on an interface.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| 12.4(24) | This command was removed. |

## Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

## Examples

The following example shows how to enable the ASE feature on a specified interface:

```
Router(config-if)# ase enable
```

## Related Commands

| Command | Description |
|---|---|
| **ase collector** | Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector. |
| **ase group** | Identifies the TIDP group number for the ASE feature. |
| **ase signature extraction** | Enables the ASE feature globally on the router. |
| **clear ase signature** | Clears ASE signatures that were detected on the router. |
| **debug ase** | Provides error, log, messaging, reporting, status, and timer information. |
| **show ase** | Shows the ASE run-time status, which includes the TIDP group number. |

# ase group

**Note** Effective with Cisco IOS Release 12.4(24), the **ase group** command is not available in Cisco IOS software.

To identify the Threat Information Distribution Protocol (TIDP) group number used for exchange between the Automatic Signature Extraction (ASE) sensor and ASE collector, use the **ase group** command in global configuration mode. To disable this group number, use the **no** form of this command.

**ase group** *TIDP-group-number*
**no ase group** *TIDP-group-number*

## Syntax Description

| | |
|---|---|
| *TIDP-group-number* | TIDP group number for the ASE feature. The range of group numbers is between 1 and 65535. |

## Command Default

No TIDP group number is specified.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| 12.4(24) | This command was removed. |

## Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

## Examples

The following example shows how to configure a TIDP group number for the ASE feature:

```
Router(config)# ase group 10
```

## Related Commands

| Command | Description |
|---|---|
| **ase collector** | Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector. |
| **ase enable** | Enables the ASE feature on a specified interface. |
| **ase signature extraction** | Enables the ASE feature globally on the router. |
| **clear ase signature** | Clears ASE signatures that were detected on the router. |
| **debug ase** | Provides error, log, messaging, reporting, status, and timer information. |
| **show ase** | Shows the ASE run-time status, which includes the TIDP group number. |

# ase signature extraction

**Note** Effective with Cisco IOS Release 12.4(24), the **ase signature extraction**command is not available in Cisco IOS software.

To enable the Automatic Signature Extraction (ASE) feature globally on the router, use the **ase signature extraction**command in global configuration mode. To disable the ASE feature globally on the router, use the **no** form of this command.

**ase signature extraction**
**no ase signature extraction**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The ASE feature is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| 12.4(24) | This command was removed. |

## Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

## Examples

The following example shows how to enable the ASE feature globally on the router:

```
Router(config)# ase signature extraction
```

## Related Commands

| Command | Description |
|---|---|
| **ase collector** | Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector. |
| **ase group** | Identifies the TIDP group number for the ASE feature. |
| **ase enable** | Enables the ASE feature on a specified interface. |
| **clear ase signature** | Clears ASE signatures that were detected on the router. |
| **debug ase** | Provides error, log, messaging, reporting, status, and timer information. |
| **show ase** | Displays the ASE run-time status, which includes the TIDP group number. |

# asymmetric-routing

To set up an asymmetric routing link interface and to enable applications to divert packets received on the standby redundancy group to the active, use the **asymmetric-routing** command in redundancy application group configuration mode. To disable the configuration, use the **no** form of this command.

**asymmetric-routing** {**always-divert enable** | **interface** *type number*}
**no asymmetric-routing** {**always-divert enable** | **interface**}

## Syntax Description

| | |
|---|---|
| **always-divert enable** | Always diverts packets from the standby redundancy group (RG) to the active RG. |
| **interface** *type number* | Specifies the asymmetric routing interface that is used by the RG. |

## Command Default

Asymmetric routing is disabled.

## Command Modes

Redundancy application group configuration (config-red-app-grp)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.5S | This command was introduced. |
| 15.2(3)T | This command was integrated into Cisco IOS Release 15.2(3)T. |

## Usage Guidelines

Asymmetric routing occurs when packets from TCP or UDP connections flow in different directions through different routes. In asymmetric routing, packets that belong to a single connection are forwarded through one router, but return packets of the connection return through another router in the same RG. When you configure the **asymmetric routing always-divert enable** command, the packets received on the standby RG are redirected to the active RG for processing. If the **asymmetric routing always-divert enable** command is disabled, the packets received on the standby RG may be dropped.

When you configure the **asymmetric-routing interface** command, the asymmetric routing feature is enabled. After enabling the feature, configure the **asymmetric-routing always-divert enable** command to enable Network Address Translation (NAT) to divert packets that are received on the standby RG to the active RG.

**Note** The zone-based policy firewall does not support the **asymmetric-routing always-divert enable** command that diverts packets received on the standby RG to the active RG. The firewall forces all packet flows to be diverted to the active RG.

## Examples

The following example shows how to configure asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 2
Router(config-red-app-grp)# asymmetric-routing interface gigabitethernet 0/0/0
Router(config-red-app-grp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **application redundancy** | Configures application redundancy. |
| **group** | Configures a redundancy group. |
| **redundancy** | Enters redundancy configuration mode. |
| **redundancy asymmetric-routing enable** | Establishes an asymmetric flow diversion tunnel for each redundancy group. |

# attribute (server-group)

To add attributes to an accept or reject list, use the **attribute** command in server-group configuration mode. To remove attributes from the list, use the **no** form of this command.

**attribute** *number* [**number** [**number**] . . .]
**no attribute** *number* [**number** [**number**] . . .]

## Syntax Description

| | |
|---|---|
| *number* [*number* [*number* ... | Attributes to include in an accept or reject list. The value can be a single integer, such as 7, or a range of numbers, such as 56-59. At least one attribute value must be specified. |

## Command Default

If this command is not enabled, all attributes are sent to the network access server (NAS).

## Command Modes

Server-group configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(1)DX | This command was introduced. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(13)T | Platform support was added for the Cisco 7401 ASR. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Used in conjunction with the **radius-server attribute list** command (which defines the list name), the **attribute** command can be used to add attributes to an accept or reject list (also known as a filter). Filters are used to prevent the network access server (NAS) from receiving and processing unwanted attributes for authorization or accounting.

The **attribute** command can be used multiple times to add attributes to a filter. However, if a required attribute is specified in a reject list, the NAS will override the command and accept the attribute. Required attributes are as follows:



**Note** The user-password (RADIUS attribute 2) and nas-ip (RADIUS attribute 4) attributes can be filtered together successfully in the access request if they are configured to be filtered. An access request must contain either a user-password or a CHAP password or a state. Also, either a NAS IP address or NAS identifier must be present in a RADIUS accounting request.

- For authorization:
  - 2 (user-password)
  - 6 (Service-Type)
  - 7 (Framed-Protocol)
- For accounting:
  - 4 (NAS-IP-Address)
  - 40 (Acct-Status-Type)
  - 41 (Acct-Delay-Time)
  - 44 (Acct-Session-ID)



**Note** The user will not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose--authorization or accounting. The server will determine whether an attribute is required when it is known what the attribute is to be used for.

## Examples

The following example shows how to add attributes 2, 4, 12, 217, 6-10, 13, 64-69, and 218 to the list name “standard”:

```
radius-server attribute list standard
attribute 2,4,12,217,6-10,13
attribute 64-69,218
```

## Related Commands

| Command | Description |
|---|---|
| **accounting (server-group configuration)** | Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request. |
| **authorization (server-group configuration)** | Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server. |
| **radius-server attribute list** | Defines an accept or reject list name. |

# attribute map

To attach an attribute map to a particular Lightweight Directory Access Protocol (LDAP) server, use the **attribute map**command in LDAP server configuration mode. To remove the attribute maps, use the **no** form of this command.

**attribute map** *map-name*
**no attribute map** *map-name*

## Syntax Description

| | |
|---|---|
| *map-name* | Attribute map name. |

## Command Default

No attribute maps exist for any LDAP servers.

## Command Modes

LDAP server configuration (config-ldap-server)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Usage Guidelines

To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

## Examples

The following example shows how to attach “attribute att_map_1” to the attribute map in LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# attribute map att_map_1
```

## Related Commands

| Command | Description |
|---|---|
| ldap attribute-map | Configures a dynamic LDAP attribute map. |
| map-type | Defines the mapping of a attribute in the LDAP server. |
| show ldap attribute | Displays information about default LDAP attribute mapping. |

# attribute nas-port format

To configure services to use specific named methods for different service types, which can be set to use their own respective RADIUS server groups, use the **attribute nas-port format** command in server-group configuration mode. To remove the override, which is to use specific named methods for different service types, use the **no** form of this command.

**attribute nas-port format** *format-type* [*string*]
**no attribute nas-port format format-type** [*string*]

## Syntax Description

| | |
|---|---|
| *format-type* | Type of format (see the first table below). |
| *string* | (Optional) Pattern of the data format (see the second table below). |

## Command Default

Default format type is used for all services.

## Command Modes

Server-group configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

The following format types may be configured.

***Table 13: Format Types***

| | |
|---|---|
| **a** | Format is type, channel, or port. |
| **b** | Either interface(16), isdn(16), or async(16). |
| **c** | Data format (bits): shelf(2), slot(4), port(5), or channel(5). |
| **d** | Data format (bits): slot(4), module(1), port(3), vpi(8), or vci(16). |
| **e** | Configurable data format (see the table below). |

The following characters may be used in the string pattern of the data format.

***Table 14: Characters Supported by Format-Type e***

| | |
|---|---|
| **0** | Zero |
| **1** | One |
| **f** | DS0 shelf |
| **s** | DS0 slot |

| | |
|---|---|
| **a** | DS0 adapter |
| **P** | DS0 port |
| **i** | DS0 subinterface |
| **c** | DS0 channel |
| **F** | Async shelf |
| **S** | Async slot |
| **P** | Async port |
| **L** | Async line |
| **S** | PPPoX slot (includes PPP over ATM [PPPoA], PPP over Ethernet over ATM [PPPoEoA], PPP over Ethernet over Ethernet [PPPoEoE], PPP over Ethernet over VLAN [PPPoEoVLAN], and PPP over Ethernet over Queue in Queue [PPPoEoQinQ]). |
| **A** | PPPoX adapter |
| **P** | PPPoX port |
| **V** | PPPoX VLAN ID |
| **I** | PPPoX virtual path identifier (VPI) |
| **C** | PPPoX virtual channel indicator (VCI) |
| **U** | Session ID |

## Examples

The following example shows that a leased-line PPP client has chosen to send no RADIUS Attribute 5 while the default is set for format d:

```
interface Serial2/0
 no ip address
 encapsulation ppp
 ppp accounting SerialAccounting
 ppp authentication pap
aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1
aaa group server radius group1
 server 10.101.159.172 auth-port 1645 acct-port 1646
 attribute nas-port none
radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **ip radius source-interface** | Forces RADIUS to use the IP adressing of a specified interface for all outgoing RADIUS packets. |

| Command | Description |
|---|---|
| **radius-server host** | Specifies a RADIUS server host. |

# attribute type

To define an attribute type that is to be added to an attribute list locally on a router, use the **attribute type**command in global configuration mode. To remove the attribute type from the list, use the **no** form of this command.

**attribute type** *name value* [**service** *service*] [**protocol** *protocol*] [*tag*]
**no attribute type** *name value* [**service** *service*] [**protocol** *protocol*] [*tag*]

## Syntax Description

| | |
|---|---|
| *name* | The Cisco IOS authentication, authorization, and accounting (AAA) internal name of the IETF RADIUS attribute to be added to the attribute list. For a list of supported attributes, use the CLI help option (**?**) on your platform. |
| *value* | A string, binary, or IPv4 address value. This is the RADIUS attribute that is being defined in Cisco IOS AAA format. A string added to the attribute value must be inside quotation marks. For example, if the value is “interface-config” and the string is “ip unnumbered FastEthernet0,” you would write interface-config “ip unnumbered FastEthernet0”. |
| **service** *service* | (Optional) Specifies the Access method, which is typically PPP. |
| **protocol** *protocol* | (Optional) Specifies the type of protocol, which can be ATM, IP, or virtual private dialup network (VPDN). |
| *tag* | (Optional) A means of grouping attributes that refer to the same VPDN tunnel. |

## Command Default

An attribute type is not added to the attribute list.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(55)SE | This command was modified in Cisco IOS Release 12.2(55)SE. The following options were added for the *service* argument: **ap-lsc-join** , **ap-mic-join**, **ap-ssc-join**, **lbs-mic-join**, and **lbs-ssc-join**. |

## Usage Guidelines

Attributes are added to the attribute list each time a new attribute type is defined. Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation is applicable to both

RADIUS and TACACS+ AAA servers. Thus, if you are not familiar in configuring a AAA server, Cisco recommends that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

## Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “example.com.” The attribute TEST includes the attribute types interface-config “ip unnumbered FastEthernet0” and interface-config “ip vrf forwarding vrf1.”

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding vrf1" service ppp protocol lcp
!
ip vrf blue
 description vrf vrf1 template1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
subscriber authorization enable
!
subscriber profile example.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile example.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa attribute list** | Defines a AAA attribute list locally on a router. |

# audit filesize

To change the size of the audit file, use the **audit filesize**command in global configuration mode. To return the audit file to its default size, use the **no** form of this command.

**audit filesize** *size*
**no audit filesize** *size*

## Syntax Description

| | |
|---|---|
| *size* | Size of the audit file in KB. Valid values range from 32 KB to 128 KB. 32 KB is the default size. |

## Command Default

The audit file is 32 KB.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)S | This command was introduced. |
| 12.0(27)S | This feature was integrated into Cisco IOS Release 12.0(27)S. |
| 12.2(27)SBC | This commnad was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also referred to as hashes), which monitor changes that have been made to your router. Because the audit file that is stored on the disk is circular, the number of messages that can be stored is dependent on the size of the selected file. Also, the size determines the number of messages that can be stored on the disk before a wrap around occurs.

You should always ensure that the audit file is secure. The audit file should be access protected so that only the audit subsystem can access it.



**Note** Audit logs are enabled by default and cannot be disabled.

## Examples

The following example shows how to change the audit file size to 128 KB:

```
Router(config)# audit filesize 128
```

## Related Commands

| Command | Description |
|---|---|
| **audit interval** | Changes the time interval that is used for calculating hashes. |

| Command | Description |
|---|---|
| **show audit** | Displays contents of the audit file. |

# audit interval

To change the time interval that is used for calculating hashes, use the **audit interval**command in global configuration mode. To return to the default value, which is 5 minutes, use the **no** form of this command.

**audit interval** *seconds*
**no audit interval** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Time interval, in seconds, between hash calculations. Valid values range from 120 seconds to 3600 seconds. The default value is 300 seconds (5 minutes). |

## Command Default

300 seconds (5 minutes)

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)S | This command was introduced. |
| 12.0(27)S | This feature was integrated into Cisco IOS Release 12.0(27)S. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27) SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Hashes are used to monitor changes in your router. A separate hash is maintained for each of the following areas:

- Running version--A hash of the information that is provided in the output of the **show version** command--running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
- Hardware configuration--A hash of platform-specific information that is generally provided in the output of the **show diag**command.
- File system--A hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
- Running configuration--A hash of the running configuration.
- Startup configuration--A hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data files.

By default, the hashes are calculated every 5 minutes to see if any changes (events) have been made to the network. The time interval prevents a large number of hashes from being generated.



**Note** Audit logs are enabled by default and cannot be disabled.

## Examples

The following example shows how to specify hashes to be calculated every 120 seconds (2 minutes):

```
Router(config)# audit interval 120
```

## Related Commands

| Command | Description |
|---|---|
| **audit filesize** | Changes the size of the audit file. |
| **show audit** | Displays contents of the audit file. |

# audit-trail

To enable message logging for established or torn-down connections, use the **audit-trail**command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**audit-trail** {**on** | **off**}
**no audit-trail** {**on** | **off**}

## Syntax Description

| | |
|---|---|
| **on** | Audit trail messages are generated. |
| **off** | Audit trail messages are not generated. |

## Command Default

If this command is not issued, the default value specified via the **ip inspect audit-trail**command will be used.

## Command Modes

cfg-appfw-policy-http
configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(4)T | Support for the inspection of instant messenger applications was introduced. |

## Usage Guidelines

The **audit-trail** command will override the **ip inspect audit-trail** global command.

Before you can issue the **audit-trail**command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol*configuration mode, where "*protocol*" is dependent upon the specified protocol.

## Examples

The following example, which shows how to define the HTTP application firewall policy "mypolicy," enables audit trail messages for the given policy. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  audit trail on
  strict-http action allow alarm
```

```
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

## Related Commands

| Command | Description |
|---|---|
| **ip inspect audit-trail** | Turns on audit trail messages. |

# audit-trail (zone)

To turn audit trail messages on or off, use the **audit-trail** command in parameter-map type inspect configuration mode or URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

**audit trail** {**on** | **off**}
**no audit trail** {**on** | **off**}

## Syntax Description

| | |
|---|---|
| **on** | Audit trail messages will be issued. |
| **off** | Audit trail messages will not be issued. |

## Command Default

There are no audit trail messages.

## Command Modes

Parameter-map type inspect configuration
URL parameter-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

You can use the **audit-trail** subcommand when you are creating a parameter map. For each inspected protocol, you can set the audit trail to **on** or **off**.

When you are configuring an inspect type parameter map, you can enter the **audit-trail**subcommand after you enter the **parameter-map type inspect** command.

When you are creating or modifying a URL parameter map, you can enter the **audit-trail**subcommand after you enter the **parameter-map type urlfilter** command.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** or **parameter-map type urlfilter** command.

## Examples

The following example generates audit trail messages:

```
parameter-map type inspect insp-params
 audit-trail on
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type inspect** | Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action. |
| **parameter-map type urlfilter** | Creates or modifies a parameter map for URL filtering parameters. |

# authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication**command in redundancy application protocol configuration mode. To disable the authentication settings in the redundancy group, use the **no** form of this command.

**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}
**no authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

## Syntax Description

| | |
|---|---|
| **text** *string* | Uses clear text authentication. |
| **md5 key-string** | Uses MD5 key authentication. The *key* argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted. |
| **0** | (Optional) Specifies that the text following immediately is not encrypted. |
| **7** | (Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm. |
| **md5 key-chain** *key-chain-name* | Uses MD5 key-chain authentication. |

## Command Default

The key is not encrypted.

## Command Modes

Redundancy application protocol configuration (config-red-app-prtcl)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.1S | This command was introduced. |

## Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# authentication text name1
```

## Related Commands

| Command | Description |
|---|---|
| **application redundancy** | Enters redundancy application configuration mode. |
| **group** | Enters redundancy application group configuration mode. |
| **name** | Configures the redundancy group with a name. |
| **preempt** | Enables preemption on the redundancy group. |
| **protocol** | Defines a protocol instance in a redundancy group. |

| Command | Description |
| --- | --- |
| **timers hellotime** | Configures timers for hellotime and holdtime messages for a redundancy group. |

# authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange (IKE) policy, use the **authentication** command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the **no** form of this command.

**authentication** {**rsa-sig** | **rsa-encr** | **pre-share** | **ecdsa-sig**}
**no authentication**

## Syntax Description

| | |
|---|---|
| **rsa-sig** | Specifies RSA signatures as the authentication method. This method is not supported in IPv6. |
| **rsa-encr** | Specifies RSA encrypted nonces as the authentication method. This method is not supported in IPv6. |
| **pre-share** | Specifies preshared keys as the authentication method. |
| **ecdsa-sig** | Specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method. |

## Command Default

The RSA signatures authentication method is used.

## Command Modes

ISAKMP policy configuration (config-isakmp)

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |
| 15.1(2)T | This command was modified. The **ecdsa-sig** keyword was added. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the authentication method to be used in an IKE policy.

If you specify RSA signatures, you must configure your peer routers to obtain certificates from a certification authority (CA).

If you specify RSA encrypted nonces, you must ensure that each peer has the other peer's RSA public keys. (See the **crypto key pubkey-chain rsa**, **addressed-key**, **named-key**, **address**, and commands.)

If you specify preshared keys, you must also separately configure these preshared keys. (See the **crypto isakmp identity** and **crypto isakmp key** commands.)

## Examples

The following example configures an IKE policy with preshared keys as the authentication method (all other parameters are set to the defaults):

```
Router(config)#
 crypto isakmp policy 15
Router
(config-isakmp)#
 authentication pre-share
Router
(config-isakmp)#
 exit
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp key** | Configures a preshared authentication key. |
| **crypto isakmp policy** | Defines an IKE policy. |
| **crypto key generate rsa (IKE)** | Generates RSA key pairs. |
| **encryption (IKE policy)** | Specifies the encryption algorithm within an IKE policy. |
| **group (IKE policy)** | Specifies the Diffie-Hellman group identifier within an IKE policy. |
| **hash (IKE policy)** | Specifies the hash algorithm within an IKE policy. |
| **lifetime (IKE policy)** | Specifies the lifetime of an IKE SA. |
| **show crypto isakmp policy** | Displays the parameters for each IKE policy. |

# authentication (IKEv2 profile)

To specify the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile, use the **authentication** command in IKEv2 profile configuration mode. To delete the authentication method, use the **no** form of this command.

**authentication** {**local** {**rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig** | **eap** | [**gtc** | **md5** | **mschapv2** | {**username** *username*} | {**password** *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig**}}
**no authentication** {**local** {**rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig** | **eap** | [**gtc** | **md5** | **mschapv2** | {**username** *username*} | {**password** *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig**}}

## Syntax Description

| | |
|---|---|
| **local** | Specifies the local authentication method. |
| **rsa-sig** | Specifies Rivest, Shamir, and Adelman (RSA) signature as the authentication method. |
| **pre-share** | Specifies preshared key as the authentication method. |
| **key** | Specifies a preshared key. |
| *password* | Specifies a password for preshared key. This argument defines the following values:<br>• **0**—Specifies that the password is unencrypted.<br>• **6**—Specifies that the password is encrypted.<br>• *password*—Specifies an unencrypted user password. |
| **ecdsa-sig** | Specifies Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method. |
| **eap** | Specifies Extensible Authentication Protocol (EAP) as the authentication method. |
| **gtc** | (Optional) Specifies Extensible Authentication Protocol (EAP) as the authentication method using Generic Token Card (GTC) for verifying the credentials. |
| **md5** | (Optional) Specifies Extensible Authentication Protocol (EAP) as the authentication method using Message Digest 5 (MD5) for verifying the credentials. |
| **mschapv2** | (Optional) Specifies Extensible Authentication Protocol (EAP) as the authentication method using Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2) for verifying the credentials. |
| **username** *username* | Specifies the EAP user name. |
| **password** | Specifies the EAP password. |
| **remote** | Specifies the remote authentication method. |
| **query-identity** | (Optional) Queries EAP identity from the peer. |

| | |
|---|---|
| **timeout** *seconds* | (Optional) Specifies the duration, in seconds, to wait for the next IKE_AUTH request after sending the first IKE_AUTH response. The range is from 45 to 180, and the default is 90. |

## Command Default

The default local and remote authentication method is not configured.

## Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| 15.1(2)T | This command was modified. The **ecdsa-sig** keyword was added. |
| 15.1(3)T | This command was modified. The **eap** and **query-identity** keywords were added. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(3)T | This command was modified. The **eap** keyword was added for the local authentication method and the **timeout** *seconds* keyword-argument pair was added for the remote EAP authentication method. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |
| 15.3(3)M | This command was modified. The following keywords and arguments were added:<br>• *password*<br>• **gtc**<br>• **md5**<br>• **mschapv2**<br>• **username** *username*<br>• **username** |

## Usage Guidelines



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the local and remote authentication methods in an IKEv2 profile. You can configure only one local authentication method and multiple remote authentication methods. Multiple remote authentication methods are allowed because the profile caters to multiple peers, and the authentication method that a peer uses is not known. However, each remote authentication method must be specified in a separate command.

If the RSA signature is configured as the local or remote authentication method, you must specify the PKI trustpoints to obtain the signing and verification certificates using the **pki trustpoint** command.

If a preshared key is configured as the local or remote authentication method, you must separately configure the preshared keys and the keyring using the **keyring** command to specify the local and remote keys.

If the **query-identity** keyword is specified, the EAP identity request is sent when the remote peer indicates the intent to use EAP authentication by omitting the Auth payload in the IKE-AUTH request and the local policy allows EAP authentication for the remote peer. The remote EAP identity is used in the following scenarios:

- The EAP identity is used to switch to another IKEv2 profile.
- The remote EAP identity is passed to the RADIUS EAP server as the username for the peer to be authenticated for external EAP.
- The remote EAP identity is used to derive a name for requests using a name mangler.

The **timeout** *seconds* keyword-argument pair is used with the remote EAP authentication method and specifies the duration to obtain EAP credentials on the EAP client.

Extensible Authentication Protocol (EAP) as the local authentication method is supported only on the IKEv2 initiator and EAP as the remote authentication is supported only on the IKEv2 responder. If EAP is specified as the local authentication method, the remote authentication method must be certificate based. If the **authentication remote eap query-identity** command is not configured on the FlexVPN server, the client cannot have an IPv4 or IPv6 address as the local identity because the IP address cannot be used as the username for the EAP authentication method.

## Examples

The following example shows how to specify an authentication method in an IKEv2 profile:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# match identity remote address 192.168.1.1
Device(config-ikev2-profile)# authentication local rsa-sig
Device(config-ikev2-profile)# authentication remote eap query-identity
Device(config-ikev2-profile)# authentication remote rsa-sig
Device(config-ikev2-profile)# identity local email user1@example.com
Device(config-ikev2-profile)# keyring keyring-1
Device(config-ikev2-profile)# pki trustpoint tp-remote verify
```

In the above example, the profile profile1 specifies preshare as the local authentication method and rsa-sig and EAP query identity as the remote authentication methods that use keyring keyring-1 and the trustpoint tp-remote.

The following example shows how to configure an IKEv2 profile for two peers using different authentication methods:

```
Device(config)# crypto ikev2 profile profile2
Device(config-ikev2-profile)# match identity local email user1@example.com
Device(config-ikev2-profile)# match identity remote email user2@example.com
Device(config-ikev2-profile)# authentication local eap
Device(config-ikev2-profile)# authentication remote rsa-sig
```

The above profile caters to two peers, user1@example.com authenticated with EAP and user2@example.com authenticated with preshare.

The following example shows how to configure the EAP as the local authentication method on the IKEv2 initiator:

```
Device(config)# crypto ikev2 profile prof-flex
Device(config-ikev2-profile)# match identity remote address 0.0.0.0
```

```
Device(config-ikev2-profile)# match certificate cmap-1
Device(config-ikev2-profile)# authentication remote rsa-sig
Device(config-ikev2-profile)# authentication local eap
Device(config-ikev2-profile)# keyring local key
Device(config-ikev2-profile)# pki trustpoint ca-server
```

The following example shows how to configure EAP as the remote authentication method on the IKEv2 responder:

```
Device(config)# crypto ikev2 profile prof-flex
Device(config-ikev2-profile)# match identity remote address 0.0.0.0
Device(config-ikev2-profile)# identity local dn
Device(config-ikev2-profile)# authentication remote eap query-identity
Device(config-ikev2-profile)# authentication local rsa-sig
Device(config-ikev2-profile)# keyring local key
Device(config-ikev2-profile)# pki trustpoint ca-server
Device(config-ikev2-profile)# aaa authentication eap rad
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 keyring** | Defines an IKEv2 keyring. |
| **keyring** | Specifies the keyring used with a preshared key authentication method. |
| **pki trustpoint** | Specifies the PKI trustpoints used with the RSA signature authentication method. |
| **show crypto ikev2 profile** | Displays the IKEv2 profile. |

# authentication bind-first

To configure the sequence of the search and bind operations of an authentication request in the Lightweight Directory Access Protocol (LDAP) server, use the **authentication bind-first** command in LDAP server configuration mode. To remove the search and bind configuration, use the **no** form of this command.

**authentication bind-first** [**no-authorization**]
**no authentication bind-first** [**no-authorization**]

## Syntax Description

| | |
|---|---|
| **no-authorization** | (Optional) Specifies that no authorization is required for authentication requests. |

## Command Default

The search operation is performed first, and the bind operation is performed later.

## Command Modes

LDAP server configuration (config-ldap-server)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| 15.2(1)T | This command was modified. The **no-authorization**keyword was added. |

## Usage Guidelines

In an LDAP deployment, the search operation is performed first, and the bind operation is performed later. The search operation is performed first because if the password attribute is returned as part of the search operation, then the password verification can be done locally on the LDAP client and there is no need for the bind operation. If the password attribute is not returned, a bind operation can be performed. Another advantage of performing the search operation first and the bind operation later is that the distinguished name (DN) received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with the base DN.

Use the **no-authorization**keyword to specify whether authorization is required for authentication requests. The **no-authorization** keyword should be used when you do not want to download the user profile from the server.

## Examples

The following example shows how to configure the search and bind operations for an authentication request that does not require authorization:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication bind-first no-authorization
```

The following example shows how to configure the search and bind operations for an authentication request:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication bind-first
```

## Related Commands

| Command | Description |
|---|---|
| **ldap server** | Defines an LDAP server and enters LDAP server configuration mode. |

# authentication command

To specify the HTTP command that is sent to the certification authority (CA) for authentication, use the **authentication command**in ca-profile-enroll configuration mode.

**authentication command** *http-command*

## Syntax Description

| | |
|---|---|
| *http-command* | Defines the HTTP command.<br>**Note**<br>The *http-command* argument is not the HTTP URL. |

## Command Default

No default behavior or values

## Command Modes

Ca-profile-enroll configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)ZH | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

## Usage Guidelines

Use the **authentication command** to send the HTTP request to the CA server for certificate authentication. Before enabling this command, you must use the **authentication url** command.

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

## Examples

The following example shows how to configure certificate authentication via HTTP for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## Related Commands

| Command | Description |
|---|---|
| **authentication url** | Specifies the URL of the CA server to which to send authentication requests. |
| **crypto ca profile enrollment** | Defines an enrollment profile. |

| Command | Description |
| --- | --- |
| **parameter** | Specifies parameters for an enrollment profile. |

# authentication command bounce-port ignore

To configure the router to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the **authentication command bounce-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

**authentication command bounce-port ignore**
**no authentication command bounce-port ignore**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The router accepts a RADIUS CoA bounce port command.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(52)SE | This command was introduced. |
| 12.2(33)SXI4 | This command was integrated into Cisco IOS Release 12.2(33)SXI4. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

A RADIUS CoA bounce port command sent from a RADIUS server can cause a link flap on an authentication port, which triggers Dynamic Host Configuration Protocol (DHCP) renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The **authentication command bounce-port ignore** command configures the router to ignore the RADIUS CoA bounce port command to prevent a link flap from occuring on any hosts that are connected to an authentication port.

## Examples

This example shows how to configure the router to ignore a RADIUS CoA bounce port command:

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

## Related Commands

| Command | Description |
|---|---|
| **authentication command disable-port ignore** | Configures the router to ignore a RADIUS server CoA **disable port** command. |

# authentication command disable-port ignore

To allow the router to ignore a RADIUS server Change of Authorization (CoA) disable port command, use the **authentication command disable-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

**authentication command disable-port ignore**
**no authentication command disable-port ignore**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The router accepts a RADIUS CoA disable port command.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(52)SE | This command was introduced. |
| 12.2(33)SXI4 | This command was integrated into Cisco IOS Release 12.2(33)SXI4. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the **authentication command disable-port ignore** command to configure the router to ignore the RADIUS server CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

## Examples

This example shows how to configure the router to ignore a CoA **disable port** command:

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

## Related Commands

| Command | Description |
|---|---|
| **authentication command bounce-port ignore** | Configures the router to ignore a RADIUS server CoA bounce port command. |

# authentication compare

To replace a bind request with a compare request for an authentication, use the **authentication compare** command in LDAP server configuration mode. To disable the comparison of bind operations for the authentication requests, use the **no** form of this command.

**authentication compare**
**no authentication compare**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Authentication request is performed with bind request.

## Command Modes

LDAP server configuration (config-ldap-server)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Examples

The following example shows how to replace a bind request with a compare request for an authentication:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication compare
```

## Related Commands

| Command | Description |
|---|---|
| **ldap server** | Defines an LDAP server and enters LDAP server configuration mode. |

# authentication control-direction

To set the direction of authentication control on a port, use the **authentication control-direction**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication control-direction** {**both** | **in**}
**no authentication control-direction**

## Syntax Description

| | |
|---|---|
| **both** | Enables bidirectional control on the port. |
| **in** | Enables unidirectional control on the port. |

## Command Default

The port is set to bidirectional mode.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

The IEEE 802.1x standard is implemented to block traffic between the nonauthenticated clients and network resources. This means that nonauthenticated clients cannot communicate with any device on the network except the authenticator. The reverse is true, except for one circumstance--when the port has been configured as a unidirectional controlled port.

### Unidirectional State

The IEEE 802.1x standard defines a unidirectional controlled port, which enables a device on the network to "wake up" a client so that it continues to be reauthenticated. When you use the **authentication control-direction in** command to configure the port as unidirectional, the port changes to the spanning-tree forwarding state, thus allowing a device on the network to wake the client, and force it to reauthenticate.

### Bidirectional State

When you use the **authentication control-direction both** command to configure a port as bidirectional, access to the port is controlled in both directions. In this state, the port does not receive or send packets.

## Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# authentication control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# authentication control-direction both
```

# authentication critical recovery delay

To configure the Auth Manager critical recovery delay, use the **authentication critical recovery delay**command in global configuration mode. To remove a previously configured recovery delay, us the **no** form of this command.

**authentication critical recovery delay** *milliseconds*
**no authentication critical recovery delay**

## Syntax Description

| | |
|---|---|
| *milliseconds* | The period of time, in milliseconds, that the Auth Manager waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000. |

## Command Default

The default delay is 1000 milliseconds.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Examples

The following example shows how to configure the critical recovery delay period to 1500 milliseconds:

```
Switch(config)# authentication critical recovery delay 1500
```

# authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication event fail** [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id* | **next-method**}
**no authentication event fail**

## Syntax Description

| | |
|---|---|
| retry *retry-count* | (Optional) Specifies how many times the authentication method is tried after an initial failure. |
| **action** | Specifies the action to be taken after an authentication failure as a result of incorrect user credentials. |
| **authorize vlan** *vlan-id* | Authorizes a restricted VLAN on a port after a failed authentication attempt. |
| next-method | Specifies that the next authentication method be invoked after a failed authentication attempt. The order of authentication methods is specified by the **authentication order** command. |

## Command Default

Authentication is attempted two times after the initial failed attempt.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

Only the dot1x authentication method can signal this type of authentication failure.

## Examples

The following example specifies that after three failed authentication attempts the port is assigned to a restricted VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event fail retry 3 action authorize vlan 40

Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication event no-response action** | Specifies the action to be taken when authentication fails due to a nonresponsive host. |

| Command | Description |
| --- | --- |
| **authentication order** | Specifies the order in which authentication methods are attempted. |

# authentication event no-response action

To specify how the Auth Manager handles authentication failures as a result of a nonresponsive host, use the **authentication event no-response action** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication event no-response action authorize vlan** *vlan-id*
**no authentication event no-response**

## Syntax Description

| | |
|---|---|
| **authorize vlan** *vlan-id* | Authorizes a restricted VLAN on a port after a failed authentication attempt. |

## Command Default

Authentication fails.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

Use the **authentication event no-response action** command to specify how to handle authentication failures as a result of a nonresponsive host.

## Examples

The following example specifies that when authentication fails as a result of a non-responsive host, the port is assigned to a VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event no-response action authorize vlan 40

Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication event fail** | Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials |

# authentication event server alive action reinitialize

To reinitialize an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting (AAA) server becomes available, use the **authentication event server alive action reinitialize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication event server alive action reinitialize**
**no authentication event server alive action reinitialize**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The session is not reinitialized .

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

Use the **authentication event server alive action reinitialize** command to reinitialize authorized sessions when a previously unreachable AAA server becomes available.

## Examples

The following example specifies that authorized sessions are reinitialized when a previously unreachable AAA server becomes available:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication event server dead action authorize** | Specifies how to handle authorized sessions when the AAA server is unreachable. |

# authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication event server dead action authorize vlan** *vlan-id*
**no authentication event server dead action authorize**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | Authorizes a restricted VLAN on a port after a failed authentication attempt. |

## Command Default

No session is authorized.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

Use the **authentication event server dead action authorize** command to authorize sessions even when the AAA server is unavailable.

## Examples

The following example specifies that when the AAA server becomes unreachable, the port is assigned to a VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server dead action authorize vlan 40

Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication event server alive action reinitialize** | Reinitializes an authorized session when a previously unreachable AAA server becomes available. |

# authentication fallback

To enable a web authentication fallback method, use the **authentication fallback** command in interface configuration mode. To disable web authentication fallback, use the **no** form of this command.

**authentication fallback** *fallback-profile*
**no authentication fallback**

## Syntax Description

| | |
|---|---|
| *fallback-profile* | The name of the fallback profile for web authentication. |

## Command Default

Web authentication fallback is not enabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

Use the **authentication fallback** command to specify the fallback profile for web authentication. Use the **fallback profile** command to specify the details of the profile.

## Examples

The following example shows how to specify a fallback profile on a port:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet1/0/3
Router(config-if)# authentication fallback profile1
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **fallback profile** | Specifies the profile for web authentication. |

# authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication host-mode** {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]
**no authentication host-mode**

## Syntax Description

| | |
|---|---|
| **single-host** | Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected. |
| **multi-auth** | Specifies that multiple clients can be authenticated on the port at any given time. |
| **multi-domain** | Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time. |
| **multi-host** | Specifies that after the first client is authenticated all subsequent clients are allowed access. |
| **open** | (Optional) Specifies that the port is open; that is, there are no access restrictions. |

## Command Default

Access to a port is not allowed.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

Before you use this command, you must use the **authentication port-control** command with the keyword **auto**.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

## Examples

:The following example shows how to enable authentication in **multi-host** mode:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# authentication port-control auto

Switch(config-if)# authentication host-mode multi-host
```

**Related Commands**

| Command | Description |
|---|---|
| **authentication port-control** | Displays information about interfaces. |

# authentication list (tti-registrar)

To authenticate the introducer in an Secure Device Provisioning (SDP) transaction, use the **authentication list**command in tti-registrar configuration mode. To disable the authentication, use the **no** form of this command.

**authentication list** *list-name*
**no authentication list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of the list. |

## Command Default

An introducer is not authenticated.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

This command is used in SDP transactions. When the command is configured, the RADIUS or TACACS+ AAA server checks for a valid account by looking at the username and password.

The authentication list and the authorization list will usually both point to the same AAA list, but it is possible that the lists can be on different databases. This latter scenario is not recommended.

## Examples

The following example shows that an authentication list named “authen-tac” has been configured. In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authorization list** (tti-registrar) | Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an SDP operation. |
| **debug crypto wui** | Displays information about an SDP operation. |
| **template config** | Specifies a remote URL for a Cisco IOS CLI configuration template. |

| Command | Description |
| --- | --- |
| **template username** | Establishes a template username and password to access the configuration template on the file system. |

# authentication open

To enable open access on this port, use the **authentication open** command in interface configuration mode. To disable open access on this port, use the **no** form of this command.

**authentication open**
**no authentication open**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | Support for this command was introduced. |

## Usage Guidelines

Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings by entering the **show authentication** privileged EXEC command.

This command overrides the **authentication host-mode** *session-type* **open** global configuration mode command for the port only.

## Examples

The following example shows how to enable open access to a port:

```
Router(config-if)# authentication open
Router(config-if)#
```

The following example shows how to enable open access to a port:

```
Router(config-if)# no authentication open
Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show authentication** | Displays Authentication Manager information. |

# authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

**authentication order** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
**no authentication order**

## Syntax Description

| | |
|---|---|
| **dot1x** | Specifies IEEE 802.1X authentication. |
| **mab** | Specifies MAC-based authentication(MAB). |
| **webauth** | Specifies web-based authentication. |

## Command Default

The default authentication order is **dot1x**, **mab**, and **webauth**.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

Use the **authentication order** command to specify explicitly which authentication methods are run and the order in which they are run. Each method may be entered only once in the list and no method can be listed after **webauth**.

## Examples

The following example sets the authentication order for a port:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x
Router(config-if)# end
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **authentication priority** | Specifies the priority of authentication methods on a port. |

# authentication periodic

To enable automatic reauthentication on a port, use the **authentication periodic** command in interface configuration or template configuration mode. To disable, use the **no** form of this command.



**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication periodic** command replaces the **dot1x reauthentication** command.

**authentication periodic**
**no authentication periodic**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Reauthentication is disabled.

## Command Modes

Interface configuration (config-if)

Template configuration (config-template)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |
| 15.2(2)E | This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode. |
| Cisco IOS XE Release 3.6E | This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode. |

## Usage Guidelines

Use the **authentication periodic** command to enable automatic reauthentication on a port. To configure the interval between reauthentication attempts, use the **authentication timer reauthenticate** command.

## Examples

The following example shows how to enable reauthentication and sets the interval to 1800 seconds:

```
Device(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface fastethernet0/2
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate 1800
```

The following example shows how to enable reauthentication and sets the interval to 1800 seconds for an interface template:

```
Device# configure terminal
Device(config)# template user-template1
```

```
Device(config-template)# authentication periodic
Device(config-template)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication timer reauthenticate** | Specifies the period of time between attempts to reauthenticate an authorized port. |

# authentication port-control

To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.



**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1x port-control** command.

**authentication port-control** {**auto** | **force-authorized** | **force-unauthorized**}
**no authentication port-control**

## Syntax Description

| | |
|---|---|
| **auto** | Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port. |
| **force-authorized** | Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default. |
| **force-unauthorized** | Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. |

## Command Default

Ports are authorized without authentication exchanges.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

To verify port-control settings, use the **show interfaces** command and check the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

With CSCtr06196, use the **dot1x pae authenticator** command in interface configuration mode to set the Port Access Entity (PAE) type.

## Examples

The following example shows how to specify that the authorization status of the client be determined by the authentication process:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface ethernet0/2
Device(config-if)# authentication port-control auto
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Configures the authorization state of a controlled port. |

# authentication priority

To specify the priority of authentication methods on a port, use the **authentication priority**command in interface configuration mode. To return to the default, use the **no** form of this command.

**authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
**no authentication priority**

## Syntax Description

| | |
|---|---|
| **dot1x** | Specifies IEEE 802.1X authentication. |
| **mab** | Specifies MAC-based authentication. |
| **webauth** | Specifies web-based authentication. |

## Command Default

The default priority order is **dot1x**, **mab**, and **webauth**.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

The **authentication order** command specifies the order in which authentication methods are attempted. This order is the default priority. To override the default priority and allow higher priority methods to interrupt a running authentication method, use the **authentication priority** command.

## Examples

The following example shows the commands used to configure the authentication order and the authentication priority on a port:

```
Router# configure terminal
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x webauth
Router(config-if)# authentication priority dot1x mab
Router(config-if)# end
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **authentication order** | Specifies the order in which the Auth Manager attempts to authenticate a client on a port. |

# authentication terminal

To manually cut-and-paste certificate authentication requests, use the **authentication terminal**command in ca-profile-enroll configuration mode. To delete a current authentication request, use the **no** form of this command.

**authentication terminal**
**no authentication terminal**

## Syntax Description

This command has no arguments or keywords.

## Command Default

An authentication request is not specified.

## Command Modes

Ca-profile-enroll configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)ZH | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

## Usage Guidelines

A user may manually cut-and-paste certificate authentication requests when a network connection between the router and certification authority (CA) is not available. After this command is enabled, the authentication request is printed on the console terminal so that it can be manually copied (cut) by the user.

## Examples

The following example shows how to specify manual certificate authentication and certificate enrollment via HTTP:

```
crypto ca profile enrollment E
 authentication terminal
 enrollment terminal
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca profile enrollment** | Defines an enrollment profile. |

# authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity**command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

**authentication timer inactivity** {*seconds* | **server**}
**no authentication timer inactivity**

## Syntax Description

| | |
|---|---|
| *seconds* | The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535. |
| **server** | Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server. |

## Command Default

The inactivity timer is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

In order to prevent reauthentication of inactive sessions, use the **authentication timer inactivity**command to set the inactivity timer to an interval shorter than the reauthentication interval set with the **authentication timer reauthenticate** command.

## Examples

The following example sets the inactivity interval on a port to 900 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer inactivity 900

Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **configuration timer reauthenticate** | Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port. |
| **authentication timer restart** | Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port. |

# authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration or template configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

**authentication timer reauthenticate** {*seconds* | **server**}
**no authentication timer reauthenticate**

## Syntax Description

| | |
|---|---|
| *seconds* | The number of seconds between reauthentication attempts. The range is from 1 to 65535. The default is 3600. |
| **server** | Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server. |

## Command Default

The automatic reauthentication interval is set to 3600 seconds.

## Command Modes

Interface configuration (config-if)

Template configuration (config-template)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |
| 15.2(2)E | This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode. |
| Cisco IOS XE Release 3.6E | This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode. |

## Usage Guidelines

Use the **authentication timer reauthenticate** command to set the automatic reauthentication interval of an authorized port. If you use the **authentication timer inactivity** command to configure an inactivity interval, configure the reauthentication interval to be longer than the inactivity interval.

## Examples

The following example shows how to set the reauthentication interval on a port to 1800 seconds:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface GigabitEthernet6/0
Device(config-if)# authentication timer reauthenticate 1800
Device(config-if)# end
```

The following example shows how to set the reauthentication interval on a port to 1500 seconds for an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# authentication timer reauthenticate 1500
Device(config-template)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication periodic** | Enables automatic reauthentication. |
| **authentication timer inactivity** | Specifies the interval after which the Auth Manager ends an inactive session. |
| **authentication timer restart** | Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port. |

# authentication timer restart

To specify the period of time after which the Auth Manager attempts to authenticate an unauthorized port, use the **authentication timer restart** command in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

**authentication timer restart**
*seconds*
**no authentication timer restart**

## Syntax Description

| | |
|---|---|
| *seconds* | The number of seconds between attempts to authenticate an unauthorized port. The range is 1 to 65535. The default is 60. |

## Command Default

No attempt is made to authenticate unauthorized ports.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

Use the **authentication timer restart** command to specify the interval between attempts to authenticate an unauthorized port. The default interval is 60 seconds.

## Examples

The following example sets the authentication timer interval to 120 seconds:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet6/0

Router(config-if)# authentication timer restart 120

Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication timer inactivity** | Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port. |
| **configuration timer reauthenticate** | Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port. |

# authentication trustpoint

To specify the trustpoint used to authenticate the Secure Device Provisioning (SDP) petitioner device's existing certificate, use the **authentication trustpoint**command in tti-registrar configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

**authentication trustpoint** {*trustpoint-label* | **use-any**}
**no authentication trustpoint** {*trustpoint-label* | **use-any**}

## Syntax Description

| | |
|---|---|
| *trustpoint-label* | Name of trustpoint. |
| **use-any** | Use any configured trustpoint. |

## Command Default

If this command is not specified, the petitioner-signing certificate is not verified.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Issue the **authentication trustpoint** command in tti-registrar configuration mode to validate the signing certificate that the petitioner used.

## Examples

The following example shows how to specify the trustpoint mytrust for the petitioner-signing certificate:

```
crypto provisioning registrar
 authentication trustpoint mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

## Related Commands

| Command | Description |
|---|---|
| crypto ca trustpoint | Declares the CA that your router should use. |
| **crypto provisioning petitioner** | Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode. |

| Command | Description |
| --- | --- |
| trustpoint signing | Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar for signing the SDP data including the certificate. |

# authentication violation

To specify the action to be taken when a security violation occurs on a port, use the **authentication violation**command in interface configuration mode. To return to the default action, use the **no** form of this command.

**authentication violation** {**restrict** | **shutdown**}
**no authentication violation**

## Syntax Description

| | |
|---|---|
| **restrict** | Specifies that the port restrict traffic with the domain from which the security violation occurs. |
| shutdown | Specifies that the port shuts down upon a security violation. |

## Command Default

Ports are shut down when a security violation occurs.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

## Examples

The following example configures the GigabitEthernet interface to restrict traffic when a security violation occurs:

```
Switch(config)# interface GigabitEthernet6/2

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict

Switch(config-if)# end
```

# authentication url

To specify the URL of the certification authority (CA) server to which to send authentication requests, use the **authentication url** command in ca-profile-enroll configuration mode. To delete the authentication URL from your enrollment profile, use the **no** form of this command.

**authentication url** *url*
**no authentication url** *url*

## Syntax Description

| | |
|---|---|
| *url* | URL of the CA server to which your router should send authentication requests.<br>If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the url argument must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.<br>If you are using TFTP for enrollment, the url argument must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.) |

## Command Default

Your router does not recognize the CA URL until you declare one using this command.

## Command Modes

Ca-profile-enroll configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)ZH | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

## Usage Guidelines

If you do not specify the **authentication command** after you enable the **authentication url** command, the **authentication url** command functions the same as the **enrollment url** *url* command in trustpoint configuration mode. That is, the **authentication url** command will then be used only for certificate enrollment--not authentication.

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

## Examples

The following example shows how to configure an enrollment profile for direct HTTP enrollment with a CA server. In this example, the authentication command is also present.

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
```

```
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

The following example shows how to configure the enrollment profile named "E" to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## Related Commands

| Command | Description |
|---|---|
| **authentication command** | Specifies the HTTP command that is sent to the CA for authentication. |
| **crypto ca profile enrollment** | Defines an enrollment profile. |
| **enrollment** | Specifies the enrollment parameters of your CA. |

# authorization

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line configuration mode. To disable authorization, use the no form of this command.

**authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default***list-name*]
**no authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default***list-name*]

## Syntax Description

| | |
|---|---|
| **arap** | Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol. |
| **commands** | Enables authorization on the selected lines for all commands at the specified privilege level. |
| *level* | Specific command level to be authorized. Valid entries are 0 through 15. |
| **exec** | Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines. |
| **reverse-access** | Enables authorization to determine if the user is allowed reverse access privileges. |
| **default** | (Optional) The name of the default method list, created with the **aaa authorization**command. |
| *list-name* | (Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command. |

## Command Default

Authorization is not enabled.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

## Examples

The following example enables command authorization (for level 15) using the method list named charlie on line 10:

```
line 10
 authorization commands 15 charlie
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization** | Sets parameters that restrict user access to a network. |

# authorization (server-group)

To filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization, use the **authorization**command in server-group configuration mode. To remove the filter on the authorization request or reply, use the **no** form of the command.

**authorization** [**request** | **reply**] [**accept** | **reject**] *list-name*
**no authorization** [**request** | **reply**] [**accept** | **reject**] *list-name*

## Syntax Description

| | |
|---|---|
| **request** | (Optional) Defines filters for outgoing authorization Access Requests. |
| **reply** | (Optional) Defines filters for incoming authorization Accept or Reject packets and for outgoing accounting requests. |
| **accept** | (Optional) Indicates that the required attributes and the attributes specified in the *list-name* argument will be accepted. All other attributes will be rejected. |
| **reject** | (Optional) Indicates that the attributes specified in the list-name will be rejected . All other attributes will be accepted. |
| *list-name* | Defines the given name for the accept or reject list. |

## Command Default

If specific attributes are not accepted or rejected, all attributes will be accepted.

## Command Modes

Server-group configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(1)DX | This command was introduced. |
| 12.2(2)DD | This command was integrated into Cisco IOS Release 12.2(2)DD. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(13)T | Platform support was added for the Cisco 7401ASR. |
| 12.3(3)B | The **request** and **reply** keywords were added. |
| 12.3(7)T | The **request** and **reply** keywords were integrated into Cisco IOS Release 12.3(7)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS authorization allows users to configure the network access server (NAS) to restrict the use of specific attributes, thereby preventing the NAS from processing unwanted attributes.

Only one filter may be used for RADIUS authorization per server group.

**Note** The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute (server-group configuration)**command to add to an accept or reject list.

## Examples

The following example shows how to configure accept list "min-author" in an Access-Accept packet from the RADIUS server:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
 server 10.1.1.1
 authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
 attribute 6-7
```

The following example shows that the attribute "all-attr" will be rejected in all outbound authorization Access Request messages:

```
aaa group server radius ras
 server 192.168.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict network access to the user. |
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **accounting (server-group configuration)** | Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request. |
| **attribute (server-group configuration)** | Adds attributes to an accept or reject list. |
| **radius-server attribute list** | Defines an accept or reject list name. |

# authorization (tti-registrar)

To enable authentication, authorization, and accounting (AAA) authorization for an introducer or a certificate, use the **authorization**command in tti-registrar configuration mode. To disable authorization, use the **no** form of this command.

{**authorization login** | **certificate** | **login certificate**}
{**no authorization login** | **certificate** | **login certificate**}

## Syntax Description

| | |
|---|---|
| **login** | Use the username of the introducer for AAA authorization. |
| **certificate** | Use the certificate of the petitioner for AAA authorization. |
| login certificate | Use the username of the introducer and the certificate of the petitioner for AAA authorization. |

## Command Default

If an authorization list is configured, then authorization is enabled by default.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

This command controls the authorization of the introduction. Authorization can be based on the following:

- The login of the petitioner (username and password) to the registrar
- The current certificate of the petitioner
- Both the login of the introducer and the current certificate of the petitioner

If you issue the **authorization login** command, the introducer logs in with a username and password such as ttiuser and mypassword, which are used against the configured authorization list to contact the AAA server and determine the appropriate authorization.

If you issue the **authorization certificate** command, the certificate of the petitioner is used to build an AAA username, which is used to obtain authorization information.

If you issue the **authorization login certificate** command, authorization for the introducer combines with authorization for the petitioner's current certificate. This means that two AAA authorization lookups occur. In the first lookup, the introducer username is used to retrieve any AAA attributes associated with the introducer. The second lookup is done using the configured certificate name field. If an AAA attribute appears in both lookups, the second one prevails.

## Examples

The following example shows how to specify authorization for both the introducer and the current certificate of the petitioner:

```
crypto provisioning registrar
 authorization login certificate
```

## Related Commands

| Command | Description |
|---|---|
| authorization list (tti-registrar) | Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction. |

# authorization address ipv4

To specify a list of addresses for a Group Domain of Interpretation (GDOI) group, use the **authorization address ipv4** command in GDOI local server configuration mode. To remove an address from the group, use the **no** form of this command.

**authorization address ipv4** {*access-list-name* | *access-list-number*}
**no authorization address ipv4** {*access-list-name* | *access-list number*}

## Syntax Description

| | |
|---|---|
| *access-list-name* | A hostname or distinguished name (DN). |
| *access-list number* | Standard IP access list number. Value: 1 through 99 |

## Command Default

A list of addresses is not specified.

## Command Modes

GDOI local server configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

If the identity of the Internet Key Exchange (IKE) authentication matches an entry in the access control list, the address is authorized.

## Examples

The following example shows that access list number 99 has been specified to be part of a GDOI group:

```
authorization address ipv4 99
```

## Related Commands

| Command | Description |
|---|---|
| **crypto gdoi group** | Identifies a GDOI group and enters GDOI group configuration mode. |
| **server local** | Designates a device as a GDOI key server and enters GDOI local server configuration mode. |

# authorization identity

To specify an authorization identity for a Group Domain of Interpretation (GDOI) group based on a distinguished name (DN) or Fully Qualified Domain Name (FQDN), use the **authorization identity** command in GDOI local server configuration mode. To delete a GDOI group authorization identity, use the **no** form of this command.

**authorization identity** *name*
**no authorization identity** *name*

## Syntax Description

| | |
|---|---|
| *name* | The name of the authorization identity, which can be a DN or FQDN. |

## Command Default

An authorization identity for a GDOI group is not defined.

## Command Modes

GDOI local server configuration (gdoi-local-server)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Cisco Group Encrypted Transport Virtual Private Network (GET VPN) supports GDOI group member (GM) authorization using the authorization identity command when using Public Key Infrastructure (PKI) authentication between the GM and a key server (KS).

An authorization identity for a GDOI group is used to restrict registration of group members within a GDOI group. In order to successfully register with the KS, the DN or FQDN of the group members should match the configured identity string in this command. Use the authorization identity command to configure an authorization identity for a GDOI group.

## Examples

The following example specifies an authorization identity using a DN called GETVPN_FILTER for the GETVPN GDOI group:

```
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# server local
Router(gdoi-local-server)# authorization identity GETVPN_FILTER
Router(gdoi-local-server)# exit
Router(config-gdoi-group)# exit
Router(config)# crypto indentity GETVPN_FILTER
```

## Related Commands

| Command | Description |
|---|---|
| **crypto gdoi group** | Identifies a GDOI group and enters GDOI group configuration mode. |
| crypto identity | Configures the identity of a router with a given list of DNs in the certificate of the router. |
| server local | Designates a device as a GDOI key server and enters GDOI local server configuration mode. |

# authorization list (global)

To specify the authentication, authorization, and accounting (AAA) authorization list, use the **authorization list** command in global configuration mode. To disable the authorization list, use the **no** form of this command.

**authorization list** *list-name*
**no authorization list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of the AAA authorization list. |

## Command Default

An authorization list is not configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(1) | This command was introduced. |

## Usage Guidelines

Use the **authorization list** command to specify a AAA authorization list. For components that do not support specifying the application label, a default label of "any" from the AAA server will provide authorization. Likewise, a label of "none" from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent to a label of "none," but "none" is included for completeness and clarity.)

## Examples

The following example shows that the AAA authorization list "maxaa" is specified:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaa
 authorization username subjectname serialnumber
```

## Related Commands

| Command | Description |
|---|---|
| **authorization username** | Specifies the parameters for the different certificate fields that are used to build the AAA username. |

# authorization list (tti-registrar)

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner in an Secure Device Provisioning (SDP) operation, use the **authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

**authorization list** *list-name*
**no authorization list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of the list. |

## Command Default

There is no authorization list on the AAA server.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

This command is used in SDP operations. When the command is used, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```



**Note** The existence of a valid AAA username record is enough to pass the authentication check. The "cisco-avpair=tti" information is necessary only for the authorization check.

If a subject name was received in the authorization response, the TTI registrar stores it in the enrollment database, and that "subjectname" overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered "tti:iosconfig" values are expanded into the TTI Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.



**Note** The template configuration location may include a variable "$n," which is expanded to the name with which the user is logged in.

## Examples

The following example shows that the authorization list name is "author-rad." In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

## Related Commands

| Command | Description |
|---|---|
| **authentication list (tti-registrar)** | Authenticates the introducer in an SDP operation. |
| **debug crypto wui** | Displays information about an SDP operation. |
| **template config** | Specifies a remote URL for a Cisco IOS CLI configuration template. |
| **template username** | Establishes a template username and password to access the configuration template on the file system. |

# authorization username

To specify the parameters for the different certificate fields that are used to build the authentication, authorization and accounting (AAA) username, use the **authorization username** command in global configuration mode. To disable the parameters, use the **no** form of this command.

**authorization username** {**subjectname** *subjectname*}
**no authorization username** {**subjectname** *subjectname*}

## Syntax Description

| | |
|---|---|
| **subjectname** | AAA username that is generated from the certificate subject name. |
| *subjectname* | Builds the username. The f**ollowing are**options that may be used as the AAA username:<br>• **all** --Entire distinguished name (subject name) of the certificate.<br>• **commonname** --Certificate common name.<br>• **country** --Certificate country.<br>• **email** --Certificate email.<br>• **ipaddress** --Certificate ipaddress.<br>• **locality** --Certificate locality.<br>• **organization** --Certificate organization.<br>• **organizationalunit** --Certificate organizational unit.<br>• **postalcode** --Certificate postal code.<br>• **serialnumber** --Certificate serial number.<br>• **state** --Certificate state field.<br>• **streetaddress** --Certificate street address.<br>• **title** --Certificate title.<br>• **unstructuredname** --Certificate unstructured name. |

## Command Default

Parameters for the certificate fields are not specified.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(1) | This command was introduced. |
| 12.3(11)T | The **all** option for the *subjectname argument*was added. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |

## Examples

The following example shows that the serialnumber option is to be used as the authorization username:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

## Related Commands

| Command | Description |
|---|---|
| **authorization list** | Specifies the AAA authorization list. |

# authorization username (tti-registrar)

To specify the parameters for the different certificate fields that are used to build the authentication, authorization, and accounting (AAA) username, use the **authorization username** command in tti-registrar configuration mode. To disable the parameters, use the **no** form of this command.

**authorization username** {**subjectname** *subjectname*}
**no authorization username** {**subjectname** *subjectname*}

## Syntax Description

| | |
|---|---|
| **subjectname** | AAA username that is generated from the certificate subject name. |
| *subjectname* | Builds the username. The f**ollowing**options can be used as the AAA username:<br>• **all** --Entire distinguished name (subject name) of the certificate<br>• **commonname** --Certificate common name<br>• **country** --Certificate country<br>• **email** --Certificate e-mail<br>• **ipaddress** --Certificate IP address<br>• **locality** --Certificate locality<br>• **organization** --Certificate organization<br>• **organizationalunit** --Certificate organizational unit<br>• **postalcode** --Certificate postal code<br>• **serialnumber** --Certificate serial number<br>• **state** --Certificate state field<br>• **streetaddress** --Certificate street address<br>• **title** --Certificate title<br>• **unstructuredname** --Certificate unstructured name |

## Command Default

Parameters for the certificate fields are not specified.

## Command Modes

tti-registrar configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Examples

The following example shows that the **serialnumber** option is used as the authorization username:

```
aaa authorization network maxaaa group tacac+
```

```
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

## Related Commands

| Command | Description |
|---|---|
| **authorization list** | Specifies the AAA authorization list. |

# authorize accept identity

To configure an identity policy profile, use the **authorize accept identity**command in parameter-map-type consent configuration mode. To remove an identity policy profile, use the **no** form of this command with the configured policy name.

**authorize accept identity** *identity-policy-name*
**no authorize accept identity** *identity-policy-name*

## Syntax Description

| | |
|---|---|
| *identity-policy-name* | Name of an identify profile. |

## Command Default

An identity policy does not exist.

## Command Modes

Parameter-map-type consent (config-profile)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

If an identity policy is not configured, the interface policy will be used.

## Examples

The following example shows how to configure accept policies within the consent-specific parameter maps:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

# auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

**auth-type** {**authorize** | **not-authorize**} **policy** *policy-name*
**no auth-type** {**authorize** | **not-authorize**} **policy** *policy-name*

## Syntax Description

| | |
|---|---|
| **authorize** | Policy is specified for all authorized devices. |
| **not-authorize** | Policy is specified for all unauthorized devices. |
| **policy** *policy-name* | Specifies the name of the identity policy to apply for the associated authentication result. |

## Command Default

A policy is not set for authorized or unauthorized devices.

## Command Modes

Identity profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

## Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit
Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit
Router (config)# identity profile dot1x

Router (config-identity-prof)# auth-type authorize policy grant
```

## Related Commands

| Command | Description |
|---|---|
| **identity policy** | Creates an identity policy. |
| **identity profile dot1x** | Creates an 802.1x identity profile. |

# auth-type (ISG)

To specify the type of authorization Intelligent Services Gateway (ISG) will use for RADIUS clients, use the **auth-type**command in dynamic authorization local server configuration mode. To return to the default authorization type, use the **no** form of this command.

**auth-type** {**all** | **any** | **session-key**}
**no auth-type**

## Syntax Description

| | |
|---|---|
| **all** | All attributes must match for authorization to be successful. This is the default. |
| **any** | Any attribute must match for authorization to be successful. |
| **session-key** | The session-key attribute must match for authorization to be successful.<br>**Note**<br>The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid. |

## Command Default

All attributes must match for authorization to be successful.

## Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |

## Usage Guidelines

An ISG can be configured to allow external policy servers to dynamically send policies to the ISG. This functionality is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer to peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server. Use the **auth-type**command to specify the type of authorization ISG will use for RADIUS clients.

## Examples

The following example configures the ISG authorization type:

```
aaa server radius dynamic-author
 client 10.0.0.1
 auth-type any
```

## Related Commands

| Command | Description |
|---|---|
| **aaa server radius dynamic-author** | Configures an ISG as a AAA server to facilitate interaction with an external policy server. |

# auto-enroll

To enable certificate autoenrollment, use the **auto-enroll** command in ca-trustpoint configuration mode. To disable certificate autoenrollment, use the **no** form of this command.

**auto-enroll** [*percent*] [**regenerate**]
**no auto-enroll** [*percent*] [**regenerate**]

## Syntax Description

| | |
|---|---|
| percent | (Optional) The renewal percentage parameter, causing the router to request a new certificate after the specified percent lifetime of the current certificate is reached. If the percent lifetime is not specified, the request for a new certificate is made when the old certificate expires. The specified percent value must not be less than 10 . If a client certificate is issued for less than the configured validity period due to the impending expiration of the certification authority (CA) certificate, the rollover certificate will be issued for the balance of that period. A minimum of 10 percent of the configured validity period, with an absolute minimum of 3 minutes is required, to allow rollover enough time to function. |
| **regenerate** | (Optional) Generates a new key for the certificate even if the named key already exists. |

## Command Default

Certificate autoenrollment is not enabled.

## Command Modes

Ca-trustpoint configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.3(7)T | The *percent* argument was added to support key rollover. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) was added. |

## Usage Guidelines

Use the auto-enroll command to automatically request a router certificate from the CA that is using the parameters in the configuration. This command will generate a new Rivest, Shamir, and Adelman (RSA) key only if a new key does not exist with the requested label.

A trustpoint that is configured for certificate autoenrollment will attempt to reenroll when the router certificate expires.

Use the **regenerate** keyword to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded

and the new key pair is renamed with the name of the original key pair. Some CAs require a new key for reenrollment to work.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```



**Note** If you are using a Secure Shell (SSH) service, you should set up specific RSA key pairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructure share the same default RSA key pair, a temporary disruption of SSH service could occur. The RSA key pair could become invalid or change because of the CA system, in which case you would not be able to log in using SSH. You could receive the following error message: "key changed, possible security problem.")

## Examples

The following example shows how to configure the router to autoenroll with the CA named "trustme1" on startup. In this example, the **regenerate** keyword is issued, so a new key will be generated for the certificate. The renewal percentage is configured as 90; so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires.

```
crypto ca trustpoint trustme1
 enrollment url http://trustme1.example.com/
 subject-name OU=Spiral Dept., O=example1.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
 password revokeme
 rsakeypair trustme1 2048
 exit
crypto ca authenticate trustme1
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca authenticate** | Retrieves the CA certificate and authenticates it. |
| **crypto ca trustpoint** | Declares the CA that your router should use. |

# auto-rollover

To enable the automated certificate authority (CA) certificate rollover functionality, use the **auto-rollover**command in certificate server mode. To disable the automated rollover functionality, use the **no** form of this command.

**auto-rollover** [*time-period*]
**no auto-rollover**

## Syntax Description

| | |
|---|---|
| *time-period* | (Optional) Indicates when the shadow CA certificate should be generated in absolute time (not a percentage).<br>Default is 30 calendar days before the expiration of the active private key infrastructure (PKI) root certificate. |

## Command Default

Automated CA rollover is not enabled.

## Command Modes

Certificate server configuration (cs-server)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

CAs, like their clients, have certificates with expiration dates that have to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring it must generate a new certificate and possibly a new key pair. This process, called rollover, allows for continuous operation of the network while clients and the certificate server are switching from an expiring CA certificate to a new CA certificate.

The command **auto-rollover** initiates the automatic CA certificate rollover process.

## Examples

The following example shows how to configure automated CA certificate rollover.

```
Router(config)# crypto pki server mycs
Router(cs-server)# auto-rollover 25
Router(cs-server)# no shut
%Some server settings cannot be changed after CA certificate generation.
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
```

```
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
Router(cs-server)#
```

With auto rollover enabled, the show crypto pki server command displays the current configuration of the certificate server.

```
Router# show crypto pki server
Certificate Server mycs:
    Status:enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name:CN=mycs
    CA cert fingerprint:70AFECA9 211CDDCC 6AA9D7FF 3ADB03AE
    Granting mode is:manual
    Last certificate issued serial number:0x1
    CA certificate expiration timer:00:49:26 PDT Jun 20 2008
    CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
    Current storage dir:nvram:
    Database Level:Minimum - no cert data written to storage
    Auto-Rollover configured, overlap period 25 days
    Autorollover timer:00:49:26 PDT May 26 2008....
```

## Related Commands

| Command | Description |
|---|---|
| **auto-rollover** | Enables the automated CA certificate rollover functionality. |
| **cdp-url** | Specifies a CDP to be used in certificates that are issued by the certificate server. |
| **crl (cs-server)** | Specifies the CRL PKI CS. |
| **crypto pki server** | Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials |
| **database archive** | Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file. |
| **database level** | Controls what type of data is stored in the certificate enrollment database. |
| **database url** | Specifies the location where database entries for the CS is stored or published. |
| **database username** | Specifies the requirement of a username or password to be issued when accessing the primary database location. |

| Command | Description |
|---|---|
| **default (cs-server)** | Resets the value of the CS configuration command to its default. |
| **grant auto rollover** | Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA. |
| **grant auto trustpoint** | Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests. |
| **grant none** | Specifies all certificate requests to be rejected. |
| **grant ra-auto** | Specifies that all enrollment requests from an RA be granted automatically. |
| **hash (cs-server)** | Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA. |
| **issuer-name** | Specifies the DN as the CA issuer name for the CS. |
| **lifetime (cs-server)** | Specifies the lifetime of the CA or a certificate. |
| **mode ra** | Enters the PKI server into RA certificate server mode. |
| **mode sub-cs** | Enters the PKI server into sub-certificate server mode |
| **redundancy (cs-server)** | Specifies that the active CS is synchronized to the standby CS. |
| **serial-number (cs-server)** | Specifies whether the router serial number should be included in the certificate request. |
| **show (cs-server)** | Displays the PKI CS configuration. |
| **shutdown (cs-server)** | Allows a CS to be disabled without removing the configuration. |

# auto-update client

To configure automatic update parameters for an Easy VPN remote device, use the **auto-update client** command in global configuration mode. To disable the parameters, use the **no** form of this command.

**auto-update client** *type-of-system* **url** *url* **rev** *review-version*
**no auto-update client** *type-of-system* **url** *url* **rev** *review-version*

## Syntax Description

| | |
|---|---|
| *type-of-system* | Free-format string (see the table below). |
| **url** *url* | URL from which the Easy VPN device obtains the automatic update. |
| **rev** *review-version* | The version number is a comma-delimited string of acceptable versions. |

## Command Default

Automatic updates cannot occur.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

The URL is a generic way to specify the protocol, username, password, address of the server, directory, and filename. The format of a URL is as follows: protocol://username:password@server address:port/directory/filename.

The automatic update on the remote device is triggered only if the current version of the software is earlier than the one specified in the revision string. Otherwise, the automatic update is ignored.

The table below lists possible free-format strings to be used for the type-of-system argument.

***Table 15: Possible Free-format Strings***

| Free-Format String | Operating System |
|---|---|
| Win | Microsoft Windows |
| Win95 | Microsoft Windows 95 |
| Win98 | Microsoft Windows 98 |
| WinNt | Microsoft Windows NT |
| Win2000 | Microsoft Windows 2000 |

| Free-Format String | Operating System |
|---|---|
| Linux | Linux |
| Mac | Macintosh |
| VPN3002 | Cisco VPN 3002 Hardware Client |

## Examples

The following example shows update parameters have been set for a Windows 2000 operating system, a URL of http:www.ourcompanysite.com/newclient, and versions 3.0.1(Rel) and 3.1(Rel):

```
crypto isakmp client configuration group {group-name
}
 auto-update client Win2000 url http:www.ourcompanysite.com/newclient rev 3.0.1(Rel),
3.1(Rel)
```

# automate-tester (config-ldap-server)

To enable automated testing on the Lightweight Directory Access Protocol (LDAP) server, use the **automate-tester** command in LDAP server configuration mode. To disable automated testing, use the **no** form of this command.

**automate-tester username** *user* **probe-on**
**no automate-tester username** *user* **probe-on**

## Syntax Description

| | |
|---|---|
| **username** *user* | Specifies the automatic test username. |
| **probe-on** | Verifies the status of the server by sending a packet. |

## Command Default

Automated testing is disabled by default.

## Command Modes

LDAP server configuration (config-ldap-server)

## Command History

| Release | Modification |
|---|---|
| 15.4(2)T | This command was introduced. |

## Usage Guidelines

The **aaa new-model** command must be configured before issuing the **automate-tester** command.

Use the **automate-tester** command when clients (for example, dot1x) expect the state of the server (DEAD or ALIVE) before any request is sent to the AAA server.

### Example

The following example shows how to enable automatic testing on the LDAP server:

```
Device> enable
Device# configure terminal
Device(config)# username user1 password 0 pwd1
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# deadtime 1
Device(config-ldap-server)# automate-tester username user1 probe-on
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **ldap server** | Specifies the name for the LDAP server configuration and enters LDAP server configuration mode. |

# automate-tester (config-radius-server)

To enable the automated testing feature for the RADIUS server, use the **automate-tester** command in RADIUS server configuration mode. To remove the automated testing feature, use the **no** form of this command.

**automate-tester username** *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*]
**no automate-tester username** *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*]

## Syntax Description

| | |
|---|---|
| **username** *user* | Specifies the automatic test user ID username. |
| **ignore-auth-port** | (Optional) Disables testing on the User Datagram Protocol (UDP) port for the RADIUS authentication server. |
| **ignore-acct-port** | (Optional) Disables testing on the UDP port for the RADIUS accounting server. |
| **idle-time** *minutes* | (Optional) Specifies the time, in minutes, for which the server remains idle before it is quarantined and test packets are sent out. The default value is 60. |

## Command Default

The automated testing feature is disabled for the RADIUS server accounting and authentication UDP ports.

## Command Modes

RADIUS server configuration (config-radius-server)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

The **aaa new-model** command must be configured before issuing this command.

Use the **automate-tester** command to enable automatic testing on the RADIUS server accounting and authentication UDP ports for RADIUS server load balancing.

## Examples

The following example shows how to enable automatic testing on the RADIUS server with the authorization and accounting ports specified with an idle time of 2 hours:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812
Device(config-radius-server)# automate-tester username user1 idle-time 120
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **address ipv4** | Configures the IPv4 address for the RADIUS server accounting and authentication parameters. |
| **address ipv6** | Configures the IPv6 address for the RADIUS server accounting and authentication parameters. |

| Command | Description |
| --- | --- |
| **radius server** | Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode. |

# auto secure

To secure the management and forwarding planes of the router, use the **auto secure** command in privileged EXEC mode.

**auto secure** [**management** | **forwarding**] [**no-interact** | **full**] [**ntp** | **login** | **ssh** | **firewall** | **tcp-intercept**]

## Syntax Description

| | |
|---|---|
| **management** | (Optional) Only the management plane will be secured. |
| **forwarding** | (Optional) Only the forwarding plane will be secured. |
| **no-interact** | (Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter. |
| **full** | (Optional) The user will be prompted for all interactive questions. This is the default. |
| ntp | (Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command line-interface (CLI). |
| login | (Optional) Specifies the configuration of the Login feature in the AutoSecure CLI. |
| ssh | (Optional) Specifies the configuration of the Secure Shell (SSH) feature in the AutoSecure CLI. |
| firewall | (Optional) Specifies the configuration of the firewall feature in the AutoSecure CLI. |
| **tcp-intercept** | (Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI. |

## Command Default

Autosecure is not enabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(1) | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)T. |
| 12.3(4)T | The following keywords were added in Cisco IOS Release 12.3(4)T: **full**, **ntp**, **login**, **ssh**, **firewall**, and **tcp-intercept** |
| 12.3(8)T | Support for the roll-back functionality and system logging messages were added to Cisco IOS Release 12.3(8)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The **auto secure** command allows a user to disable common IP services that can be exploited for network attacks by using a single CLI. This command eliminates the complexity of securing a router both by automating the configuration of security features and by disabling certain features that are enabled by default and that could be exploited for security holes.

**Caution** If you are using Security Device Manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

This command takes you through a semi-interactive session (also known as the AutoSecure dialogue) in which to secure the management and forwarding planes. This command gives you the option to secure just the management or forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

**Caution** If your device is managed by a network management (NM) application, securing the management plane could turn off vital services and disrupt the NM application support.

This command also allows you to go through all noninteractive configuration portions of the dialogue before the interactive portions. The noninteractive portions of the dialogue can be enabled by selecting the optional **no-interact**keyword.

**Roll-back and System Logging Message Support**

In Cisco IOS Release 12.3(8)T, support for roll-back of the AutoSecure configuration is introduced. Roll-back enables a router to revert back to its preautosecure configuration state if the AutoSecure configuration fails.

System Logging Messages capture any changes or tampering of the AutoSecure configuration that were applied on the running configuration.

**Note** Prior to Cisco IOS Release 12.3(8)T, roll-back of the AutoSecure configuration is unavailable; thus, you should always save the running configuration before configuring AutoSecure.

## Examples

The following example shows how to enable AutoSecure to secure only the management plane:

```
Router# auto secure management
```

## Related Commands

| Command | Description |
|---|---|
| ip http server | Enables the HTTP server on your system, including the Cisco web browser user interface. |
| **show auto secure config** | Displays AutoSecure configurations. |

# backoff exponential

To configure the router for exponential backoff retransmit of accounting requests per RADIUS server or server group, enter the **backoff exponential** command in server-group RADIUS configuration mode or RADIUS server configuration mode. To disable this functionality, use the **no** form of this command.

**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits*]
**no backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

## Syntax Description

| | |
|---|---|
| **max-delay** *minutes* | (Optional) Number of retransmissions done in exponential max-delay mode. The max-delay mode indicates that the router starts retransmitting with a minimum time that keeps doubling with each retransmit failure until the maximum configured delay time is reached. The valid range for the *minutes* argument is 1 through 120; if the *minutes* value is not specified, the default value of 60 will be used. |
| **backoff-retry** *retransmits* | (Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. The valid range for the *retransmits* argument is 1 through 50; if the *retransmits* value is not specified, the default value of 5 will be used. |

## Command Default

This command is disabled.

## Command Modes

Server-group RADIUS configuration (config-sg-radius)

RADIUS server configuration (config-radius-server)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)B | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.2(2)T | This command was modified. The RADIUS server configuration (config-radius-server) mode was added to this command. |

## Usage Guidelines

Before enabling the **backoff exponential** command, you must configure one of the following commands:

- The **aaa group server radius** command allows you to specify a server group and enter server-group RADIUS configuration mode.
- The **radius server** command allows you to enter the RADIUS server configuration mode.

The **backoff exponential** command allows you to configure an exponential backoff retransmission per RADIUS server or server group. That is, after the normally configured retransmission retries have been used, the router will keep on trying with an interval that doubles on each retransmit failure until a configured maximum interval is reached. This functionality allows you to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

## Examples

The following example shows how to configure an exponential backoff retransmission in the server-group RADIUS configuration (config-sg-radius) mode:

```
Device(config)# aaa group server radius cat
Device(config-sg-radius)# backoff exponential max-delay 90 backoff-retry 10
```

The following example shows how to configure an exponential backoff retransmission in the RADIUS server configuration (config-radius-server) mode:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2 acct-port 1813 auth-port 1812
Device(config-radius-server)# backoff exponential max-delay 60 backoff-retry 32
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **address ipv4** | Configures the IPv4 address for the RADIUS server accounting and authentication parameters. |
| **radius server** | Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode. |
| **radius-server backoff exponential** | Configures the router for exponential backoff retransmit of accounting requests. |

# backup-gateway

To configure a server to "push down" a list of backup gateways to the client, use the **backup-gateway** command in global configuration mode or IKEv2 authorization policy configuration mode. To remove a backup gateway, use the **no** form of this command.

**backup-gateway** {*ip-addresshostname*}
**no backup-gateway** {*ip-addresshostname*}

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the gateway. |
| *hostname* | Host name of the gateway. |

## Command Default

A list of backup gateways is not configured.

## Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

Before using the **backup-gateway** command, you must first configure the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command.

When using this command with the **crypto ikev2 authorization policy** command to configure a backup gateway, you can configure up to ten backup gateway commands. FlexVPN server pushes the configured backup gateways to the client via Cisco Unity attribute MODECFG_BACKUPSERVERS.

An example of an attribute-value (AV) pair for the backup gateway attribute is as follows:

```
ipsec:ipsec-backup-gateway=10.1.1.1
```

## Examples

The following example shows that gateway 10.1.1.1 has been configured as a backup gateway:

```
crypto isakmp client configuration group group1
 backup-gateway 10.1.1.1
```

The following output example shows that five backup gateways have been configured:

```
crypto isakmp client configuration group sdm
 key 6 RMZPPMRQMSdiZNJg`EBbCWTKSTi\d[
 pool POOL1
 acl 150
```

```
 backup-gateway 172.16.12.12
 backup-gateway 172.16.12.13
 backup-gateway 172.16.12.14
 backup-gateway 172.16.12.130
 backup-gateway 172.16.12.131
 max-users 250
 max-logins 2
```

The following example shows how to configure five backup gateways.

```
crypto ikev2 authorization policy policy1
 backup-gateway gw1
 backup-gateway gw2
 backup-gateway gw3
 backup-gateway 1.1.1.1
 backup-gateway 1.1.1.2
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 authorization policy** | Specifies an IKEv2 authorization policy. |
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |

# backup group

To add a peer to a backup group, use the **backup group** in the IKEv2 FlexVPN client profile configuration mode. To declare a peer as part of no group, use the **no** form of this command.

**backup group** {*group-number* | **default**}
**no backup group**

## Syntax Description

| | |
|---|---|
| *group-number* | Backup group number. |
| **default** | The default group. |

## Command Default

The clients belong to the backup group 0 and are not nvgened.

## Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Release 3.7S | This command was integrated into Cisco IOS XE Release 3.7S. |

## Usage Guidelines

If two peers are in the same backup group, they will try to connect to each of their peer in the same order as described in the backup gateway list. The only difference is that they will refrain from connecting to the same peer at the same moment.

If the peers are not present in the same backup group, they live an independent life and connect to their peers in the order described in backup gateway list but will not look at each other and may end up connecting to the same peer if the configuration authorizes it.

**Note** Any changes to this command terminates the active session.

## Examples

The following example shows how to configure the **backup group** command:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# backup group default
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 client flexvpn** | Defines an IKEv2 FlexVPN client profile. |

# banner

To configure an extended authentication (Xauth) banner string under a group policy definition, use the **banne**r command in global configuration mode. To disable the banner, use the **no** form of this command.

**banner c** *banner-text* **c**
**no c** *banner-text* **c**

## Syntax Description

| | |
|---|---|
| **c** | Delimiting character that must precede and follow the banner text. The delimiting character may be a character of your choice, such as "c" or "@." |
| *banner-text* | Text string of the banner. Maximum number of characters = 1024. |

## Command Default

If a banner is not configured, a banner will not be displayed.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

## Examples

The following example shows that the banner "The quick brown fox jumped over the lazy dog" has been specified:

```
crypto isakmp client configuration group EZVPN
 banner @ The quick brown fox jumped over the lazy dog @
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |

# banner (parameter-map webauth)

To display a banner on the web-authentication login web page, use the **banner** command in parameter map webauth configuration mode. To disable the banner display, use the **no** form of this command.

**banner** [**file** *location*:*filename* | **text** *banner-text*]
**no banner** [**file** *location*:*filename* | **text** *banner-text*]

## Syntax Description

| | |
|---|---|
| **file** *location*:*filename* | (Optional) Specifies a file that contains the banner to display on the web authentication login page. |
| **text** *banner-text* | (Optional) Specifies a text string to use as the banner. You must enter a delimiting character before and after the banner text. The delimiting character can be any character of your choice, such as "c" or "@." |

## Command Default

No banner displays on the web-authentication login web page.

## Command Modes

Parameter map webauth configuration (config-params-parameter-map)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2SE | This command was introduced. |

## Usage Guidelines

The **banner** command allows you to configure one of three possible scenarios:

- The **banner** command without any keyword or argument—Displays the default banner using the name of the device: "Cisco Systems, <device's hostname> Authentication."
- The **banner** command with the **file** *filename* keyword-argument pair—Displays the banner from the custom HTML file you supply. The custom HTML file must be stored in the disk or flash of the device.
- The **banner** command with the **text** *banner-text* keyword-argument pair—Displays the text that you supply. The text must include any required HTML tags.

**Note** If the **banner** command is not enabled, nothing displays on the login page except text boxes for entering the username and password.

## Examples

The following example shows that a file in flash named webauth_banner.html is specified for the banner:

```
parameter-map type webauth MAP_1
 type webauth
 banner file flash:webauth_banner.html
```

The following example shows how to configure the message "login page banner" by using "c" as the delimiting character, and it shows the resulting configuration output.

```
Device(config-params-parameter-map)# banner text c login page banner c
```

```
parameter-map type webauth MAP_2
 type webauth
 banner text ^c login page banner ^c
```



**Note** The caret symbol (^) displays in the configuration output before the delimiting character that you entered even though you do not enter it.

## Related Commands

| Command | Description |
|---|---|
| **consent email** | Requests a user's e-mail address on the web-authentication login web page. |
| **redirect** (parameter-map webauth) | Redirects users to a particular URL during web-based authentication. |
| **show ip admission status banner** | Displays information about configured banners for web authentication. |

# banner (WebVPN)

To configure a banner to be displayed after a successful login, use the **banner** command in webvpn group policy configuration mode or IKEv2 authorization policy configuration mode. To remove the banner, use the **no** form of this command.

**banner** *string*
**no banner**

## Syntax Description

| | |
|---|---|
| *string* | Text string that contains 7-bit ASCII values and HTML tags and escape sequences. The text banner must be in quotation marks if it contains spaces. |

## Command Default

A banner is not configured.

## Command Modes

Webvpn group policy configuration (config-webvpn-group)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Before using this command, you must first configure the **crypto ikev2 authorization policy** command.

When using this command with the **crypto ikev2 authorization policy** command, the format of the banner text shoule be 'c banner-text c', where 'c' is a delimiting character. Any character can be used as a delimiting character. The banner text can have spaces, special characters and can span multiple lines. FlexVPN server pushes the banner to the client via Cisco Unity attribute MODECFG_BANNER.

## Examples

The following example configures “Login Successful” to be displayed after login:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner “Login Successful”
Router(config-webvpn-group)#
```

This example shows how to display banner text that has spaces, spans multiple lines and is delimited by character 'z'

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-author-policy)# banner z
Enter TEXT message. End with the character 'z'.
This is banner text
z
Router# show run | beg policy2
crypto ikev2 authorization policy policy2
banner ^C
This
is
banner text
```

```
^C
!
Router# sh cry ikev2 authorization policy policy2
IKEv2 Authorization Policy : policy2
Banner :
This
is
banner text
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# base-dn

To configure a base distinguished name (DN) that you want to use to perform search operations in the Lightweight Directory Access Protocol (LDAP) server directory tree, use the **base-dn** command in LDAP server configuration mode. To delete a configured base DN for the LDAP server, use the **no** form of this command.

**base-dn** *string*
**no base-dn** *string*

## Syntax Description

| | |
|---|---|
| *string* | Distinguished name of the search base. |

## Command Default

No distinguished names are created.

## Command Modes

LDAP server configuration (config-ldap-server)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Usage Guidelines

This command is valid only for LDAP servers. A base DN can take a form such as dc=example,dc=domain, where the base DN uses the Domain Name Server (DNS) domain name as its basis and is split into the domain components.

## Examples

The following example shows how to configure the base DN for an LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"
```

## Related Commands

| Command | Description |
|---|---|
| **ipv4** (l**dap)** | Creates an IPv4 address within an LDAP server address pool. |
| **ldap server** | Defines an LDAP server and enters LDAP server configuration mode. |
| **transport port** (**ldap)** | Configures the transport protocol for establishing a connection with the LDAP server. |

# bidirectional

To enable incoming and outgoing IP traffic to be exported across a monitored interface, use the **bidirectional** command in router IP traffic export (RITE) configuration mode. To return to the default functionality, use the **no** form of this command.

**bidirectional**
**no bidirectional**

## Syntax Description

This command has no arguments or keywords.

## Command Default

If this command is not enabled, only incoming traffic is exported.

## Command Modes

RITE configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

## Usage Guidelines

By default, only incoming IP traffic is exported. If you choose to export outgoing IP traffic, you must issue both the **bidirectional** command, which enables outgoing traffic to be exported, and the **outgoing** command, which specifies how the outgoing traffic will be filtered.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

## Examples

The following example shows how to export both incoming and outgoing IP traffic on the FastEthernet interface:

```
Router(config)# ip traffic-export profile johndoe
Router(config-rite)# interface FastEthernet1/0.1
Router(config-rite)# bidirectional

Router(config-rite)# incoming access-list 101

Router(config-rite)# outgoing access-list 101

Router(config-rite)# mac-address 6666.6666.3333
```

## Related Commands

| Command | Description |
|---|---|
| **interface (RITE)** | Specifies the outgoing interface for exporting traffic. |

| Command | Description |
|---|---|
| **ip traffic-export profile** | Creates or edits an IP traffic export profile and enables the profile on an ingress interface. |
| **outgoing** | Configures filtering for outgoing export traffic. |

# binary file

To specify the binary file location on the registrar and the destination binary file location on the petitioner, use the **binary file** command in tti-registrar configuration mode.

**binary file** *sourceURL destinationURL*

## Syntax Description

| | |
|---|---|
| *sourceURL* | Specifies the source URL on the registrar for the binary file using one of the keywords in . |
| *destinationURL* | Specifies the destination URL on the petitioner for binary file using one of the keywords in . |

## Command Default

None

## Command Modes

tti-registrar configuration (tti-registrar)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

Use the **binary file** command to specify the location where a binary file will be retrieved from and copied to during the Trusted Transitive Introduction (TTI) exchange. There may be up to nine binary files transferred, each with a different source and destination location. A destination URL could also be a token on the petitioner, such as usbtoken0:

The binary files are retrieved from the registrar and copied to the petitioner. Source URLs for the binary file location are expanded on the registrar. Destination URLs are expanded on the petitioner. Binary files are not processed through the binary expansion functions.

***Table 16: Source and Destination URL Keywords***

| Keyword | Description |
|---|---|
| **archive:** | Retrieves from the archive location. |
| **cns:** | Retrieves from the Cisco Networking Services (CNS) configuration engine. |
| **disk0:** | Retrieves from disk0. |
| **disk1:** | Retrieves from disk1. |
| flash: | Retrieves from flash memory. |
| **ftp:** | Retrieves from the FTP network server. |
| **http:** | Retrieves from a HTTP server. |

| Keyword | Description |
|---|---|
| **https:** | Retrieves from a Secure HTTP (HTTPS) server. |
| **null:** | Retrieves from the file system. |
| **nvram:** | Retrieves from the NVRAM of the router. |
| **rcp:** | Retrieves from a remote copy (rcp) protocol network server. |
| **scp:** | Retrieves from a network server that supports Secure Shell (SSH). |
| **system:** | Retrieves from system memory, which includes the running configuration. |
| **tar:** | Retrieves from a compressed file in tar format. |
| **tftp:** | Retrieves from a TFTP network server. |
| **tmpsys:** | Retrieves from a temporary system location. |
| **unix:** | Retrieves from the UNIX system location. |
| **usbtoken:** | Retrieves from the USB token. |

## Examples

The following example shows how to specify on the registrar where the source binary files are located and where the binary files will be copied to on the petitioner:

```
crypto provisioning registrar
  pki-server cs1
  binary file http://myserver/file1 usbtoken0://file1
  binary file http://myserver/file2 flash://file2
```

## Related Commands

| Command | Description |
|---|---|
| **crypto provisioning registrar** | Configures a device to become a secure device provisioning (SDP) registrar and enter tti-registrar configuration mode. |
| template file | Specifies the source template file location on the registrar and the destination template file location on the petitioner. |

# bind authenticate

To authenticate the client to a Lightweight Directory Access Protocol (LDAP) server, use the **bind authenticate** command in LDAP server configuration mode. To disable authenticated bind and to allow anonymous bind, use the **no** form of this command.

**bind authenticate root-dn** *username* **password** [**0** *string* | **6** *string* | **7** *string*] *string*
**no bind authenticate root-dn** *username* **password** [**0** *string* | **6** *string* | **7** *string* ] *string*

## Syntax Description

| | |
|---|---|
| **root-dn** | Specifies the bind distinguished name (DN) for an authenticated user. |
| *username* | Root user of the LDAP server. |
| **password** | Specifies the LDAP server password. |
| **0** | (Optional) Specifies the unencrypted (cleartext) shared key. |
| **6** | (Optional) Specifies the advanced encryption scheme (AES) encrypted key.<br>**Note**<br>Type 6 AES encrypted passwords are configured using the **password encryption aes** command. |
| **7** | (Optional) Specifies the hidden shared key. |
| *string* | The unencrypted (cleartext) shared key. |

## Command Default

Anonymous bind is performed. Anonymous bind refers to a simple bind operation with no DN and password.

## Command Modes

LDAP server configuration (config-ldap-server)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| 15.4(1)T | This command was modified. The **6** keyword was added. |

## Examples

The following example shows how to authenticate the “user1” user to the LDAP server using the password “123”:

```
Device> enable
Device# configure terminal
Device(config)# ldap server server1
Device(config-ldap-server)# bind authenticate root-dn
cn=user1,cn=users,dc=nac-blr2,dc=example,dc=com password 123
```

## Related Commands

| Command | Description |
|---|---|
| **ipv4** (**ldap**) | Creates an IPv4 address within an LDAP server address pool. |
| **ldap server** | Defines an LDAP server and enters LDAP server configuration mode. |
| **password encryption aes** | Enables a type 6 encrypted preshared key. |
| **transport port (ldap)** | Configures the transport protocol for establishing a connection with the LDAP server. |

# block count

To lock out group members for a length of time after a set number of incorrect passwords are entered, use the **block count**command in local RADIUS server group configuration mode. To remove the user block after invalid login attempts, use the **no** form of this command.

**block count** *count* **time** {**seconds** | **infinite**}
**no block count** *count* **time** {**seconds** | **infinite**}

## Syntax Description

| | |
|---|---|
| *count* | Number of failed passwords that triggers a lockout. Range is from 1 to 4294967295. |
| **time** | Specifies the time to block the account. |
| *seconds* | Number of seconds that the lockout should last. Range is from 1 to 4294967295. |
| **infinite** | Specifies the lockout is indefinite. |

## Command Default

No default behavior or values

## Command Modes

Local RADIUS server group configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200. |
| 12.3(11)T | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Usage Guidelines

If the **infinite keyword**is entered, an administrator must manually unblock the locked username.

## Examples

The following command locks out group members for 120 seconds after three incorrect passwords are entered:

```
Router(config-radsrv-group)#
block count 3 time 120
```

## Related Commands

| Command | Description |
|---|---|
| **clear radius local-server** | Clears the statistics display or unblocks a user. |
| **debug radius local-server** | Displays the debug information for the local server. |
| **group** | Enters user group configuration mode and configures shared setting for a user group. |

| Command | Description |
|---|---|
| **nas** | Adds an access point or router to the list of devices that use the local authentication server. |
| **radius-server host** | Specifies the remote RADIUS server host. |
| **radius-server local** | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| **reauthentication time** | Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group. |
| **show radius local-server statistics** | Displays statistics for a local network access server. |
| **ssid** | Specifies up to 20 SSIDs to be used by a user group. |
| **user** | Authorizes a user to authenticate using the local authentication server. |
| **vlan** | Specifies a VLAN to be used by members of a user group. |

# browser-attribute import

To import user-defined browser attributes into a webvpn context, use the **browser-attribute import**command in webvpn context configuration mode. To remove a browser attribute, use the **no** form of this command.

**browser-attribute import** *device* **:** *file*
**no browser-attribute import** *device* **:** *file*

## Syntax Description

| | |
|---|---|
| *device* **:** *file* | • *device* **:** --Storage device on the system.<br>• *file* --Name of file to be imported. The file name should include the directory location. |

## Command Default

Default values of the attributes are used.

## Command Modes

Webvpn context configuration (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. Attributes that are currently supported are primary color, secondary color, text color, secondary text color, login-message, browser title, and title color. |

## Usage Guidelines

This command will override any other browser attributes that have already been configured using command-line interface (CLI).

## Examples

The following example shows that the file "test-attr.xml" is to be imported from flash:

```
Router (config)# webvpn context sslvpn
 Router (config-webvpn-context)# browser-attribute import flash:test-attr.xml
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn create template** | Creates templates for multilanguage support for messages in an SSL VPN. |

# browser-proxy

To apply browser-proxy parameter settings to a group, use the **browser-proxy** command in ISAKMP group configuration mode. To disable the parameter settings, use the **no** form of this command.

**browser-proxy** *browser-proxy-map-name*
**no browser-proxy** *browser-proxy-map-name*

## Syntax Description

| | |
|---|---|
| *browser-proxy-map-name* | Name of the browser proxy. |

## Command Default

Browser-proxy settings are not applied to a group.

## Command Modes

ISAKMP group configuration (config-isakmp-group)

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

Ensure that you define the browser proxy name before you define the crypto Internet Security Association and Key Management Protocol (ISAKMP) client configuration group name. The two names have to be the same.

## Examples

The following example shows that browser proxy map “EZVPN” has been applied to the group “EZVPN”:

```
crypto isakmp client configuration group EZVPN
 browser-proxy EZVPN
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |



# ca trust-point through clear eou


- ca trust-point, on page 383
- cabundle url, on page 385
- cache authentication profile (server group configuration), on page 387
- cache authorization profile (server group configuration), on page 388
- cache clear age, on page 389
- cache disable, on page 390
- cache expiry (server group configuration), on page 391
- cache max, on page 392
- cache refresh, on page 393
- call admission limit, on page 394
- call guard-timer, on page 395
- category (ips), on page 396
- cdp-url, on page 397
- certificate, on page 401
- chain-validation (ca-trustpool), on page 403
- chain-validation, on page 405
- cifs-url-list, on page 407
- cipherkey, on page 409
- ciphervalue, on page 410
- cisco (ips-auto-update), on page 412
- cisp enable, on page 413
- citrix enabled, on page 414
- class type inspect, on page 415
- class type urlfilter, on page 418
- class-map type inspect, on page 420
- class-map type urlfilter, on page 424
- clear aaa cache filterserver acl, on page 427
- clear aaa cache filterserver group, on page 428
- clear aaa cache group, on page 429
- clear aaa counters servers, on page 430
- clear aaa local user fail-attempts, on page 431
- clear aaa local user lockout, on page 432
- clear access-list counters, on page 433

- clear access-template, on page 434
- clear appfw dns cache, on page 436
- clear ase signatures, on page 437
- clear authentication sessions, on page 439
- clear content-scan, on page 441
- clear crypto call admission statistics, on page 442
- clear crypto ctcp, on page 443
- clear crypto datapath, on page 444
- clear crypto engine accelerator counter, on page 445
- clear crypto gdoi, on page 448
- clear crypto gdoi ks cooperative role, on page 450
- clear crypto ikev2 cluster dead-slaves, on page 451
- clear crypto ikev2 cluster stats, on page 452
- clear crypto ikev2 sa, on page 453
- clear crypto ikev2 stats, on page 454
- clear crypto ipsec client ezvpn, on page 455
- clear crypto isakmp, on page 457
- clear crypto sa, on page 459
- clear crypto session, on page 462
- clear crypto pki benchmarks, on page 464
- clear crypto pki crls, on page 465
- clear cws, on page 466
- clear dmvpn session, on page 467
- clear dmvpn statistics, on page 469
- clear dot1x, on page 470
- clear eap, on page 471
- clear eou, on page 472

# ca trust-point

To identify the trustpoints that is used to validate a certificate during Internet Key Exchange (IKE) authentication, use the **ca trust-point**command in ISAKMP profile configuration mode. To remove the trustpoint, use the **no** form of this command.

**ca trust-point** *trustpoint-name*
**no ca trust-point** *trustpoint-name*

## Syntax Description

| | |
|---|---|
| *trustpoint-name* | The trustpoint name as defined in the global configuration. |

## Command Default

If there is no trustpoint defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

## Command Modes

ISAKMP profile configuration (conf-isa-prof)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

The **ca trust-point** command can be used multiple times to define more than one trustpoint.

This command is useful when you want to restrict validation of certificates to a list of trustpoints. For example, the router global configuration has two trustpoints, A and B, which are trusted by VPN1 and VPN2, respectively. Each Virtual Private Network (VPN) wants to restrict validation only to its trustpoint.

Before you can use this command, you must enter the **crypto isakmp profile** command.



**Note** A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate is rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

To validate a certificate chain sent by the initiator, it is recommended that you configure the required trustpoints of the certificate chain in the ISAKMP profile of the responder. For example, the following configuration on the responder will fail when the initiator sends a certificate chain for myroot trustpoint.

```
crypto pki trustpoint mysub
 chain-validation continue myroot
 revocation-check crl
 rsakeypair mysub
!
```

```
crypto pki trustpoint myroot
 enrollment terminal
 revocation-check crl

crypto isakmp identity dn
crypto isakmp profile mypeer
   ca trust-point mysub
   match certificate cisco
```

This is because the responder builds the CERT_REQ based on trustpoints in the reverse order in which they are defined globally. IKE responder sends the CERT_REQ for myroot to the initiator and IKE initiator sends myroot certificate chain to validate this certificate chain. This can be avoided by the following configuration on the responder ISAKMP profile.

```
crypto pki trustpoint mysub
chain-validation continue myroot
revocation-check crl
rsakeypair mysub
!
crypto pki trustpoint myroot
enrollment terminal
revocation-check crl
!
crypto isakmp identity dn
crypto isakmp profile mypeer
ca trust-point myroot
ca trust-point mysub
match certificate cisco
```

## Examples

The following example specifies two trustpoints, A and B. The ISAKMP profile configuration restricts each VPN to one trustpoint.

```
crypto ca trustpoint A
enrollment url http://kahului:80
crypto ca trustpoint B
enrollment url http://arjun:80
!
crypto isakmp profile vpn1
 trustpoint A
!
crypto isakmp profile vpn2
 ca trust-point B
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp profile** | Defines an ISAKMP profile. |

# cabundle url

To configure the URL from which the public key infrastructure (PKI) trustpool certificate authority (CA) bundle is downloaded, use the **cabundle url** command in ca-trustpool configuration mode. To remove the URL, use the **no** form of this command.

**cabundle url** {*url* | **none**}
**no cabundle url** {*url* | **none**}

## Syntax Description

| | |
|---|---|
| *url* | The URL of the CA certificate bundle. |
| **none** | Specifies that autoupdates of the PKI trustpool CA are not permitted. |

## Command Default

The PKI trustpool CA bundle download URL is not configured.

## Command Modes

Ca-trustpool configuration (ca-trustpool)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Multiple bundle commands can be issued so that the bundle update process is not connected to a single application.

## Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# cabundle url http://www.cisco.com/security/pki/crl/crca2048.crl
```

## Related Commands

| Command | Description |
|---|---|
| **chain-validation** | Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool. |
| **crl** | Specifes the CRL query and cache options for the PKI trustpool. |
| **crypto pki trustpool import** | Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA certificate bundle. |
| **crypto pki trustpool policy** | Configures PKI trustpool policy parameters. |

| Command | Description |
|---|---|
| **default** | Resets the value of a ca-trustpool configuration command to its default. |
| **match** | Enables the use of certificate maps for the PKI trustpool. |
| **ocsp** | Specifies OCSP settings for the PKI trustpool. |
| **revocation-check** | Disables revocation checking when the PKI trustpool policy is being used. |
| **show** | Displays the PKI trustpool policy of the router in ca-trustpool configuration mode. |
| **show crypto pki trustpool** | Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy. |
| **source interface** | Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool. |
| **storage** | Specifies a file system location where PKI trustpool certificates are stored on the router. |
| **vrf** | Specifies the VRF instance to be used for CRL retrieval. |

# cache authentication profile (server group configuration)

To specify a cache authentication profile to use in a named RADIUS or TACACS+ server group, use the **cache authentication profile**command in server group configuration mode. To disable an authentication cache profile, use the **no** form of this command.

**cache authentication profile** *name*
**no cache authentication profile** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of an authentication cache profile. |

## Command Default

No authentication cache profile is enabled.

## Command Modes

Server group configuration (config-sg-radius)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use this command to specify a cache authentication profile for a RADIUS or TACACS+ server group.

Configure the authentication profile prior to applying it to a RADIUS or TACACS+ server group to avoid an error message.

## Examples

The following example caches authentication responses from a RADIUS server according to the rules configured in the authentication profile authen-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkauthentications
Router(config-sg-radius)# cache authentication profile authen-profile
```

## Related Commands

| Command | Description |
|---|---|
| **cache authorization profile** | Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group. |

# cache authorization profile (server group configuration)

To specify a cache authorization profile to use in a named RADIUS or TACACS+ server group, use the **cache authorization profile**command in server group configuration mode. To disable an authorization cache profile, use the **no** form of this command.

**cache authorization profile** *name*
**no cache authorization profile** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of a cache authorization profile to apply to either a RADIUS or TACACS+ server group. |

## Command Default

No authorization cache profile is enabled.

## Command Modes

Server group configuration (config-sg-radius)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use this command to specify an authorization profile for a RADIUS or TACACS+ server group.

## Examples

The following example caches authorization responses from a RADIUS server according to the rules configured in the authorization profile author-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius authorizations
Router(config-sg-radius)# cache authorization profile author-profile
The authorization profile author-profile must be configured prior to applying it to a RADIUS
 or TACACS+ server group or an error message is generated.
```

## Related Commands

| Command | Description |
|---|---|
| **cache authentication profile** | Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group. |

# cache clear age

To specify when, in minutes, cache entries expire and the cache is cleared, use the **cache clear age** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

**cache clear age** *minutes*
**no cache clear age**

## Syntax Description

| | |
|---|---|
| *minutes* | Any value from 0 to 4294967295; the default value is 1440 minutes. |

## Command Default

1440 minutes (1 day)

## Command Modes

AAA filter configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

After enabling the **aaa cache filter**command, which allows you to configure cache filter parameters, you can use the **cache clear age** command to specify when cache entries should expire. If this command is not specified, the default value (1440 minutes) will be enabled.

## Examples

The following example shows how to configure the cache entries to expire every 60 minutes:

```
aaa cache filter
 cache clear age 60
```

## Related Commands

| Command | Description |
|---|---|
| **aaa cache filter** | Enables filter cache configuration. |

# cache disable

To disable the cache, use the **cache disable** command in AAA filter configuration mode. To return to the default, use the **no** form of this command.

**cache disable**
**no cache disable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Caching is enabled.

## Command Modes

AAA filter configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

After enabling the **aaa cache filter**command, which allows you to configure cache filter parameters, you can use the **cache disable** command to disable filter caching. This command can be used to verify that the access control lists (ACLs) are being downloaded.

## Examples

The following example shows how to disable filter caching:

```
aaa cache filter
 cache disable
```

## Related Commands

| Command | Description |
|---|---|
| **aaa cache filter** | Enables filter cache configuration. |

# cache expiry (server group configuration)

To configure how long cached database profile entries in RADIUS or TACACS+ server groups are stored before they expire, use the **cache expiry**command in server group configuration mode. To reset the expiration time to the default value, use the **no** form of this command.

**cache expiry** *hours* [**enforce** | **failover**]
**no cache expiry**

## Syntax Description

| | |
|---|---|
| *hours* | Length of time, in hours, for a cache database profile entry to expire. Range is from 0 to 2147483647. Default is 24 hours. |
| **enforce** | (Optional) Specifies to not use expired entries. |
| **failover** | (Optional) Specifies to use an expired entry if all other methods fail. |

## Command Default

Cache entries expire in 24 hours.

## Command Modes

Server group configuration (config-sg-radius)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use this command to set the amount of time before a cache entry expires (becomes stale). A stale entry is still usable, but the entry will, by default, revise its record with more updated information.

## Examples

The following example sets the expiry time for cache profile entries to 10 days such that the expired entries cannot be used:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkusers
Router(config-sg-radius)# cache expiry 240 enforce
```

## Related Commands

| Command | Description |
|---|---|
| cache authentication profile | Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group. |
| **cache authorization profile** | Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group. |

# cache max

To limit the absolute number of entries that a cache can maintain for a particular server, use the **cache max** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

**cache max** *number*
**no cache max**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of entries the cache can maintain. Any value from 0 to 4294967295; the default value is 100 entries. |

## Command Default

100 entries

## Command Modes

AAA filter configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

After enabling the **aaa cache filter**command, which allows you to configure cache filter parameters, you can use the **cache max** command to specify the maximum number of entries the cache can have at any given time. If this command is not specified, the default value (100 entries) will be enabled.

## Examples

The following example shows how to configure the cache to maintain a maximum of 150 entries:

```
aaa cache filter
 password mycisco
 cache max 150
```

## Related Commands

| Command | Description |
|---|---|
| **aaa cache filter** | Enables filter cache configuration. |

# cache refresh

To refresh a cache entry after a new session begins, use the **cache refresh** command in AAA filter configuration mode. To disable this functionality, use the **no** form of this command.

**cache refresh**
**no cache refresh**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is enabled by default.

## Command Modes

AAA filter configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

The **cache refresh** command is used in an attempt to keep cache entries from the filter server, that are being referred to by new sessions, within the cache. This command resets the idle timer for these entries when they are referenced by new calls.

## Examples

The following example shows how to disable the **cache refresh** command:

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

## Related Commands

| Command | Description |
|---|---|
| **aaa cache filter** | Enables filter cache configuration. |

# call admission limit

To instruct Internet Key Exchange (IKE) to drop security association (SA) requests (that is, calls for Call Admission Control [CAC]) when a specified level of system resources is being consumed, use the **call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

**call admission limit** *charge*
**no call admission limit** *charge*

## Syntax Description

| | |
|---|---|
| *charge* | Level of the system resources that, when used, causes IKE to stop accepting new SA requests. Valid values are 1 to 100000. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

To prevent IKE processes from using excessive CPU resources, you can set a limit value depending on the network topology, the capabilities of the router, and the traffic patterns.

## Examples

The following example causes IKE to drop calls when a given level of system resources are being used:

```
Router(config)# call admission limit 90000
```

## Related Commands

| Command | Description |
|---|---|
| **call admission load** | Configures a CAC metric for scaling WAN protocol session load. |
| **crypto call admission limit** | Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests. |
| **show call admission statistics** | Monitors the global CAC configuration parameters and the behavior of CAC. |

# call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** command in controller configuration mode. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
**no call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]

## Syntax Description

| | |
|---|---|
| *milliseconds* | Specifies the number of milliseconds to wait for a response from the RADIUS server. |
| **on-expiry accept** | (Optional) Accepts the call if a response is not received from the RADIUS server within the specified time. |
| **on-expiry reject** | (Optional) Rejects the call if a response is not received from the RADIUS server within the specified time. |

## Command Default

No default behavior or values.

## Command Modes

Controller configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example shows a guard timer that is set at 20000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
  call guard-timer 20000 on-expiry accept
aaa preauth
group radius
  dnis required
```

## Related Commands

| Command | Description |
|---|---|
| **aaa preauth** | Enters AAA preauthentication configuration mode. |

# category (ips)

To specify a signature category that is to be used for multiple signature actions or conditions, use the **category** command in IPS-category configuration mode.

**category** *category* [*sub-category*]

## Syntax Description

| | |
|---|---|
| *category* | Category name. For a list of supported top-level categories, use the router CLI help (**?**). |
| *sub-category* | (Optional) Category submode. Submode categories are dependent on the category type; that is, submode categories vary from category to category.<br>For a list of supported submode categories, use the router CLI help (**?**). |

## Command Default

None

## Command Modes

IPS-category configuration (config-ips-category)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Cisco IOS Intrusion Prevention System (IPS) 5.x uses signatures and signature categories. All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category.

## Examples

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-categor
y
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

## Related Commands

| Command | Description |
|---|---|
| **ip ips signature-category** | Enters IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS IPS signature parameters on the basis of a signature category. |

# cdp-url

To specify a certificate revocation list (CRL) distribution point (CDP) to be used in certificates that are issued by the certificate server, use the **cdp-url** command in certificate server configuration mode. To remove a CDP from your configuration, use the **no** form of this command.

**cdp-url** *url*
**no cdp-url** *url*

## Syntax Description

| | |
|---|---|
| *url* | HTTP URL where CRLs are published. |

## Command Default

When verifying a certificate that does not have a specified CDP, Cisco IOS public key infrastructure (PKI) clients use the Simple Certificate Enrollment Protocol (SCEP) to retrieve the CRL directly from their configured certificate server.

## Command Modes

Certificate server configuration (cs-server)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

CRLs can be distributed through SCEP, which is the default method, or a CDP, if configured and available. If you set up a CDP, use the **cdp-url**command to specify the CDP location. The CDP URL may be changed after the certificate server is running, but existing certificates are not reissued with the new CDP that is specified through the **cdp-url** command.

You may specify the CDP location by a simple HTTP URL string for example,

**cdp-url** http://server.company.com/ca1.crl

The certificate server supports only one CDP; thus, all certificates that are issued include the same CDP.

If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request, you can specify a non-SCEP request for the retrieval of the CRL from the certificate server by specifying **cdp-url** command with the URL in the following format where *cs-addr* is the location of the certificate server:

**cdp-url** http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL



**Note** If your Cisco IOS certificate authority (CA) is also configured as your HTTP CDP server, specify your CDP with the **cdp-url** http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL command syntax.

It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified through the **cdp-url** command.

In order to force the parser to retain the embedded question mark within the specified location, enter Ctrl-v prior to the question mark. If this action is not taken, CRL retrieval through HTTP returns an error message.

## Examples

The following example shows how to configure a CDP location where the PKI clients do not support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1/
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://server.company.com/certEnroll/aaa.crl
```

The following example shows how to configure a CDP location where the PKI clients support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1 /
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://aaa/cgi-bin/pkiclient.exe?operation=GetCRL
```

### Verifying a CDP Configuration

The following example is sample output from the **show crypto ca certificates** command, which allows you to verify the specified CDP. In this example, the CDP is "http://msca-root.cisco.com/certEnroll/aaa.crl."

```
Router# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 03
  Certificate Usage: General Purpose
  Issuer:
    CN = aaa
  Subject:
    Name: Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root.cisco.com/certEnroll/aaa.crl
  Validity Date:
    start date: 18:44:49 GMT Jun 6 2003
    end   date: 18:44:49 GMT Jun 5 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: bbb
```

## Related Commands

| Command | Description |
|---|---|
| **auto-rollover** | Enables the automated CA certificate rollover functionality. |
| **crl (cs-server)** | Specifies the CRL PKI CS. |
| **crypto pki server** | Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials |

| Command | Description |
|---|---|
| **database archive** | Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file. |
| **database level** | Controls what type of data is stored in the certificate enrollment database. |
| **database url** | Specifies the location where database entries for the CS is stored or published. |
| **database username** | Specifies the requirement of a username or password to be issued when accessing the primary database location. |
| **default (cs-server)** | Resets the value of the CS configuration command to its default. |
| **grant auto rollover** | Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA. |
| **grant auto trustpoint** | Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests. |
| **grant none** | Specifies all certificate requests to be rejected. |
| **grant ra-auto** | Specifies that all enrollment requests from an RA be granted automatically. |
| **hash (cs-server)** | Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA. |
| **issuer-name** | Specifies the DN as the CA issuer name for the CS. |
| **lifetime (cs-server)** | Specifies the lifetime of the CA or a certificate. |

| Command | Description |
|---|---|
| **mode ra** | Enters the PKI server into RA certificate server mode. |
| **mode sub-cs** | Enters the PKI server into sub-certificate server mode |
| **redundancy (cs-server)** | Specifies that the active CS is synchronized to the standby CS. |
| **serial-number (cs-server)** | Specifies whether the router serial number should be included in the certificate request. |
| **show (cs-server)** | Displays the PKI CS configuration. |
| **shutdown (cs-server)** | Allows a CS to be disabled without removing the configuration. |

# certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

**certificate** *certificate-serial-number*
**no certificate** *certificate-serial-number*

## Syntax Description

| | |
|---|---|
| *certificate-serial-number* | Serial number of the certificate to add or delete. |

## Command Default

No default behavior or values.

## Command Modes

Certificate chain configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You could use this command to manually specify a certificate. However, this command is rarely used in this manner. Instead, this command is usually used only to add or delete certificates.

## Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used in this example to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
myrouter# configure terminal
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
```

**Related Commands**

| Command | Description |
|---|---|
| **crypto ca certificate chain** | Enters the certificate chain configuration mode. |

# chain-validation (ca-trustpool)

To enable chain validation from the peer's certificate to the root certificate authority (CA) certificate in the public key infrastructure (PKI) trustpool, use the **chain-validation** command in ca-trustpool configuration mode. To revert to the command default, use the **no** form of this command.

**chain-validation**
**no chain-validation**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Chain validation is disabled.

## Command Modes

Ca-trustpool configuration (ca-trustpool)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

If the **chain-validation** command is not configured, then the validation stops at the peer certificate's issuer.

## Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# chain-validation
```

## Related Commands

| Command | Description |
|---|---|
| **cabundle url** | Configures the URL from which the PKI trustpool CA bundle is downloaded. |
| **crl** | Specifes the CRL query and cache options for the PKI trustpool. |
| **crypto pki trustpool import** | Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle. |
| **crypto pki trustpool policy** | Configures PKI trustpool policy parameters. |
| **default** | Resets the value of a ca-trustpool configuration command to its default. |

| Command | Description |
|---|---|
| **match** | Enables the use of certificate maps for the PKI trustpool. |
| **ocsp** | Specifies OCSP settings for the PKI trustpool. |
| **revocation-check** | Disables revocation checking when the PKI trustpool policy is being used. |
| **show** | Displays the PKI trustpool policy of the router in ca-trustpool configuration mode. |
| **show crypto pki trustpool** | Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy. |
| **source interface** | Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool. |
| **storage** | Specifies a file system location where PKI trustpool certificates are stored on the router. |
| **vrf** | Specifies the VRF instance to be used for CRL retrieval. |

# chain-validation

To configure the level to which a certificate chain is processed on all certificates, including subordinate certificate authority (CA) certificates, use the **chain-validation** command in ca-trustpoint configuration mode. To revert to the command default, use the **no** form of this command.

**chain-validation** [ {**stop** | **continue**} [*parent-trustpoint*]]
**no chain-validation** [ {**stop** | **continue**} [*parent-trustpoint*]]

## Syntax Description

| | |
|---|---|
| **stop** | (Optional) Specifies that the certificate is already trusted.<br>This is the default setting. |
| **continue** | (Optional) Specifies that the subordinate CA certificate associated with the trustpoint must be validated. |
| *parent-trustpoint* | (Optional) The name of the CA parent trustpoint. |

## Command Default

Certificate chain path processing continues until the first trusted certificate, or trustpoint, is reached.

## Command Modes

Ca-trustpoint configuration (ca-trustpoint)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, or the completion of a certificate chain that contains a gap. Devices must be enrolled in your PKI hierarchy and the appropriate key pair associated with the certificate.

If there is more than one parent trustpoint configured, Cisco IOS will select a parent trustpoint based upon configured settings to validate the certificate chain. If you want a specific parent trustpoint to validate certificates, then that trustpoint must be configured with the *parent-trustpoint* argument specified. All certificates, peer and subordinate CA certificates, are validated in the same manner. All trustpoint settings--ACLs, AAA authorization lists, CDP or OCSP overrides--will apply, as will trustpoint policies for trusted and untrusted certificates.

A trustpoint associated with the root CA cannot be configured to be validated to the next level. If **chain-validation continue** is configured for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation stop**.

## Examples

In the following configuration example, all of the certificates will be validated--the peer, SubCA11, SubCA1, and RootCA certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
```

```
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

In the following configuration example, the following certificates will be validated--the peer and SubCA1 certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer sends SubCA1, SubCA11, and the peer certificates in the certificate chain, the following certificates will be validated--the peer, SubCA11, and SubCA1 certificates.

If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA11
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| **revocation-check** | Checks the revocation status of a certificate. |

# cifs-url-list

To enter webvpn URL list configuration mode to configure a list of Common Internet File System (CIFS) server URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **cifs-url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the CIFS server URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

**cifs-url-list** *name*
**no cifs-url-list** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the URL list. The list name can up to 64 characters in length. |

## Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of an SSL VPN website is not configured. If the command is not used to attach a CIFS server URL list to a policy group, then a URL list is not attached to a group policy.

## Command Modes

Webvpn context configuration (config-webvpn-context)
Webvpn group policy configuration (config-webvpn-group)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

Entering this command places the router in webvpn URL list configuration mode. In this mode, the list of CIFS server URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual CIFS server URL list configurations must have unique names.

## Examples

The following example shows that CIFS URL lists have been added under the webvpn context and for a policy group:

```
webvpn context context1
 ssl authenticate verify all
 !
 acl "acl1"
   error-msg "warning!!!..."
   permit url "http://www.exampleurl1.com"
   deny url "http://www.exampleurl2.com"
   permit http any any
 !
 nbns-list l1
   nbns-server 10.1.1.20
 !
 cifs-url-list "c1"
   heading "cifs-url"
   url-text "SSLVPN-SERVER2" url-value "\\SSLVPN-SERVER2"
   url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
 !
 policy group default
```

```
  acl "acl1"
  cifs-url-list "c1"
  nbns-list "l1"
  functions file-access
  functions file-browse
  functions file-entry
default-group-policy default
gateway public
inservice
```

## Related Commands

| Command | Description |
|---|---|
| **heading** | Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website. |
| **policy group** | Attaches a URL list to policy group configuration. |
| **url-text** | Adds an entry to a URL list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# cipherkey

**Note** Effective with Cisco IOS Release 15.2(4)M, the **cipherkey** command is not available in Cisco IOS software.

To specify the symmetric keyname that is used to decrypt the filter, use the **cipherkey** command in FPM match encryption filter configuration mode.

**cipherkey** *keyname*

## Syntax Description

| | |
|---|---|
| *keyname* | String that is used to decrypt the filter. The value that can be used is realm-etcdf-01.sym. |

## Command Default

No symmetric keyname is specified.

## Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 15.2(4)M | This command was removed from the Cisco IOS software. |

## Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **cipherkey** command to specify the the symmetric keyname that is used to decrypt the filter.

## Examples

The following example shows how to configure the cipherkey for filter decryption:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# cipherkey realm-abc.sym
Router(c-map-match-enc-config)#
```

## Related Commands

| Command | Description |
|---|---|
| **class-map type** | Creates a class map to be used for matching packets to a specified class. |
| **match encrypted** | Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode. |

# ciphervalue

**Note** Effective with Cisco IOS Release 15.2(4)M, the **ciphervalue** command is not available in Cisco IOS software.

To specify the encrypted filter contents, use the **ciphervalue** command in FPM match encryption filter configuration mode.

**ciphervalue** *contents*

## Syntax Description

| | |
|---|---|
| *contents* | The encrypted filter contents in the format c encrypted-filter-contents c, where c is any delimiting character except + (plus sign), = (equals sign), and / (forward slash). |

## Command Default

No filter content is specified.

## Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 15.2(4)M | This command was removed from the Cisco IOS software. |

## Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **ciphervalue** command to specify the encrypted filter contents. You can enter up to 200 characters at a time in a multiline input mode for the encrypted filter contents. The new line character (\n) and line feed character (\r) entered in the multiline input mode are ignored in the final cipher value contents.

## Examples

The following example shows how to specify the encrypted filter contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# ciphervalue #2bcXhFL8Ld1v+DqU+dnxgmONCxl4JrYfcLl95xg
ET0b2B1z0sjoCkozE8YxiH/SXL+eG2wf3ogaA7/Fh
awIH7OF3tUcS5Jwim/u95Xlzh2RLNw819tuIBCdorV
Cu0ZzWCF3vqwpGQzaxtSE4sFgPAvSE2LxZc/VT22
F7EQKBhRo=#
Router(c-map-match-enc-config)#
```

## Related Commands

| Command | Description |
|---|---|
| **class-map type** | Creates a class map to be used for matching packets to a specified class. |
| **match encrypted** | Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode. |

# cisco (ips-auto-update)

To enable automatic Cisco IOS Intrusion Prevention System (IPS) signature updates from Cisco.com, use the **cisco** command in IPS-auto-update configuration mode. To disable automatic IPS signature updates from Cisco.com, use the **no** form of this command.

**cisco**
**no cisco**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Automatic IPS signature updates from Cisco.com are not enabled.

## Command Modes

IPS-auto-update configuration (config-ips-auto-update)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Usage Guidelines

The **cisco**command cannot be used in conjunction with the **url**command.

## Examples

The following example shows how to configure automatic signature updates from Cisco.com that occur at the third hour of the 5 day of the month, at the 56th minute of this hour.



**Note** Adjustments are made for months without 31 days and daylight savings time.

```
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# cisco
Router(config-ips-auto-update)# occur-at monthly 5 56 3
```

## Related Commands

| Command | Description |
|---|---|
| **ip ips auto-update** | Enables automatic signature updates for Cisco IOS IPS. |
| occur-at | Defines a preset time for which the Cisco IOS Intrusion Prevention System (IPS) automatically obtains updated signature information. |

# cisp enable

To enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch, use the **cisp enable** command in global configuration mode. To disable CISP, use the **no** form of this command.

**cisp enable**
**no cisp enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

CISP is disabled on the switch.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

Use CISP on a switch so that it acts as an authenticator to a supplicant switch. The link between the authenticator and supplicant switch is a trunk. When you enable VLAN Trunk Protocol (VTP) on both switches, the VTP domain name must be the same, and the VTP mode must be *server*.

When you configure VTP mode, to avoid the MD5 checksum mismatch error, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have the different configuration revision numbers.

## Examples

The following example shows how to enable CISP on a switch so that it acts as an authenticator to a supplicant switch:

```
Switch(config)# cisp enable
```

## Related Commands

| Command | Description |
|---|---|
| **dot1x credentials** | Configures a profile on a supplicant switch. |

# citrix enabled

To enable Citrix application support for end users in a policy group, use the **citrix enabled** command in webvpn group policy configuration mode. To remove Citrix support from the policy group configuration, use the **no** form of this command.

**citrix enabled**
**no citrix enabled**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Citrix application support is not enabled.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Citrix support allows a citrix client to use applications running on a remote server as if they were running locally. Entering the **citrix-enabled** command configures Citrix support for the policy group.

## Examples

The following example configures Citrix support under the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# citrix enabled

Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **filter citrix** | Configures a Citrix application access filter. |
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# class type inspect

To specify the traffic (class) on which an action is to be performed, use the **class type inspect** command in policy-map configuration mode. To delete a class, use the **no** form of this command.

**class type inspect** *class-map-name*
**no class type inspect** *class-map-name*

**Layer 7 (Application-Specific) Traffic Class Syntax**
**class type inspect** *protocol-name class-map-name*
**no class type inspect** *protocol-name class-map-name*

## Syntax Description

| | |
|---|---|
| *class-map-name* | Name of the class on which an action is to be performed.<br>• The *class-map-name* must match the appropriate class name specified with the **class-map type inspect** command. |
| *protocol-name* | Layer 7 application-specific traffic class. The supported protocols are as follows:<br>• **aol** - America Online Instant Messenger (IM)<br>• **edonkey** - eDonkey peer-to-peer (P2P)<br>• **fasttrack** - FastTrack traffic P2P<br>• **gnutella** - Gnutella Version 2 traffic P2P<br>• **gtpv0** - General Packet Radio Service (GPRS) Tunnel Protocol Version 0 (GTPv0)<br>• **gtpv1** - GTP Version 1 (GTPv1)<br>• **h323** - H.323 protocol Version 4<br>• **http** - HTTP<br>• **icq** - I Seek You (ICQ) IM protocol<br>• **imap** - Internet Message Access Protocol (IMAP)<br>• **kazaa2** - Kazaa Version 2 P2P protocol<br>• **msnmsgr** - MSN Messenger IM protocol<br>• **pop3** - Post Office Protocol Version 3 (POP3)<br>• **sip** - Session Initiation Protocol (SIP)<br>• **smtp** - Simple Mail Transfer Protocol (SMTP)<br>• **sunrpc** - SUN Remote Procedure Call (SUNRPC)<br>• **winmsgr** - Windows Messenger IM protocol<br>• **ymsgr** - Yahoo IM |

## Command Default

None

## Command Modes

Policy-map configuration (config-pmap)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(9)T | This command was modified. Support for the IM protocol and the following keywords was added: **aol**, **msnmsgr**, **ymsgr**.<br>Support for the P2P protocol and the following keywords was added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**. |
| 12.4(20)T | This command was modified. Support for the ICQ and Windows Messenger IM protocols and the following keywords was added: **icq**, **winmsgr**.<br>Support for the H.323 protocol and the following keyword was added: **h323**.<br>Support for SIP and the following keyword was added: **sip**. |
| Cisco IOS XE Release 3.4S | This command was modified. The following GTP keywords were added: **gtpv0**, **gtpv1**. |

## Usage Guidelines

Use the **class type inspect** command to specify the class and protocol (if applicable) on which an action is to be performed.

Thereafter, you can specify any of the following actions: drop, inspect, pass, reset, urlfilter, or attach a Layer 7 (application-specific) policy map to a “top-level” (Layer 3 or Layer 4) policy map (with the **service-policy (policy-map)** command).

**Note** A Layer 7 policy is considered to be a nested policy of the top-level policy, and it is called a child policy.

**Note** To attach a Layer 7 policy-map, it is mandatory to configure the **inspect** action under class type inspect .

The following protocols are supported for Cisco IOS XE Release 3.4S.

- GTPv0
- GTPv1
- HTTP
- IMAP
- Match-all Logical-AND all matching statements under this classmap
- Match-any Logical-OR all matching statements under this classmap
- POP3

- SMTP
- Sun RPC

## Examples

The following example shows how to configure the “my-im-pmap” policy map with two IM classes (AOL and Yahoo Messenger) and only allow text-chat messages to pass through. When any packet with a service other than “text-chat” is seen, the connection will be reset.

```
class-map type inspect aol match-any my-aol-cmap
 match service text-chat
!
class-map type inspect ymsgr match-any my-ysmgr-cmap
 match service any
!
policy-map type inspect im my-im-pmap
 class type inspect aol my-aol-cmap
 allow
 log
!
 class type inspect ymsgr my-ysmgr-cmap
 rest
 log
!
class-map type inspect gtpv1
 match-any gtp_policy_gtpv1
 match message-id 18

policy-map type inspect gtpv1 gtp_policy_gtpv1
class type inspect gtpv1 gtp_policy_gtpv1
 log
```

## Related Commands

| Command | Description |
|---|---|
| **class-map type inspect** | Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type class map. |
| **policy-map type inspect** | Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type policy map. |
| **service-policy (policy-map)** | Attaches a Layer 7 policy map to a top-level Layer 3 or Layer 4 policy map. |

# class type urlfilter

To associate a URL filter class with a URL filtering policy map, use the **class type urlfilter** command in policy-map configuration mode. To disassociate the class, use the **no** form of this command.

**class type urlfilter** [**trend** | **n2h2** | **websense**] *class-map-name*
**no class type urlfilter** [**trend** | **n2h2** | **websense**] *class-map-name*

## Syntax Description

| | |
|---|---|
| **trend** | (Optional) Specifies that the class map applies to a Trend Micro filtering URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy. |
| **n2h2** | (Optional) Specifies that the class map applies to a SmartFilter URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy. |
| **websense** | (Optional) Specifies that the class map applies to a Websense URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy. |
| *class-map-name* | Name of the URL filter class map. |

## Command Default

No class is associated with a policy map.

## Command Modes

Policy-map configuration (config-pmap)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)XZ | This command was introduced. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **class type urlfilter** command to associate a class with a URL filtering policy map. You can associate one or more classes with the URL filtering policy map. You must create the class map for the class before you can associate the class with the policy map. In addition, you must use the **parameter type urlfpolicy** command to associate URL filtering parameters with the policy before you canassociate a class with the URL filtering policy map.

## Examples

The following example shows how the **class type urlfilter**command is used to create the URL filtering policy map trend-policy and associate three classes with the policy map--trusted-domain-class, untrusted-domain-class, and drop-category.

```
policy-map type inspect urlfilter trend-policy
 parameter type urlfpolicy trend trend-param-map
 class type urlfilter trusted-domain-class
  log
  allow
 class type urlfilter untrusted-domain-class
  log
  reset
 class type urlfilter trend drop-category
```

```
log
reset
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map type inspect urlfilter** | Creates or modifies a URL filter type inspect policy map. |

# class-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map, use the **class-map type inspect** command in global configuration mode. To remove a class map from the router configuration file, use the **no** form of this command.

**Layer 3 and Layer 4 (Top Level) Class Map Syntax**
**class-map type inspect** {**match-any** | **match-all**} *class-map-name*
**no class-map type inspect** {**match-any** | **match-all**} *class-map-name*

**Layer 7 (Application-Specific) Class Map Syntax**
**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
**no class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*

## Syntax Description

| | |
|---|---|
| **match-any** | Determines how packets are evaluated when multiple match criteria exist. Packets must meet one of the match criteria to be considered a member of the class. |
| **match-all** | Determines how packets are evaluated when multiple match criteria exist. Packets must meet all of the match criteria to be considered a member of the class.<br>**Note**<br>The **match-all** keyword is available only with Layer 3, Layer 4, SMTP, and HTTP type class maps. |
| *class-map-name* | Name of the class map. The name can have a maximum of 40 alphanumeric characters. The class map name is used to configure the policy for the class in the policy map. |

| | |
|---|---|
| *protocol-name* | Layer 7 application-specific class map. The supported protocols are as follows:<br>• **aol** - America Online Instant Messenger (IM)<br>• **edonkey** - eDonkey peer-to-peer (P2P)<br>• **fasttrack** - FastTrack traffic P2P<br>• **gnutella** - Gnutella Version 2 traffic P2P<br>• **gtpv0** - General Packet Radio Service (GPRS) Tunnel Protocol Version 0 (GTPv0)<br>• **gtpv1**- GTP Version 1 (GTPv1)<br>• **gtpv2**gtpv2 - GTP Version 2 (GTPv2)<br>• **h323** - h323 Protocol, Version 4<br>• **http** - HTTP<br>• **icq** - I Seek You (ICQ) IM<br>• **imap** - Internet Message Access Protocol (IMAP)<br>• **kazaa2** - Kazaa Version 2 P2P<br>• **msnmsgr** - MSN Messenger IM protocol<br>• **pop3** - Post Office Protocol, Version 3 (POP 3)<br>• **sip** - Session Initiation Protocol (SIP)<br>• **smtp** - Simple Mail Transfer Protocol (SMTP)<br>• **sunrpc** - SUN Remote Procedure Call (SUNRPC)<br>• **winmsgr** - Windows IM<br>• **ymsgr** - Yahoo IM |

## Command Default

The behavior of the **match-any** keyword is the default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(9)T | This command was modified. The following P2P protocol keywords were added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**.<br>The following IM protocol keywords were added: **aol**, **msnmsgr**, **ymsgr**. |
| 12.4(15)XZ | This command was modified. Support for the Session Initiation Protocol (SIP) was added. |

| Release | Modification |
|---|---|
| 12.4(20)T | This command was modified. The following IM protocol keywords were added: **icq, winmsgr**.<br>The following VoIP protocol keyword was added: **h323 (Version 4)**. |
| 15.1(2)T | This command was modified. Support for IPv6 was added. |
| Cisco IOS XE Release 3.2S | This command was modified. The following keywords were added: **smtp**, **imap**, **pop3**, and **sunrpc**. |
| Cisco IOS XE Release 3.4S | This command was modified. The following GTP keywords were added: **gtpv0**, **gtpv1**. |
| Cisco IOS XE Release 3.9S | This command was modified. The **gtpv2** keyword was added. |

## Usage Guidelines

Use the **class-map type inspect** command to specify the name and protocol (if applicable) of a Layer 3, Layer 4, or Layer 7 class map.

### Layer 3 and Layer 4 (Top-Level) Class Maps

You can configure a top-level (Layer 3 or Layer 4) class map, which allows you to identify the traffic stream at a high level, by issuing the **match access-group** and **match protocol** commands. These class maps cannot be used to classify traffic at the application level (the Layer 7 level).

### Layer 7 (Application-Specific) Class Maps

Application-specific class maps allow you to identify traffic based on the attributes of a given protocol. Match conditions in these class maps are specific to an application (for example, HTTP or SMTP). In addition to the type inspect, you must specify a protocol name (*protocol-name* argument) to create an application-specific class map.



**Note** Configuring the **match access-group** 101 filter enables Layer-4 inspection. As a result, Layer-7 inspection is skipped unless the class-map is of type **match-all**.

## Examples

The following example shows how to configure class map c1 with the match criterion of ACL 101 based on the HTTP protocol:

```
class-map type inspect match-all c1
 match access-group 101
 match protocol http
```

The following example shows how to configure the class map winmsgr-textchat with the match criterion of text-chat based on the Windows IM protocol:

```
class-map type inspect match-any winmsgr winmsgr-textchat
 match service text-chat
```

The following example shows how to configure the class map gtpv2_l4c with the match criterion of Layer7 based on the GTPv1 protocol:

```
class-map type inspect match-all gtpv2_l4c
 match protocol gtpv1
```

## Related Commands

| Command | Description |
|---|---|
| **match access-group** | Configures the match criteria for a class map based on the specified ACL number or name. |
| **match class-map** | Uses a traffic class as a classification policy. |
| **match protocol** | Configures the match criteria for a class map based on the specified protocol. |
| **match service** | Configures the match criteria for a class map based on the specified IM protocol. |

# class-map type urlfilter

To create or modify a URL filter class map, use the **class-map type urlfilter** command in global configuration mode. To remove the class map, use the **no** form of this command.

### Releases Prior to Cisco IOS 15.4(3)M

**class-map type urlfilter** [**trend** | **n2h2** | **websense**] [**match-any**] *class-map-name*
**no class-map type urlfilter** [**trend** | **n2h2** | **websense**] [**match-any**] *class-map-name*

### Cisco IOS Release 15.4(3)M and Later Releases

**class-map type urlfilter** [**match-any**] *class-map-name*
**no class-map type urlfilter** [**match-any**] *class-map-name*

## Syntax Description

| | |
|---|---|
| **trend** | (Optional) Specifies that the class map applies to a Trend Micro URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy. |
| **n2h2** | (Optional) Specifies that the class map applies to a SmartFilter URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy. |
| **websense** | (Optional) Specifies that the class map applies to a Websense URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy. |
| **match-any** | (Optional) Specifies how URL requests are evaluated when multiple match criteria exist in a class map. |
| *class-map-name* | Name of the URL filter class map. |

## Command Default

No class maps are created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)XZ | This command was introduced. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 15.4(3)M | This command was modified. The following keywords are removed: **trend**, **n2h2**, **websense**. |

## Usage Guidelines

Use the **class-map type urlfilter** command to enter class-map configuration mode and create or modify a URL filter class map. The class map is used as a traffic filter to segregate HTTP traffic for which a URL filtering policy applies. If you specify multiple match criteria and want to segregate the traffic when there is at least one match, use the **match-any** keyword. If you do not specify a type of filtering policy with the **trend**, **n2h2**, or **websense** keyword, then the class map applies to a local URL filtering policy.

**Local Class Maps**

Use the **class-map type urlfilter match-any** *class-m ap-name* to create or modify a local class map. filtering mode. Typically, you create three local class maps: one to specify trusted domains, one to specify untrusted domains, and one to specify keywords to block.

To specify the match criteria for the trusted and untrusted domain classes, use the following command:

- **match server-domain urlf-glob** *parameter-map-name*

Before you use this command, you must configure the **urlf-glob** parameter with the **parameter-map type urlf-glob** command.

To specify the match criteria for the keyword class map use the following command:

- **match url-keyword urlf-glob** *parameter-map-name*

Before you use this command, you must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** command.

**Trend Micro Class Maps**

Use the **class-map type urlfilter trend match-any** *class-m ap-name* command to create or modify a URL class map for the Trend Router Provisioning Server (TRPS). Typically, you create two Trend Micro class maps: one to specify URL categories and one to specify URL reputations.

To specify the Trend Micro URL categories for which filtering takes place, use the following command:

- **match url category** *category-name*

To specify the Trend Micro URL reputations for which filtering takes place, use the following command:

- **match url reputation** *reputation-name*

**SmartFilter Class Maps**

Use the **class-map type urlfilter n2h2** *class-map-name* command to create or modify a URL filter class map for a SmartFilter filtering service. Use the following command to specify the match condition for the class map:

- **match server-response any**

**Websense Class Maps**

Use the **class-map type urlfilter websense** *class-map-name* command to create or modify a URL filter class map for a Websense filtering server. Use the following command to specify the match condition for the class map:

- **match server-response any**

## Examples

The following example configures the parameters for local filtering, and then specifies three class maps for local URL filtering: trusted-domain-class, untrusted-domain-class, and keyword-class:

```
parameter-map type urlf-glob trusted-domains-param
 pattern www.example.com
 pattern *.example1.com
parameter-map type urlf-glob untrusted-domain-param
 pattern www.example2.com
 pattern www.example3.org
parameter-map type urlf-glob keyword-param
```

```
 pattern games
 pattern adult
class-map type urlfilter match-any trusted-domain-class
 match server-domain urlf-glob trusted-domain-param
class-map type urlfilter match-any untrusted-domain-class
 match server-domain urlf-glob untrusted-domain-param
class-map type urlfilter match-any keyword-class
 match url-keyword urlf-glob keyword-param
```

The following example configures two class maps for Trend Micro filtering: drop-category and drop-reputation:

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating
class-map type urlfilter trend match-any drop-reputation
 match url reputation PHISHING
 match url reputation ADWARE
```

The following example specifies a class map for SmartFilter filtering called n2h2-class and configures the match criteria as any response from the SmartFilter server:

```
class-map type urlfilter n2h2 match-any n2h2-class
 match server-response any
```

## Related Commands

| Command | Description |
|---|---|
| **match server-domain urlf-glob** | Specifies the server domain match criteria for a URL filtering class map. |
| **match server-response any** | Specifies the match criterion for SmartFilter and Websense class maps. |
| **match url category** | Specifies the URL category match criteria for a URL filtering class map. |
| **match url-keyword urlf-glob** | Specifies the URL keyword match criteria for a URL filtering class map. |
| **match url reputation** | Specifies the URL reputation match criteria for a URL filtering class map. |
| **parameter-map type urlf-glob** | Specifies the filtering parameters for trusted domains, untrusted domains, and blocked keywords. |

# clear aaa cache filterserver acl

To clear the cache status for a particular filter or all filters, use the **clear aaa cache filterserver acl**command in EXEC mode.

**clear aaa cache filterserver acl** [*filter-name*]

## Syntax Description

| | |
|---|---|
| *filter-name* | (Optional) Cache status of a specified filter is cleared. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 122(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

After you clear the cache status for a particular filter or all filters, it is recommended that you enable the **show aaa cache filterserver** command to verify that the cache status.

## Examples

The following example shows how to clear the cache for all filters:

```
clear aaa cache filterserver acl
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa cache filterserver** | Displays the cache status. |

# clear aaa cache filterserver group

To clear contents of the server group cache, use the **clear aaa cache filterserver group** command in privileged EXEC mode.

**clear aaa cache filterserver group** *name* {**all** | **profile** *name*}

## Syntax Description

| | |
|---|---|
| *name* | Name of the server group being cleared. |
| **all** | Clears all profiles. |
| **profile** *name* | Clears an individual profile. |

## Command Default

All profiles are cleared.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Examples

The following example shows how to clear all RADIUS server IDs:

```
Router# clear aaa cache filterserver group group1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa cache filterserver** | Enables AAA filter server definitions. |

# clear aaa cache group

To clear an individual entry or all entries in the cache, use the **clear aaa cache group**command in privileged EXEC mode.

**clear aaa cache group** *name* {**profile** *name* | **all**}

## Syntax Description

| | |
|---|---|
| *name* | Text string representing the name of a cache server group. |
| **profile** *name* | Specifies the name of an individual profile entry to clear. |
| **all** | Specifies that all profiles in the named cache group are cleared. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use this command to clear cache entries.



**Note** To update an old record with profile cache settings and to remove an old record from the cache, clear the cache for the profile.

## Examples

The following example clears all cache entries in the localusers group:

```
Router# clear aaa cache group localusers all
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa cache group** | Displays all of the cache entries stored by the AAA cache. |

# clear aaa counters servers

To clear the authentication, authorization, and accounting (AAA) server information, use the **clear aaa counters servers**command in privileged EXEC mode.

**clear aaa counters servers** {**all** | **radius** {*server-id* | **all**} | **sg** *name*}

## Syntax Description

| | |
|---|---|
| **all** | Clears all AAA server information. |
| **radius** | Clears RADIUS server information. |
| *server-id* | Clears all server IDs displayed by **show aaa servers**command. The range is from 0 to 2147483647. |
| **all** | Clears all server IDs. |
| **sg** | Clear all servers in a server group. |
| *name* | Server group name. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2 .1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 15.2(4)S1 | This command was modified. The **all** keyword was modified to clear all AAA counter server information except for the estimated outstanding and throttled (access and accounting) transactions. |

## Examples

The following example shows how to clear AAA counter server information:

```
Device# clear aaa counters servers all
```

## Related Commands

| Command | Description |
|---|---|
| **aaa cache filterserver** | Enables AAA filter server definitions. |
| **show aaa servers** | Displays the status and number of packets that are sent to and received from all public and private AAA RADIUS servers as interpreted by the AAA Server MIB. |

# clear aaa local user fail-attempts

To clear the unsuccessful login attempts of a user, use the **clear aaa local user fail-attempts**command in privileged EXEC mode.

**clear aaa local user fail-attempts** {**username** *username* | **all**}

## Syntax Description

| | |
|---|---|
| **username** *username* | Specifies the name of the user. |
| **all** | Clears unsuccessful login attempts for all users. |

## Command Default

Unsuccessful login attempts are not cleared.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |

## Usage Guidelines

This command is available only to users having the root privilege.

## Examples

The following example shows that the unsuccessful login attempts for all users will be cleared:

```
Router#
clear aaa local user fail-attempts all
```

## Related Commands

| Command | Description |
|---|---|
| **aaa local authentication attempts max-fail** | Specifies the maximum number of unsuccessful authentication attempts before a user is locked out. |
| clear aaa local user lockout | Unlocks the locked-out users. |
| show aaa local user locked | Displays a list of all locked-out users. |

# clear aaa local user lockout

To unlock the locked-out users, use the **clear aaa local user lockout** command in privileged EXEC mode.

**clear aaa local user lockout** {**username** *username* | **all**}

## Syntax Description

| | |
|---|---|
| **username** *username* | Specifies the name of the user to be unlocked. |
| **all** | Specifies that all users are to be unlocked. |

## Command Default

Locked-out users remain locked out.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |

## Usage Guidelines

Only a user having the root privilege can use this command.

## Examples

The following example shows that all locked-out users will be unlocked:

```
Router#
clear aaa local user lockout all
```

## Related Commands

| Command | Description |
|---|---|
| **aaa local authentication attempts max-fail** | Specifies the maximum number of unsuccessful authentication attempts before a user is locked out. |
| clear aaa local user fail-attempts | Clears the unsuccessful login attempts of a user. |
| show aaa local user loced | Displays a list of all locked-out users. |

# clear access-list counters

To clear the counters of an access list, use the **clear access-list counters**commandin privilegedEXEC mode.

**clear access-list counters** {*access-list-numberaccess-list-name*}

## Syntax Description

| | |
|---|---|
| *access-list-number* | Access list number of the access list for which to clear the counters. |
| *access-list-name* | Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Some access lists keep counters that count the number of packets that pass each line of an access list. The **show access-lists** command displays the counters as a number of matches. Use the **clear access-list counters** command to restart the counters for a particular access list to 0.

## Examples

The following example clears the counters for access list 101:

```
Router# clear access-list counters 101
```

## Related Commands

| Command | Description |
|---|---|
| **show access-lists** | Displays the contents of current IP and rate-limit access lists. |

# clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template** command in privileged EXEC mode.

**clear access-template** {*access-list-numbername*} *template-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostnamesource-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostnamedestination-address*}} [**timeout** *minutes*]

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the dynamic access list. The ranges are from 100 to 199 and from 2000 to 2699. |
| *name* | Name of an IP access list.<br>• The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |
| *template-name* | Name of a dynamic access list. |
| *source-address* | Source address in a dynamic access list.<br>• All other attributes are inherited from the original access-list entry. |
| *source-wildcard-bit* | Source wildcard bits. |
| **any** | Specifies any source hostname. |
| **host** | Specifies a specific source host. |
| *hostname* | Name of the host. |
| *destination-address* | Destination address in a dynamic access list.<br>• All other attributes are inherited from the original access-list entry. |
| *dest-wildcard-bit* | Destination wildcard bits. |
| **timeout** *minutes* | (Optional) Specifies a maximum time limit, in minutes, for each entry within this dynamic list. The range is from 1 to 9999.<br>• This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **any**, **host** *hostname*, and **timeout** *minutes* keywords and arguments were added. |

## Usage Guidelines

The **clear access-template** command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

## Examples

The following example shows how to clear any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
Router> enable
Router# clear access-template vendor 172.20.1.12 any host 172.20.1.13
```

## Related Commands

| Command | Description |
|---|---|
| **access-list (IP extended)** | Defines an extended IP access list. |
| **access-template** | Places a temporary access list entry on a router to which you are connected manually. |
| **show ip accounting** | Displays the active accounting or checkpointed database or displays access list violations. |

# clear appfw dns cache

To clear at least one IP address from the Domain Name System (DNS) cache, use the **clear appfw dns cache**command in privileged EXEC mode.

**clear appfw dns cache name** *dns-name* [**address** *address*]

## Syntax Description

| | |
|---|---|
| **name** *dns-name* | DNS name of the IM server as entered in the **server name** command in application firewall policy. |
| **address** *address* | (Optional) Deletes a specific IP address from the DNS server cache.<br>If an IP address is not specified, all IP addresses for the *dns-name* are deleted from the DNS server cache. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

Resolved IP addresses are never "timed out" and not automatically removed from the DNS cache. Thus, if you find an obsolete IP address in the instant messenger database (DNS cache), you can issue the **clear appfw dns cache** command to remove the IP address and prevent the address from being interpreted by the router as an IM server.

Only one IP address can be deleted at a time. If the deleted IP address appears in the subsequent DNS resolution, the IP address is added to the DNS cache again.

## Examples

The following example shows how to clear the IP address "172.16.0.0" from the cache of the DNS server "logon.cat.aol.com":

```
Router# clear appfw dns cache name logon.cat.aol.com address 172.16.0.0
```

## Related Commands

| Command | Description |
|---|---|
| **server** | Configures a set of DNS servers for which the specified instant messenger application will be interacting. |

# clear ase signatures

**Note** Effective with Cisco IOS Release 12.4(24), the **clear ase signatures** command is not available in Cisco IOS software.

To remove all Automatic Extraction Signatures (ASEs), use the **clear ase signatures** command in privileged EXEC configuration mode.

**clear ase signatures**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| 12.4(24) | This command was removed. |

## Usage Guidelines

This command is used to remove all the generated signatures that are displayed in the **show ase signatures** command output.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

## Examples

The following example output demonstrates the result of removing generated signatures:

```
Router# show ase signatures
Automatic Signature Extraction Detected Signatures
==================================================
Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02
Router# clear ase signatures
Router# show ase signatures
Automatic Signature Extraction Detected Signatures
==================================================
```

The table below describes the significant fields shown in the display.

*Table 17: clear ase signatures Field Descriptions*

| Field | Description |
|---|---|
| Signature Hash | Hash (total) value of the 40-byte pattern, used as a check number for error control |
| Offset | Offset within the packet where the pattern begins |
| Dest Port | Layer 4 destination port for packets that contain this pattern |
| Signature | 40 bytes of packet data used to potentially identify a piece of malware |

## Related Commands

| Command | Description |
|---|---|
| **ase collector** | Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector. |
| **ase group** | Identifies the TIDP group number for the ASE feature. |
| **ase enable** | Enables the ASE feature on a specified interface. |
| **ase signature extraction** | Enables the ASE feature globally on the router. |
| **debug ase** | Provides error, log, messaging, reporting, status, and timer information. |
| show ase | Shows the ASE run-time status, which includes the TIDP group number. |

# clear authentication sessions

To clear information about current Auth Manager sessions and force 802.1X clients on all 802.1X-enabled interfaces to initialize or reauthenticate, use the **clear authentication sessions**command in privileged EXEC mode.



**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **clear authentication session** command replaces the **dot1x intitialize** and **dot1x re-authenticate** commands.

**clear authentication sessions** [**handle** *handle-id*] [**interface** *type number*] [**mac** *mac-address*] [**method** *method-name*] [**session-id** *session-name*]

## Syntax Description

| | |
|---|---|
| **handle** *handle-id* | (Optional) Specifies the particular handle for which Auth Manager information is to be displayed. |
| **interface** *type number* | (Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed. |
| mac *mac-address* | (Optional) Specifies the particular MAC address for which you want to display information. |
| method *method-name* | (Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. |
| session-id *session-name* | (Optional) Clears a particular authentication session by reference to its session ID. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Examples

The following example shows how to use the **clear authentication sessions** command to clear information for all Auth Manager sessions:

```
Switch# clear authentication sessions
```

The following example shows how to use the **clear authentication sessions** command to clear information for the Auth Manager session on a particular interface:

```
Switch# clear authentication sessions interface GigabitEthernet/0/23
```

The following example shows how to use the **clear authentication sessions** command to clear information for the Auth Manager session on a particular MAC address:

```
Switch# clear authentication sessions mac 000e.84af.59bd
```

## Related Commands

| Command | Description |
|---|---|
| **show authentication sessions** | Displays information about current Auth Manager sessions. |

# clear content-scan



**Note** Effective with Cisco IOS Release 15.4(2)T, the **clear content-scan** command is replaced by the **clear cws** command. See the **clear cws** command for more information.

To clear the content scan configuration information, use the **clear content-scan** command in privileged EXEC mode.

**clear content-scan** {**session** {***** | *ip-address* [**failures**]} | **statistics** [**failures**]}

## Syntax Description

| | |
|---|---|
| **session** | Clears content scan session information. |
| ***** | Clears all content scan sessions. |
| *ip-address* | IP address of the client. |
| **failures** | (Optional) Clears content scan failure statistics. |
| **statistics** | Clears content scan statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T1 | This command was introduced. |
| 15.2(4)M | This command was modified. The *ip-address* argument and the **session**, *****, and **failures** keywords were added. |
| 15.4(2)T | This command was replaced by the **clear cws** command. |

## Usage Guidelines

Cisco ScanSafe web security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection service to web traffic. The content scanning process redirects client web traffic to the ScanSafe web servers. ScanSafe web servers scan the web traffic content and either allow or block traffic based on the compliance with configured policies and thus protect clients from malware. Content scanning is enabled on an Internet-facing WAN interface to protect web traffic that goes out. Use the **clear content-scan** command to clear content scan configuration information.

## Examples

The following example shows how to clear the content scan statistics:

```
Device# clear content-scan statistics
```

## Related Commands

| Command | Description |
|---|---|
| **content-scan out** | Enables content scanning on an egress interface. |

# clear crypto call admission statistics

To clear the counters that track the number of accepted and rejected Internet Key Exchange (IKE) requests, use the **call admission limit** command in global configuration mode.

**clear crypto call admission statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Examples

The following example sets to zero the number of accepted and rejected IKE requests:

```
Router(config)# clear crypto call admission statistics
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto call admission statistics** | Monitors Crypto CAC statistics. |

# clear crypto ctcp

To clear all Cisco Tunnel Control Protocol (cTCP) sessions and all Internet Key Exchange (IKE) and IPsec security associations (SAs) that are created on those sessions, use the **clear crypto ctcp**command in privileged EXEC mode.

**clear crypto ctcp** [**peer** *ip-address*]
**no clear crypto ctcp** [**peer** *ip-address*]

## Syntax Description

| | |
|---|---|
| **peer** | (Optional) Clears a specific cTCP peer. |
| *ip-address* | (Optional) IP address of the peer to be cleared. |

## Command Default

cTCP sessions are not cleared.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Examples

The following example shows that all cTCP sessions and all IKE and IPsec SAs that are created on those sessions are to be cleared:

```
Router# clear crypto ctcp
```

The following example shows that only cTCP sessions for peer 10.76.235.21 and all IKE and IPsec SAs that are created on those sessions are to be cleared.

```
Router# clear crypto ctcp peer 10.76.235.21
```

## Related Commands

| Command | Description |
|---|---|
| crypto ctcp | Configures cTCP encapsulation for Easy VPN. |

# clear crypto datapath

To clear the counters or error history buffers in an encrypted network, use the **clear crypto datapath**command in privileged EXEC mode.

**clear crypto datapath** {**ipv4** | **ipv6**} [**error** | **internal** | **punt** | **success**]

## Syntax Description

| | |
|---|---|
| *ipv4* | Clears all counters in a network using IPv4. |
| ipv6 | Clears all counters in a network using IPv6. |
| error | (Optional) Clears the error history buffer. |
| internal | (Optional) Clears the internal event counter. |
| punt | (Optional) Clears the punt event counter. |
| success | (Optional) Clears the success event counter. |

## Command Default

All counters are cleared, unless a keyword is entered to specify one counter.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use the **clear crypto datapath command to clear the history buffers or counters associated with an encrypted data path. You must specify the IP version for the network. If you only use the IP version keyword, all counters will be cleared. To clear only a specific counter, enter the keyword for that counter.**

## Examples

The following example shows how to clear **all the counters in a network using IP version 4**:

```
Router# clear crypto datapath ipv4
```

This example shows how to clear the success counter only:

```
Router# clear crypto datapath ipv4 success
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto datapath** | Displays the counters associated with an encrypted data path. |

# clear crypto engine accelerator counter

To reset the statistical and error counters of the hardware accelerator of the router or the IPsec Virtual Private Network (VPN) Shared Port Adapter (SPA) to zero, use the **clear crypto engine accelerator counter** command in privileged EXEC mode.

**clear crypto engine accelerator counter**

**IPsec VPN SPA**
**clear crypto engine accelerator statistic** [**slot** *slot*/*subslot* | **all**] [**detail**]

## Syntax Description

| | |
|---|---|
| **slot** *slot* / *subslot* | (IPsec VPN SPA only--Optional) Chassis slot number and secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.<br>Resets platform statistics for the corresponding IPsec VPN SPA to zero. This output will not include network interface controller statistics. |
| **all** | (IPsec VPN SPA only--Optional) Resets platform statistics for all IPsec VPN SPAs on the router to zero. This reset will not include network interface controller statistics. |
| **detail** | (IPsec VPN SPA only--Optional) Resets platform statistics for the IPsec VPN SPA and network interface controller statistics to zero. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XL | This command was introduced for the Cisco uBR905 cable access router. |
| 12.2(2)XA | Support was added for the Cisco uBR925 cable access router. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745. |
| 12.2(15)ZJ | This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM. |
| 12.3(4)T | The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 series routers and Catalyst 6500 series switches. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

No specific usage guidelines apply to the hardware accelerators.

**IPsec VPN SPA**

Enter the **slot** keyword to reset platform statistics for the corresponding IPsec VPN SPA to zero. This reset will not include network interface controller statistics.

Enter the **all** keyword to reset platform statistics for all IPsec VPN SPAs on the router to zero. This reset will not include network interface controller statistics.

Enter the **detail** keyword to reset both the platform statistics for the IPsec VPN SPA and network interface controller statistics to zero.

## Examples

### Hardware VPN Module

The following example shows the statistical and error counters of the hardware accelerator being cleared to zero:

```
Router# clear crypto engine accelerator counter
```

IPsec VPN SPA

The following example shows the platform statistics for the IPsec VPN SPA in slot 2, subslot 1 being cleared to zero:

```
Router# clear crypto engine accelerator counter slot 2/1
```

The following example shows the platform statistics for all IPsec VPN SPAs on the router being cleared to zero:

```
Router# clear crypto engine accelerator counter all
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca** | Defines the parameters for the certification authority used for a session. |
| **crypto cisco** | Defines the encryption algorithms and other parameters for a session. |
| **crypto dynamic map** | Creates a dynamic map crypto configuration for a session. |
| **crypto engine accelerator** | Enables the use of the onboard hardware accelerator for IPsec encryption. |
| **crypto ipsec** | Defines the IPSec security associations and transformation sets. |
| **crypto isakmp** | Enables and defines the IKE protocol and its parameters. |
| **crypto key** | Generates and exchanges keys for a cryptographic session. |
| **crypto map** | Creates and modifies a crypto map for a session. |
| **debug crypto engine accelerator control** | Displays each control command as it is given to the crypto engine. |

| Command | Description |
|---|---|
| **debug crypto engine accelerator packet** | Displays information about each packet sent for encryption and decryption. |
| **show crypto engine accelerator ring** | Displays the contents of command and transmits rings for the crypto engine. |
| **show crypto engine accelerator sa database** | Displays the active (in-use) entries in the crypto engine SA database. |
| **show crypto engine accelerator statistic** | Displays the current run-time statistics and error counters for the crypto engine. |
| **show crypto engine brief** | Displays a summary of the configuration information for the crypto engine. |
| **show crypto engine configuration** | Displays the version and configuration information for the crypto engine. |
| **show crypto engine connections** | Displays a list of the current connections maintained by the crypto engine. |

# clear crypto gdoi

To clear the state of the current session of a Group Domain of Interpretation (GDOI) group member (GM) with the key server, use the **clear crypto gdoi** command in privileged EXEC mode.

**clear crypto gdoi** [**group** *group-name*] [**ks coop** {**counter** | **role**} | **ks members** [**counters** | **now**] | **replay counter**]

## Syntax Description

| | |
|---|---|
| **group** *group-name* | (Optional) Name of the group. |
| **ks coop** | (Optional) Specifies that data will be cleared for the cooperative key server (KS). |
| **counter** | (Optional) Clears the counters for the cooperative KS. |
| **role** | (Optional) Clears the role of the cooperative KS. |
| **ks members** | (Optional) Specifies that the data will be cleared for GMs on the current KS. |
| **counters** | (Optional) Clears the counters for all GMs on the current KS. |
| **now** | (Optional) Forces GMs to delete old TEKs and KEKs immediately and re-register. |
| **replay counter** | (Optional) Clears the anti-replay counters. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(11)T | This command was modified. The **group** and **replay** keywords and the *group-name* argument were added. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |
| 15.1(3)T | This command was modified. The **ks members counters** keyword combination was added. |
| 15.2(1)T | This command was modified. The **now** keyword was added. |
| Cisco IOS XE Release 3.8S | This command was modified. The **now** keyword was added. |

## Usage Guidelines

If this command is issued on the group member, the policy of the group member is deleted, and the group member re-registers with the key server.

If this command is issued on the key server, the state on the key server is deleted. If redundancy is configured and this command is issued on the key server, the key server goes back into election mode to elect a new primary key server.

## Examples

If the following command is issued on the key server, the state on the key server is cleared. If the command is issued on a group member, the state is cleared for the entire group, and a re-registration to the key server is forced:

```
Device# clear crypto gdoi
```

If the following command is issued on the key server, the state of the group that is specified is cleared on the key server. If the command is issued on a group member, the state of the group that is specified is cleared on the group member, and re-registration to the key server is forced:

```
Device# clear crypto gdoi group group1
```

The following command clears the anti-replay counters for the GDOI groups:

```
Device# clear crypto gdoi replay counter
```

The following command clears the counters for the cooperative key server:

```
Device# clear crypto gdoi ks coop counter
```

The following command clears all counters for all GMs on the current key server:

```
Device# clear crypto gdoi ks members counters
```

The following command forces GMs to delete old TEKs and KEKs immediately and re-register:

```
Device# clear crypto gdoi ks members now
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto gdoi feature** | Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether each device is running a version that supports GM removal, rekey triggering with policy replacement, or the GDOI MIB. |

# clear crypto gdoi ks cooperative role

To reset the cooperative role of the key server and to initiate the election process on the key server, use the **clear crypto gdoi ks cooperative role** command in privileged EXEC mode.

**clear crypto gdoi ks cooperative role**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Cooperative role is not reset.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |

## Usage Guidelines

If the **clear crypto gdoi ks cooperative role** command is executed on a secondary key server, the election is triggered on that secondary key server although that server would most likely remain a secondary key server because there has been an elected primary key server. However, if the **clear crypto gdoi ks cooperative role** command is executed on the primary key server, the primary key server is reassigned to a secondary role, and as a result, a new election that involves all the key servers is triggered. If the previous primary server has the highest priority (of all the key servers), it again becomes the primary server. If the previous primary server does not have the highest priority, the server having the highest priority is elected as the new primary server.

## Examples

The following example shows that the cooperative role of the key server has been reset and that the election process is to be initiated:

```
clear crypto gdoi ks cooperative role
```

## Related Commands

| Command | Description |
|---|---|
| **clear crypto gdoi** | Clears the state of the current session of a group member with the key server. |

# clear crypto ikev2 cluster dead-slaves

To clear dead secondary gateways from the Internet Key Exchange Version 2 (IKEv2) cluster, use the **clear crypto ikev2 cluster dead-slaves** command in privileged EXEC mode.

**clear crypto ikev2 cluster dead-slaves**

**Note** Keywords such as **master** and **slave** in the context of cluster roles will be replaced with **primary** and **secondary** to align with inclusive language best practices. Users are advised to update their configurations accordingly.

## Syntax Description

This command has no keywords or arguments.

## Command Default

Dead secondary gateways are not cleared by default.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOSE XE 17.14.1a | This command was introduced. |

## Examples

The following is a sample output from the **show crypto ikev2 cluster dead-slaves** command:

```
Device#clear crypto ikev2 cluster dead-secondary

Role           : CLB Primary
Status         : Up
CLB Secondary  : 1
Cluster IP     : 1:1:1::100
Hold time      : 15000 msec
Overload limit : 80%
Codes          : '*' Least loaded, '-' Overloaded

Load statistics:
  Gateway           Role   Last-seen  Prio   Load     IKE  FQDN
  ------------------------------------------------------------
  1:1:1::2           Dead  00:53.867   100   21.6%      0
```

# clear crypto ikev2 cluster stats

To reset the statistics for Internet Key Exchange Version 2 (IKEv2) cluster load balancing, use the **clear crypto ikev2 cluster stats** command in privileged EXEC mode.

**clear crypto ikev2 cluster stats**

## Syntax Description

This command has no keywords or arguments.

## Command Default

The IKEv2 cluster load-balancing statistics are not reset.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOSE XE 17.14.1a | This command was introduced. |

## Usage Guidelines

Use this command to clear the statistics related to IKEv2 cluster load balancing. This can help you troubleshoot or maintain the cluster by resetting the counters to their initial state.

## Examples

The following example shows how to clear IKEv2 cluster load-balancing statistics:

```
Device# clear crypto ikev2 cluster stats

  Gateway           Last-update   redirects
  ------------------------------------------------------------------------
  1:1:1::2           00:00.492       0
  ------------------------------------------------------------------------
Total IKE SAs : 0

Device#
```

## Related Commands

| Command | Description |
|---|---|
| **clear crypto ikev2 stats** | Clears IKEv2 security associations statistics. |

# clear crypto ikev2 sa

To clear the Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **clear crypto ikev2 sa** command in privileged EXEC mode.

**clear crypto ikev2 sa** [**local** {*ipv4-addressipv6-address*} | **remote** {*ipv4-addressipv6-address*} | **fvrf** *vrf-name* | **psh** *number* | **reconnect**]

## Syntax Description

| | |
|---|---|
| **local** {*ipv4-address* \| *ipv6-address*} | (Optional) Clears the IKEv2 security associations matching the local address. |
| **remote** {*ipv4-address* \| *ipv6-address*} | (Optional) Clears the IKEv2 security associations matching the remote address. |
| **fvrf** *vrf-name* | (Optional) Clears the IKEv2 security associations matching the specified front door virtual routing and forwarding (FVRF) instance. |
| **psh** *number* | (Optional) Clears the IKEv2 platform service handler matching the specified connection ID. |
| **reconnect** | (Optional) Clears the IKEv2 reconnect security associations. |

## Command Default

The security associations are not cleared.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| 15.1(4)M | This command was modified. Support was added for IPv6 addresses. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.4(1)T | This command was modified. The **reconnect** keyword was added. |
| Cisco IOS XE Release 3.11S | This command was integrated into Cisco IOS XE Release 3.11S. |

## Usage Guidelines

Use this command to clear an IKEv2 security association and the child security associations.

## Examples

The following example shows how to clear the IKEv2 security associations:

```
Device# clear crypto ikev2 sa
```

# clear crypto ikev2 stats

To clear Internet Key Exchange Version 2 (IKEv2) security associations (SAs) statistics, use the **clear crypto ikev2 stats** command in privileged EXEC mode.

**clear crypto ikev2 stats** [**exchange** [**detailed**] | **ext-service** | **priority-queue** | **timeout**]

## Syntax Description

| | |
|---|---|
| **exchange** | (Optional) Clears information about IKEv2 exchange and notification statistics. |
| **detailed** | (Optional) Provides detailed information about IKEv2 exchange and notification statistics. |
| **ext-service** | (Optional) Clears information about pass and fail counters for IKEv2 external services. |
| **priority-queue** | (Optional) Clears information about the priority queue. |
| **timeout** | (Optional) Clears information about IKEv2 internal timers. |

## Command Default

The IKEv2 SAs statistics are not cleared.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.3(2)T | This command was modified. The keywords **exchange**, **detailed**, **ext-service**, **priority-queue**, and **timeout** were added. |

## Usage Guidelines

Use this command to clear IKEv2 SA statistics.

## Examples

The following example shows how to clear IKEv2 SA statistics:

```
Device# clear crypto ikev2 stats
Cleared crypto ikev2 statistics
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto ikev2 stats** | Displays IKEv2 SA statistics. |

# clear crypto ipsec client ezvpn

To reset the Cisco Easy VPN remote state machine and bring down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel), use the **clear crypto ipsec client ezvpn** command in privileged EXEC mode. If a tunnel name is specified, only the specified tunnel is cleared.

**clear crypto ipsec client ezvpn** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Identifies the IPSec virtual private network (VPN) tunnel to be disconnected or cleared with a unique, arbitrary name. If no name is specified, all existing tunnels are disconnected or cleared. |

## Command Default

If no tunnel name is specified, all active tunnels on the machine are cleared.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)YA | This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(8)YJ | This command was enhanced to specify an IPSec VPN tunnel to be cleared or disconnected for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

The **clear crypto ipsec client ezvpn** command resets the Cisco Easy VPN remote state machine, bringing down the current Cisco Easy VPN remote connection and bringing it back up on the interface. If you specify a tunnel name, only that tunnel is cleared. If no tunnel name is specified, all active tunnels on the machine are cleared.

If the Cisco Easy VPN remote connection for a particular interface is configured for autoconnect, this command also initiates a new Cisco Easy VPN remote connection.

## Examples

The following example shows the Cisco Easy VPN remote state machine being reset:

```
Router# clear crypto ipsec client ezvpn
```

**Related Commands**

| Command | Description |
|---|---|
| **crypto ipsec client ezvpn (global)** | Creates a Cisco Easy VPN remote configuration. |
| **crypto ipsec client ezvpn (interface)** | Assigns a Cisco Easy VPN remote configuration to an interface. |

# clear crypto isakmp

To clear active Internet Key Exchange (IKE) connections, use the **clear crypto isakmp** command in privileged EXEC mode.

**clear crypto isakmp** [*connection-id*] [**active** | **standby**]

## Syntax Description

| | |
|---|---|
| *connection-id* | (Optional) ID of the connection that is to be cleared. If this argument is not used, all existing connections will be cleared. |
| **active** | (Optional) Clears only IKE security associations (SAs) in the active state. For each active SA that is cleared, the standby router will be notified to clear the corresponding standby SA. |
| **standby** | (Optional) Clears only IKE SAs in the standby (secondary) state.<br>**Note**<br>If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.3(11)T | The **active** and **standby** keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines



**Caution** If the *connection-id*argument is not used, all existing IKE connections will be cleared when this command is issued.

## Examples

The following example clears an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
Router# show crypto isakmp sa
    dst            src           state        conn-id   slot
172.21.114.123 172.21.114.67  QM_IDLE           1       0
209.165.201.1  209.165.201.2  QM_IDLE           8       0
Router
#
```

```
clear crypto isakmp 1
Router# show crypto isakmp sa
    dst           src          state        conn-id   slot
209.165.201.1  209.165.201.2  QM_IDLE           8       0
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto isakmp sa** | Displays current IKE SAs. |

# clear crypto sa

To delete IP Security (IPSec) security associations (SAs), use the **clear crypto sa** command in privileged EXEC mode.

**clear crypto sa** [**active** | **standby**]

**Virtual Routing and Forwarding (VRF) Syntax**
**clear crypto sa peer** [**vrf** *fvrf-name*] *address*
**clear crypto sa** [**vrf ivrf-name**]

**Crypto Map Syntax**
**clear crypto sa map** *map-name*

**IP Address, Security Protocol Standard, and SPI Syntax**
**clear crypto sa entry** *destination-address protocol spi*

**Traffic Counters Syntax**
**clear crypto sa counters**

## Syntax Description

| | |
|---|---|
| **active** | (Optional) Clears only IPSec SAs that are in the active state. |
| **standby** | (Optional) Clears only IPSec SAs that are in the standby state.<br>**Note**<br>If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared. |
| **peer vrf** fvrf-name] address | Deletes any IPSec SAs for the specified peer. The *fvrf-name* argument specifies the front door VRF (FVRF) of the peer address. |
| **vrf** *ivrf-name* | (Optional) Clears all IPSec SAs whose inside virtual routing and forwarding (IVRF) is the same as the *ivrf-name*. |
| **map** | Deletes any IPSec SAs for the named crypto map set. |
| *map-name* | Specifies the name of a crypto map set. |
| **entry** | Deletes the IPSec SA with the specified address, protocol, and security parameter index (SPI). |
| *destination-address* | Specifies the IP address of the remote peer. |
| *protocol* | Specifies either the Encapsulation Security Protocol (ESP) or Authentication Header (AH). |
| *spi* | Specifies an SPI (found by displaying the SA database). |
| **counters** | Clears the traffic counters maintained for each SA; the **counters** keyword does not clear the SAs themselves. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(15)T | The **vrf**keywordand *fvrf-name*argument for **clear crypto sa peer** were added. The **vrf** keyword and *ivrf-name*argument for **clear crypto sa** were added. |
| 12.3(11)T | The **active** and **standby** keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

This command clears (deletes) IPSec SAs.

If the SAs were established via Internet Key Exchange (IKE), they are deleted and future IPSec traffic will require new SAs to be negotiated. (When IKE is used, the IPSec SAs are established only when needed.)

If the SAs are manually established, the SAs are deleted and reinstalled. (When IKE is not used, the IPSec SAs are created as soon as the configuration is completed.)



**Note** If the **peer**, **map**, **entry**, **counters, active**, or **standby**keywords are not used, all IPSec SAs will be deleted.

- The **peer** keyword deletes any IPSec SAs for the specified peer.
- The **map** keyword deletes any IPSec SAs for the named crypto map set.
- The **entry** keyword deletes the IPSec SA with the specified address, protocol, and SPI.
- The **active** and **standby** keywords delete the IPSec SAs in the active or standby state, respectively.

If any of the above commands cause a particular SA to be deleted, all the "sibling" SAs--that were established during the same IKE negotiation--are deleted as well.

The **counters** keyword simply clears the traffic counters maintained for each SA; it does not clear the SAs themselves.

If you make configuration changes that affect SAs, these changes will not apply to existing SAs but to negotiations for subsequent SAs. You can use the **clear crypto sa** command to restart all SAs so that they will use the most current configuration settings. In the case of manually established SAs, if you make changes that affect SAs you must use the **clear crypto sa** command before the changes take effect.

If the router is processing active IPSec traffic, it is suggested that you clear only the portion of the SA database that is affected by the changes, to avoid causing active IPSec traffic to temporarily fail.

Note that this command clears only IPSec SAs; to clear IKE state, use the **clear crypto isakmp** command.

## Examples

The following example clears (and reinitializes if appropriate) all IPSec SAs at the router:

```
clear crypto sa
```

The following example clears (and reinitializes if appropriate) the inbound and outbound IPSec SAs established, along with the SA established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
clear crypto sa entry 10.0.0.1 AH 256
```

The following example clears all the SAs for VRF VPN1:

```
clear crypto sa vrf vpn1
```

## Related Commands

| Command | Description |
|---|---|
| **clear crypto isakmp** | Clears active IKE connections. |

# clear crypto session

To delete crypto sessions (IP security [IPsec] and Internet Key Exchange [IKE] security associations [SAs]), use the **clear crypto session** command in privileged EXEC mode.

**clear crypto session** [**local** {*ipv4-addressipv6-address*} [**port** *local-port*]] [**remote** {*ipv4-addressipv6-address*} [**port** *remote-port*]]
[**fvrf** *vrf-name*] [**ivrf** *vrf-name*]
**isakmp group** *group-name*
**username** *user-name*

**IPsec and IKE Stateful Failover Syntax**
**clear crypto session** [**active** | **standby**]

## Syntax Description

| | |
|---|---|
| **local** {*ipv4-address*\| *ipv6-address* | (Optional) Clears crypto sessions for a local crypto endpoint.<br>• TheIP address is the IP address of the local crypto endpoint. |
| **port** *local-port* | (Optional) IKE port of the local endpoint. The *local-port* value can be 1 through 65535. The default value is 500. |
| **remote** {*ipv4-address*\| *ipv6-address* | (Optional) Clears crypto sessions for a remote IKE peer.<br>• The IP address is the IP address of the remote IKE peer. |
| **port** *remote-port* | (Optional) IKE port of the remote endpoint to be deleted. The *remote-port* value can be from 1 through 65535. The default value is 500. |
| **fvrf** *vrf-name* | (Optional) Specifies the front door virtual routing and forwarding (FVRF) session that is to be cleared. |
| **ivrf** *vrf-name* | (Optional) Specifies the inside VRF (IVRF) session that is to be cleared. |
| isakmp group **group-** *name* | (Optional) Clears the specified crypto session using the isakmp group. |
| **username user-** *name* | (Optional) Clears the crypto session for the specified xauth or pki-aaa username. |
| **active** | (Optional) Clears only IPsec and IKE SAs in the active state. |
| **standby** | (Optional) Clears only IPsec and IKE SAs in the standby state.<br>**Note**<br>If the router is in standby mode, the router will immediately resynchronize the standby SAs with the active router. |

## Command Default

All existing sessions will be deleted. The IPsec SAs will be deleted first. Then the IKE SAs are deleted.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.3(11)T | The **active** and **standby** keywords were added. |
| 12.4(11)T | The isakmp group **group-** *name* and **username user-** *name* keywords and associated arguments were added. |

## Usage Guidelines

To clear a specific crypto session or a subset of all the sessions, you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, an FVRF name, or an IVRF name.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPsec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be deleted.

## Examples

The following example shows that all crypto sessions will be deleted:

```
Router# clear crypto session
```

The following example shows that the crypto session of the FVRF named “blue” will be deleted:

```
Router# clear crypto session fvrf blue
```

The following example shows that the crypto sessions of the FVRF “blue” and the IVRF session “green” will be deleted:

```
Router# clear crypto session fvrf blue ivrf green
```

The following example shows that the crypto sessions of the local endpoint 10.1.1.1 and remote endpoint 10.2.2.2 will be deleted. The local endpoint port is 5, and the remote endpoint port is 10.

```
Router# clear crypto session local 10.1.1.1 port 5 remote 10.2.2.2 port 10
```

## Related Commands

| Command | Description |
|---|---|
| show crypto isakmp peer | Displays peer descriptions. |
| **show crypto session** | Displays status information for active crypto sessions in a router. |

# clear crypto pki benchmarks

To clear Public Key Infrastructure (PKI) benchmarking data and release all memory associated with this data, use the **clear crypto pki benchmarks**command in privileged EXEC mode.

**clear crypto pki benchmarks**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

## Usage Guidelines

Use the **clear crypto pki benchmarks**command to clear all PKI benchmarking data and release all memory associated with this data. PKI benchmarking data is used for IOS PKI performance monitoring and optimization. PKI performance monitoring and optimization is turned on or off by using the **crypto pki benchmark** command.

## Examples

The following example shows how to clear PKI benchmarking data:

```
Router# clear crypto pki benchmarks
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki benchmark** | Starts or stops benchmarking data for PKI performance monitoring and optimization. |
| **show crypto pki benchmarks** | Displays benchmarking data for PKI performance monitoring and optimization that was collected. |

# clear crypto pki crls

To remove the certificate revocation list (CRL) database that determines the validity status of digital certificates presented by encryption peers in a PKI, use the **clear crypto pki crls**command in privileged EXEC mode.

**clear crypto pki crls**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

## Usage Guidelines

The the **clear crypto pki crls**command removes the CRL database that was configured with the **crypto pki certificate chain** command, which is used to configure a certificate authority (CA).

## Related Commands

| Command | Description |
|---|---|
| **crypto pki certificate chain** | Enters certificate chain configuration mode for a specified CA. |

# clear cws

To clear the Cloud Web Security configuration information, use the **clear cws** command in privileged EXEC mode.

**clear cws** {**session** {***** | *ip-address* [**failures**]} | **statistics** [**failures**]}

## Syntax Description

| | |
|---|---|
| **session** | Clears Cloud Web Security session information. |
| ***** | Clears all Cloud Web Security sessions. |
| *ip-address* | IP address of the client. |
| **failures** | (Optional) Clears Cloud Web Security failure statistics. |
| **statistics** | Clears Cloud Web Security statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.4(2)T | This command was introduced. This command replaces the **clear content-scan** command. |

## Usage Guidelines

Cisco Cloud Web Security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection service to web traffic. The content scanning process redirects client web traffic to the Cloud Web Security web servers. Cloud Web Security web servers scan the web traffic content and either allow or block traffic based on the compliance with configured policies and thus protect clients from malware. Content scanning is enabled on an Internet-facing WAN interface to protect web traffic that goes out. Use the **clear cws** command to clear Cloud Web Security configuration information.

## Examples

The following example shows how to clear the Cloud Web Security statistics:

```
Device# clear cws statistics
```

## Related Commands

| Command | Description |
|---|---|
| **cws out** | Enables Cloud Web Security content-scanning on an egress interface. |

# clear dmvpn session

To clear Dynamic Multipoint VPN (DMVPN) sessions, use the **clear dmvpn session** command in privileged EXEC mode.

**clear dmvpn session** [**interface tunnel** *number* | **peer** {*ipv4-addressFQDN-stringipv6-address*} | **vrf** *vrf-name*] [**static**]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Displays DMVPN information based on a specific interface. |
| **tunnel** *number* | (Optional) Specifies the tunnel address for the DMVPN peer. The range is from 0 to 2147483647. |
| **peer** | (Optional) Specifies a DMVPN peer. |
| *ipv4-address* | (Optional) The IPv4 address for the DMVPN peer. |
| *FQDN-string* | (Optional) Next hop server (NHS) fully qualified domain name (FQDN) string. |
| *ipv6-address* | (Optional) The IPv6 address for the DMVPN peer. |
| **vrf** *vrf-name* | (Optional) Clears all Next Hop Resolution Protocol (NHRP) sessions related to the specified virtual routing and forwarding (VRF) configuration. |
| **static** | (Optional) Clears all static and dynamic NHRP entries.<br>• You must use the **static**keyword for all NHS FQDN configurations.<br>**Note**<br>If the **static** keyword is not specified, only dynamic NHRP entries are cleared. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| 12.4(20)T | This command was modified. The *ipv6-address* argument was added. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |
| 15.1(2)T | This command was modified. The *FQDN-string* argument was added. |
| 15.2(1)T | This command was modified. The *ipv6-address* argument was added for the **peer** keyword. |

## Usage Guidelines

This command clears existing DMVPN sessions based on input parameters.

## Examples

The following example shows how to clear all DMVPN sessions, both static and dynamic, for the specified peer nonbroadcast multiple access (NBMA) address:

```
Router# clear dmvpn session peer nbma static
```

The following example shows how to clear all DMVPN sessions, both static and dynamic, for the specified peer FQDN string:

```
Router# clear dmvpn session peer examplehub.example1.com static
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip nhrp** | Clears all dynamic entries from the IPv4 NHRP cache. |
| clear ipv6 nhrp | Clears all dynamic entries from the IPv6 NHRP cache. |

# clear dmvpn statistics

To clear Dynamic Multipoint VPN (DMVPN)-related counters, use the **clear dmvpn statistics**command in privileged EXEC mode.

**clear dmvpn statistics** [**peer** {**nbma** | **tunnel**} *ip-address*] [**interface tunnel** *number*] [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| **peer** | (Optional) Specifies a DMVPN peer. |
| **nbma** | (Optional) Specifies nonbroadcast mapping access (NBMA). |
| **tunnel** | (Optional) Specifies a tunnel. |
| *ip-address* | (Optional) Specifies the IP address for the DMVPN peer. |
| **interface** | (Optional) Displays DMVPN information based on a specific interface. |
| **tunnel** *number* | (Optional) Specifies the tunnel address for the DMVPN peer. |
| **vrf** *vrf-name* | (Optional) Clears all DMVPN counters related to the specified virtual routing forwarding (VRF) configuration. |

## Command Default

DMVPN-related counters will not be cleared.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| Cisco IOS XE Release 2.5 | This command was modified. It was integrated into Cisco IOS XE Release 2.5. |

## Usage Guidelines

Based on input parameters, DMVPN-related session counters will be cleared.

## Examples

The following example shows how to clear DMVPN related session counters for the specified tunnel interface:

```
Router# clear dmvpn statistics peer tunnel 192.0.2.3
```

## Related Commands

| Command | Description |
|---|---|
| **clear dmvpn session** | Clears DMVPN sessions. |

# clear dot1x

To clear 802.1X interface information, use the **clear dot1x** command in privileged EXEC mode.

**clear dot1x** {**all** | **interface interface-name**}

## Syntax Description

| | |
|---|---|
| **all** | Clears 802.1X information for all interfaces. |
| interface interface-name | Clears 802.1X information for the specified interface. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(2)XA | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| 12.2(25)SEE | This command was integrated into Cisco IOS Release 12.2(25)SEE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following configuration shows that 802.1X information will be cleared for all interfaces:

```
Router# clear dot1x all
```

The following configuration shows that 802.1X information will be cleared for the Ethernet 0 interface:

```
Router# clear dot1x interface ethernet 0
```

You can verify that the information was deleted by entering the **show dot1x** command.

## Related Commands

| Command | Description |
|---|---|
| **debug dot1x** | Displays 802.1X debugging information. |
| **identity profile default** | Creates an identity profile and enters identity profile configuration mode. |
| **show dot1x** | Displays details for an identity profile. |

# clear eap

To clear Extensible Authentication Protocol (EAP) information on a switch or for a specified port, use the **clear eap** command in privileged EXEC mode.

**clear eap** [**sessions** [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport** *transport-name*]]

## Syntax Description

| | |
|---|---|
| **sessions** | (Optional) Clears EAP sessions on a switch or a specified port. |
| **credentials** *credentials-name* | (Optional) Clears EAP credential information for only the specified profile. |
| **interface** *interface-name* | (Optional) Clears EAP credential information for only the specified interface. |
| **method** *method-name* | (Optional) Clears EAP credential information for only the specified method. |
| **transport** *transport-name* | (Optional) Clears EAP credential information for only the specified lower layer. |

## Command Default

All active EAP sessions are cleared.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SEE | This command was introduced. |
| 12.4(6)T | This command was integrated into Cisco IOS Release 12.4(6)T. |

## Usage Guidelines

You can clear all counters by using the **clear eap** command with the **sessions** keyword, or you can clear only the specified information by using the **credentials**, **interface**, **method**, or **transport** keywords.

## Examples

The following example shows how to clear all EAP information:

```
Router# clear eap sessions
```

The following example shows how to clear EAP session information for the specified profile:

```
Router# clear eap sessions credentials type1
```

## Related Commands

| Command | Description |
|---|---|
| **show eap registrations** | Displays EAP registration information. |
| **show eap sessions** | Displays active EAP session information. |

# clear eou

To clear all client device entries that are associated with a particular interface or that are on the network access device (NAD), use the **clear eou** command in privileged EXEC mode.

**clear eou** {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-type* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*}

## Syntax Description

| | |
|---|---|
| **all** | Clears all client device entries. |
| **authentication** | Authentication type. |
| **clientless** | Authentication type is clientless. |
| **eap** | Authentication type is Extensible Authentication Procotol (EAP). |
| **static** | Authentication type is static. |
| **interface** | Provides information about the interface. |
| *interface-type* | Type of interface (see the table below for a list of interface types). |
| **ip** | Specifies an IP address. |
| *ip-address* | IP address of the client device. |
| **mac** | Specifies a MAC address. |
| *mac-address* | The 48-bit address of the client device. |
| **posturetoken** | Posture token name. |
| *name* | Name of the posture token. |

## Command Modes

Privileged EXEC#

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

The table below lists the interface types that may be used for the *interface-type* **argument**.

***Table 18: Description of Interface Types***

| Interface Type | Description |
|---|---|
| **Async** | Asynchronous interface |

| Interface Type | Description |
|---|---|
| **BVI** | Bridge-Group Virtual Interface |
| **CDMA-Ix** | Code division multiple access Internet exchange (CDMA Ix) interface |
| **CTunnel** | Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface |
| **Dialer** | Dialer interface |
| **Ethernet** | IEEE 802.3 standard interface |
| **Lex** | Lex interface |
| **Loopback** | Loopback interface |
| **MFR** | Multilink Frame Relay bundle interface |
| Multilink | Multilink-group interface |
| **Null** | Null interface |
| **Serial** | Serial interface |
| **Tunnel** | Tunnel interface |
| **Vif** | Pragmatic General Multicast (PGM) Multicase Host interface |
| **Virtual-PPP** | Virtual PPP interface |
| **Virtual-Template** | Virtual template interface |
| **Virtual-TokenRing** | Virtual TokenRing interface |

## Examples

The following example shows that all client device entries are to be cleared:

```
Router# clear eou all
```

## Related Commands

| Command | Description |
|---|---|
| eou | Displays information about EAPoUDP. |



# clear ip access-list counters through crl-cache none


- clear ip access-list counters, on page 477
- clear ip access-template, on page 478
- clear ip admission cache, on page 480
- clear ip audit configuration, on page 481
- clear ip audit statistics, on page 482
- clear ip auth-proxy cache, on page 483
- clear ip auth-proxy watch-list, on page 484
- clear ip inspect ha, on page 486
- clear ip inspect session, on page 487
- clear ip ips configuration, on page 488
- clear ip ips statistics, on page 489
- clear ip sdee, on page 490
- clear ip trigger-authentication, on page 491
- clear ip urlfilter cache, on page 492
- clear ipv6 access-list, on page 493
- clear ipv6 inspect, on page 495
- clear ipv6 snooping counters, on page 496
- clear kerberos creds, on page 497
- clear ldap server, on page 498
- clear logging ip access-list cache, on page 499
- clear parameter-map type protocol-info, on page 500
- clear policy-firewall, on page 501
- clear policy-firewall stats global, on page 502
- clear policy-firewall stats vrf, on page 503
- clear policy-firewall stats vrf global, on page 504
- clear policy-firewall stats zone, on page 505
- clear port-security, on page 506
- clear radius, on page 508
- clear radius local-server, on page 509
- clear webvpn nbns, on page 511
- clear webvpn session, on page 512

- clear webvpn stats, on page 513
- clear xsm, on page 514
- clear zone-pair, on page 516
- clid, on page 517
- client, on page 519
- client authentication list, on page 521
- client configuration address, on page 523
- client configuration group, on page 524
- client inside, on page 525
- client pki authorization list, on page 526
- client recovery-check interval, on page 527
- client connect, on page 528
- client rekey encryption, on page 529
- client rekey hash, on page 531
- client transform-sets, on page 532
- commands (view), on page 533
- configuration url, on page 537
- configuration version, on page 539
- config-exchange, on page 540
- config-mode set, on page 541
- connect, on page 542
- content-length, on page 543
- content-scan out, on page 545
- content-scan whitelisting, on page 546
- content-type-verification, on page 547
- control, on page 551
- copy (consent-parameter-map), on page 553
- copy idconf, on page 555
- copy ips-sdf, on page 557
- consent email, on page 560
- crl, on page 561
- crl (cs-server), on page 564
- crl query, on page 567
- crl best-effort, on page 569
- crl optional, on page 571
- crl-cache delete-after, on page 573
- crl-cache none, on page 575

# clear ip access-list counters

To clear IP access list counters, use the **clear ip access-list counters** command in privileged EXEC mode.

**clear ip access-list counters** [*access-list-numberaccess-list-name*]

## Syntax Description

| | |
|---|---|
| *access-list-number* \| *access-list-name* | (Optional) Number or name of the IP access list for which to clear the counters. If no name or number is specified, all IP access list counters are cleared. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |

## Usage Guidelines

The counter counts the number of packets that match each **permit** or **deny** statement in an access list. You might clear the counters if you want to start at zero to get a more recent count of the packets that are matching an access list. The **show ip access-lists** command displays the counters as a number of matches.

## Examples

The following example clears the counter for access list 150:

```
Router# clear ip access-list counters 150
```

## Related Commands

| Command | Description |
|---|---|
| **show ip access list** | Displays the contents of IP access lists. |

# clear ip access-template

To clear statistical information on the access template, use the **clear ip access-template** command in privileged EXEC mode.

**clear ip access-template** {*access-list-numbername*} *dynamic-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostnamesource-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostnamedestination-address*}}

## Syntax Description

| | |
|---|---|
| *access-list-number* | Access list number. Range is from 100 to 199 for an IP extended access list and from 2000 to 2699 for an expanded-range IP extended access list. |
| *name* | Name of an IP access list.<br>• The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |
| *dynamic-name* | Name of a dynamic access list. |
| *source-address* | Source address in a dynamic access list.<br>• All other attributes are inherited from the original access-list entry. |
| *source-wildcard-bit* | Source wildcard bits. |
| **any** | Specifies any source host name. |
| **host** | Specifies a specific source host. |
| *hostname* | Name of the host. |
| *destination-address* | Destination address in a dynamic access list.<br>• All other attributes are inherited from the original access-list entry. |
| *dest-wildcard-bit* | Destination wildcard bits. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **any**, **host** *hostname*, and **timeout** *minutes* keywords and arguments were added. |

## Examples

This example shows how to clear statistical information on the access list:

```
Router#
clear ip access-template 201 list1 any 172.0.2.1 172.0.2.2
```

## Related Commands

| Command | Description |
|---|---|
| **show mls netflow** | Displays configuration information about the NetFlow hardware. |

# clear ip admission cache

To clear IP admission cache entries from the router, use the **clear ip admission cache**command in privileged EXEC mode.

**clear ip admission cache** {***** | **host ip address**}

## Syntax Description

| | |
|---|---|
| ***** | Clears all IP admission cache entries and associated dynamic access lists. |
| **host ip address** | Clears all IP admission cache entries and associated dynamic access lists for the specified host. |

## Command Modes

Privileged EXEC #

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

Use this command to clear entries from the admission control cache before they time out.

## Examples

The following example shows that all admission entries are to be deleted:

```
Router# clear ip admission cache *
```

The following example shows that the authentication proxy entry for the host with the IP address 192.168.4.5 is to be deleted:

```
Router# clear ip admission cache 192.168.4.5
```

## Related Commands

| Command | Description |
|---|---|
| show ip admission cache | Displays the admission control entries or the running admission control configuration. |

# clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** command in EXEC mode.

**clear ip audit configuration**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(13)T | This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **clear ip audit configuration** EXEC command to disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources.

## Examples

The following example clears the existing IP audit configuration:

```
clear ip audit configuration
```

# clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** command in EXEC mode.

**clear ip audit statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(13)T | This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **clear ip audit statistics** EXEC command to reset statistics on packets analyzed and alarms sent.

## Examples

The following example clears all IP audit statistics:

```
clear ip audit statistics
```

# clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

**clear ip auth-proxy cache** {*****|*host-ip-address*}

## Syntax Description

| | |
|---|---|
| ***** | Clears all authentication proxy entries, including user profiles and dynamic access lists. |
| *host-ip-address* | Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to clear entries from the translation table before they time out.

## Examples

The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

## Related Commands

| Command | Description |
|---|---|
| **show ip auth-proxy** | Displays the authentication proxy entries or the running authentication proxy configuration. |

# clear ip auth-proxy watch-list

To delete a single watch-list entry or all watch-list entries in Privileged EXEC configuration command mode, use the **clear ip auth-proxy watch-list** command.

**clear ip auth-proxy watch-list** {*ip-addr* | *****}

## Syntax Description

| | |
|---|---|
| *ip-addr* | IP address to be deleted from the watch list. |
| ***** | All watch-list entries from the watch list. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC.

## Command History

| Release | Modification |
|---|---|
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is supported on the systems that are configured with a Supervisor Engine 2 Supervisor Engine 2 only.

If you see entries in the watch list that you suspect are not valid, you can enter the **clear ip auth-proxy watch-list** command to clear them manually instead of waiting for the watch list to expire.

## Examples

This example shows how to delete a single watch-list entry:

```
Router# clear
 ip auth-proxy watch-list 10.0.0.2
Router#
```

This example shows how to delete all watch-list entries:

```
Router# clear
 ip auth-proxy watch-list *
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **ip auth-proxy max-login-attempts** | Limits the number of login attempts at a firewall interface and QoS filtering and enter the ARP ACL configuration submode. |
| **ip auth-proxy watch-list** | Enables and configures an authentication proxy watch list. |

| Command | Description |
|---|---|
| **show ip auth-proxy watch-list** | Displays the information about the authentication proxy watch list. |

# clear ip inspect ha

To delete the Firewall stateful failover sessions information from a router's memory, use the **clear ip inspect ha**command in privileged EXEC mode.

**clear ip inspect ha** [**sessions all** | **statistics**]

## Syntax Description

| | |
|---|---|
| **sessions all** | (Optional) Clears all the firewall HA sessions. |
| statistics | (Optional) Clears the HA statistics on the device. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

If the **clear ip inspect ha sessions all**command is used on the standby device, the standby HA sessions are cleared. This initiates re-synchronization of all HA sessions from the active device to the standby device.

## Examples

The following example shows all sessions being deleted:

```
Router# clear ip inspect ha sessions all
```

The following example shows statitics being deledted.

```
Router# clear ip inspect ha statistics
```

# clear ip inspect session

To delete Context-Based Access Control (CBAC) configuration and session information from a router's memory, use the **clear ip inspect session**command in privileged EXEC mode.

**clear ip inspect session** *session-address*

## Syntax Description

| | |
|---|---|
| *session-address* | Deletes a specific session; the format is 0-FFFFFFFF. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

Sessions consist of control channels and data channels.

Use the **clear ip inspect session** command to delete a control channel or a data channel. If you specify a control channel session, then data channel sessions may also be deleted, depending on the application protocols being used. If you specify a data channel session, then only that specific session is deleted.

If you attempt to delete a session and the **clear ip inspect session** command is not supported for the specified protocol, then an error message is generated.

If you want to delete a specific session, use the **show ip inspect session** command to display all session addresses.

**Note** The **clear ip inspect session** command is recommended for advanced users only because it may disrupt network operations if traffic is still flowing through the session.

## Examples

The following example displays the current session addresses:

```
Router# show ip inspect session
Established Sessions
 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following example shows a specific session being deleted:

```
Router# clear ip inspect session 25A6E1C
```

## Related Commands

| Command | Description |
|---|---|
| **show ip inspect** | Displays CBAC configuration and session information. |

# clear ip ips configuration

To disable Cisco IOS Firewall Intrusion Prevention System (IPS), remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip ips configuration** command in EXEC mode.

**clear ip ips configuration**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.3(8)T | The command name was changed from the **clear ip audit configuration** command to the **clear ip ips configuration** command. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example clears the existing IPS configuration:

```
clear ip ips configuration
```

# clear ip ips statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip ips statistics** command in privileged EXEC mode.

**clear ip ips statistics** [**vrf vrf-name**]

## Syntax Description

| | |
|---|---|
| **vrf** | (Optional) Resets statistics on packets analyzed and alarms sent per VRF. |
| *vrf-name* | User specific VRF. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.3(8)T | The command name was changed from the **clear ip audit statistics** command to the **clear ip ips statistics** command. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | The **vrf** *keyword and argument were added.* |

## Examples

The following example clears all Intrusion Protection System (IPS) statistics:

```
clear ip ips statistics
```

### Sample Output for the clear ip ips statistics vrf Command

The following example displays the output of the clear ip ips statistics vrf vrf-namecommand:

```
Router# clear ip ips statistics vrf VRF_600
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

# clear ip sdee

To clear Security Device Event Exchange (SDEE) events or subscriptions, use the **clear ip sdee** command in privileged EXEC mode.

**clear ip sdee** {**events** | **subscriptions**}

## Syntax Description

| | |
|---|---|
| **events** | Clears SDEE events from the event buffer. |
| **subscriptions** | Clears SDEE subscriptions. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

Because subscriptions are properly closed by the Cisco IOS Intrusion Prevention System (IPS) client, this command is typically used only to help with error recovery.

## Examples

The following example shows how to clear all open SDEE subscriptions on the router:

```
Router# clear ip sdee subscriptions
```

## Related Commands

| Command | Description |
|---|---|
| **ip ips notify** | Specifies the method of event notification. |
| **ip sdee events** | Sets the maximum number of SDEE events that can be stored in the event buffer. |
| ip sdee subscriptions | Sets the maximum number of SDEE subscriptions that can be open simultaneously. |

# clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

**clear ip trigger-authentication**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

## Examples

The following example clears the remote host table:

```
Router# show ip trigger-authentication
Trigger-authentication Host Table:
Remote Host          Time Stamp
172.21.127.114       2940514234
Router# clear ip trigger-authentication
Router# show ip trigger-authentication
```

## Related Commands

| Command | Description |
|---|---|
| **show ip trigger-authentication** | Displays the list of remote hosts for which automated double authentication has been attempted. |

# clear ip urlfilter cache

To clear the cache table, use the **clear ip urlfilter cache** command in user EXEC mode.

**clear ip urlfilter cache** {*ip-address* | **all**} [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *ip-address* | Clears the cache table of a specified server IP address. |
| **all** | Clears the cache table completely. |
| **vrf** *vrf-name* | (Optional) Clears the cache table only for the specified Virtual Routing and Forwarding (VRF) interface. |

## Command Modes

User EXEC (>)

## Command History

| Release | Modification |
|---|---|
| 12.2(11)YU | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.3(14)T | The **vrf** *vrf-name*keyword/argument pair was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address.

## Examples

The following example shows how to clear the cache table of IP address 172.18.139.21:

```
clear ip urlfilter cache 172.18.139.21
```

The following example shows how to clear the cache table of all IP addresses:

```
clear ip urlfilter cache all
```

The following example shows how to clear the cache table of all IP addresses in the vrf named bank.

```
clear ip urlfilter cache all vrf bank
```

## Related Commands

| Command | Description |
|---|---|
| **ip urlfilter cache** | Configures cache parameters. |
| **show ip urlfilter cache** | Displays the destination IP addresses that are cached into the cache table. |

# clear ipv6 access-list

To reset the IPv6 access list match counters, use the **clear ipv6 access-list**command in privileged EXEC mode.

**clear ipv6 access-list** [*access-list-name*]

## Syntax Description

| | |
|---|---|
| *access-list-name* | (Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric. |

## Command Default

No reset is initiated.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(23)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |
| 12.2(50)SY | This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed. |

## Usage Guidelines

The **clear ipv6 access-list**command is similar to the **clear ip access-list counters**command, except that it is IPv6-specific.

The **clear ipv6 access-list**command used without the *access-list-name*argument resets the match counters for all IPv6 access lists configured on the router.

This command resets the IPv6 global ACL hardware counters.

## Examples

The following example resets the match counters for the IPv6 access list named marketing:

```
Router# clear ipv6 access-list marketing
```

## Related Commands

| Command | Description |
|---|---|
| **hardware statistics** | Enables the collection of hardware statistics. |

| Command | Description |
|---|---|
| **ipv6 access-list** | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| **show ipv6 access-list** | Displays the contents of all current IPv6 access lists. |

# clear ipv6 inspect

To remove a specific IPv6 session or all IPv6 inspection sessions, use the **clear ipv6 inspect**command in privileged EXEC mode.

**clear ipv6 inspect** {**session** *session-number* | **all**}

## Syntax Description

| | |
|---|---|
| **session** *session-number* | Indicates the number of the session to clear. |
| **all** | Clears all inspection sessions. |

## Command Default

Inspection sessions previously configured are unaffected.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

## Examples

The following example clears all inspection sessions:

```
Router# clear ipv6 inspect all
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 inspect name** | Applies a set of inspection rules to an interface. |

# clear ipv6 snooping counters

To remove counter entries, use the **clear ipv6 snooping counters**command in privileged EXEC mode.

**clear ipv6 snooping counters** [**interface** *type number*]

## Syntax Description

| | |
|---|---|
| **interface** *type number* | (Optional) Clears the counter of entries that match the specified interface type and number. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |

## Usage Guidelines

The **clear ipv6 snooping counters**command removes counters from all the configured interfaces. You can use the optional **interface** *type number* keyword and argument to remove counters from the specified interface.

## Examples

The following example shows how to remove entries from the counter:

```
Router# clear
 ipv6 snooping counters
```

# clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

**clear kerberos creds**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Credentials are deleted when this command is issued.

Cisco supports Kerberos 5.

## Examples

The following example illustrates the **clear kerberos creds** command:

```
Router# show kerberos creds

Default Principal: chet@cisco.com
Valid Starting          Expires                 Service Principal
18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/CISCO.COM@CISCO.COM
Router# clear kerberos creds
Router# show kerberos creds

No Kerberos credentials.
```

## Related Commands

| Command | Description |
|---|---|
| **show kerberos creds** | Displays the contents of your credentials cache. |

# clear ldap server

To clear the TCP connection with the Lightweight Directory Access Protocol (LDAP) server, use the **clear ldap server** command in privileged EXEC mode.

**clear ldap server** *server-name* [**statistics**]

## Syntax Description

| | |
|---|---|
| *server-name* | LDAP server name. |
| **statistics** | (Optional) Clears the statistical information. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Usage Guidelines

Statistics details are not cleared when the server is cleared. To clear the statistics information, use the **statistics** keyword.

## Examples

The following example shows how to clear the statistical information:

```
Router# clear ldap server server1 statistics
```

## Related Commands

| Command | Description |
|---|---|
| **ldap server** | Defines an LDAP server and enters LDAP server configuration mode. |

# clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command in privileged EXEC mode.

**clear logging ip access-list cache**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(17d)SXB | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

## Examples

This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router#
clear logging ip access-list cache
```

## Related Commands

| Command | Description |
|---|---|
| **logging ip access-list cache (global configuration )** | Configures the OAL parameters globally. |
| **logging ip access-list cache (interface configuration )** | Enables an OAL-logging cache on an interface that is based on direction. |
| **show logging ip access-list** | Displays information about the logging IP access list. |

# clear parameter-map type protocol-info

To clear the Domain Name System (DNS) cache for name resolution of servers within a parameter map, use the **clear parameter-map type protocol-info** command in privileged EXEC mode.

**clear parameter-map type protocol-info dns-cache** *dns-name* [**ip-address** *ip-address*]

## Syntax Description

| | |
|---|---|
| **dns-cache** *dns-name* | Cache of the specified DNS server will be cleared. |
| **ip-address** *ip-address* | (Optional) Specified IP address is removed from the cache of the DNS server.<br>If an IP address is not specified, all IP addresses from the specified DNS server are cleared from the cache. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Examples

The following example shows how to clear the cache of the DNS server “sdsc.msg.yahoo.com:

```
Router#
clear parameter-map type protocol-info dns-cache sdsc.msg.yahoo.com
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type** | Creates or modifies a parameter map. |

# clear policy-firewall

To reset the information collected by the firewall, use the **clear policy-firewall** command in user EXEC or privileged EXEC mode.

**clear policy-firewall** {**session** [*session address* | **class-map** *class-map-name* | **policy-map** *policy-map-name*] | **stats** [*drop-counters*] | **summary-log** | **zone-pair**}

## Syntax Description

| | |
|---|---|
| **session** *session address* | Clears the session. |
| **class-map** *class-map-name* | Clears the class map. |
| **policy-map** *policy-map-name* | Clears the policy map. |
| **stats** [*drop-counters*] | Clears the statistics and the drop-counters. |
| **summary-log** | Clears the summary log. |
| **zone-pair** | Clears the zone-pair. |

## Command Default

The firewall information is not cleared.

## Command Modes

EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |

## Usage Guidelines

Use this command to clear the information that is collected by the firewall. The cleared counters include drop-counters, summary-log buffers, sessions and zone pairs.

## Examples

The following example shows how to clear the zone pair:

```
Router(mode-prompt
)# clear policy-firewall zone-pair
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-firewall config** | Displays the entire configuration of the firewall in the router. |
| **show policy-firewall sessions** | Displays the details of the firewall sessions. |
| **show policy-firewall stats** | Displays the statistics of all firewall activities in the router. |
| **show policy-firewall summary-log** | Displays the summary log of the firewall. |

# clear policy-firewall stats global

To reset the global statistics collected by the firewall, use the **clear policy-firewall stats global** command in user EXEC or privileged EXEC mode.

**clear policy-firewall stats global**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The firewall global statistics are not cleared.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

Use this command to clear the statistics collected by the firewall.

## Examples

The following example shows how to clear the global firewall statistics:

```
Router# clear policy-firewall stats global
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-firewall stats global** | Displays global firewall statistics. |

# clear policy-firewall stats vrf

To clear the policy firewall statistics at a VPN Routing and Forwarding (VRF) level, use the **clear policy-firewall stats vrf** command in privileged EXEC mode.

**clear policy-firewall stats vrf** *vrf-name*

## Syntax Description

| | |
|---|---|
| *vrf-name* | Name of the VRF. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |

## Examples

The following example shows how to clear the configured policy firewall VRF statistics:

```
Router# clear policy-firewall stats vrf vrf1
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-firewall stats vrf** | Displays VRF-level policy firewall statistics. |

# clear policy-firewall stats vrf global

To clear the global VPN Routing and Forwarding (VRF) policy firewall statistics, use the **clear policy-firewall stats vrf global** command in privileged EXEC mode.

**clear policy-firewall stats vrf global**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |

## Examples

The following example shows how to clear the global policy firewall statistics:

```
Router# clear policy-firewall stats vrf global
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-firewall stats vrf global** | Displays information about the global VRF firewall policies. |

# clear policy-firewall stats zone

To clear the policy firewall statistics at a zone level, use the **clear policy-firewall stats zone** command in privileged EXEC mode.

**clear policy-firewall stats zone** *zone-name*

## Syntax Description

| | |
|---|---|
| *zone-name* | Name of the zone. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |

## Examples

The following example shows how to clear the configured policy firewall zone statistics:

```
Router# clear policy-firewall stats zone zone1
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-firewall stats zone** | Displays policy firewall statistics at a zone level. |

# clear port-security

To delete configured secure MAC addresses and sticky MAC addresses from the MAC address table in the Priveleged EXEC configuration command mode, use the **clear port-security**command.

**clear port-security dynamic** [**address mac-addr** | **interface interface-id**] [**vlan vlan-id**]

## Syntax Description

| | |
|---|---|
| **address** *mac-addr* | (Optional) Deletes the specified secure MAC address or sticky MAC address. |
| **interface** *interface-id* | (Optional) Deletes all secure MAC addresses and sticky MAC addresses on the specified physical port or port channel. |
| **vlan** *vlan-id* | (Optional) Deletes the specified secure MAC address or sticky MAC address from the specified VLAN. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(18)SXE | The output of this command was changed to support sticky MAC addresses on the Supervisor Engine 720 only. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on negotiated trunks only.

If you enter the **clear port-security**command without adding any keywords or arguments, the switch removes all the secure MAC addresses and sticky MAC addresses from the MAC address table.

If you enter the **clear port-security dynamic interface***interface-id* command, all the secure MAC addresses and sticky MAC addresses on an interface are removed from the MAC address table.

You can verify that the information was deleted by entering the **show port-security** command.

## Examples

This example shows how to remove a specific secure address from the MAC address table:

```
Router# clear port-security dynamic address 0008.0070.0007
Router#
```

This example shows how to remove all the secure MAC addresses and sticky MAC addresses learned on a specific interface:

```
Router# clear port-security dynamic interface gigabitethernet0/1
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-security** | Displays information about the port-security setting. |
| switchport port-security mac-address | Adds a MAC address to the list of secure MAC addresses. |

# clear radius

To clear the RADIUS server information, use the **clear radius**command in privileged EXEC mode.

**clear radius** {**sg-stats** | **statistics**}

## Syntax Description

| | |
|---|---|
| **sg-stats** | Clears the RADIUS server group statistics. |
| **statistics** | Clears the RADIUS statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Examples

The following example shows how to clear the RADIUS statistics information:

```
Router# clear radius statistics
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server host** | Configures a RADIUS server host. |

# clear radius local-server

To clear the display on the local server or to unblock a locked username, use the **clear radius local-server**command in privileged EXEC mode.

**clear radius local-server** {**statistics** | **user** *username*}

## Syntax Description

| | |
|---|---|
| **statistics** | Clears the display of statistical information. |
| **user** | Unblocks the locked username specified. |
| *username* | Locked username. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200. |
| 12.3(11)T | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Examples

The following example shows how to unblock the locked username “smith”:

```
Router# clear radius local-server user smith
```

## Related Commands

| Command | Description |
|---|---|
| **block count** | Configures the parameters for locking out members of a group to help protect against unauthorized attacks. |
| **debug radius local-server** | Displays the debug information for the local server. |
| **group** | Enters user group configuration mode and configures shared setting for a user group. |
| **nas** | Adds an access point or router to the list of devices that use the local authentication server. |
| **radius-server host** | Specifies the remote RADIUS server host. |
| **radius-server local** | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| **reauthentication time** | Specifies the time after which access points or wireless-aware routers must reauthenticate the members of a group. |

| Command | Description |
|---|---|
| **show radius local-server statistics** | Displays statistics for a local network access server. |
| **ssid** | Specifies up to 20 SSIDs to be used by a user group. |

# clear webvpn nbns

To clear the NetBIOS name service (NBNS) cache on a SSL VPN gateway, use the **clear webvpn nbns** command in privileged EXEC mode.

**clear webvpn nbns** [**context** {*name* | **all**}]

## Syntax Description

| | |
|---|---|
| **context** | (Optional) Clears NBNS statistics for a specific context or all contexts. |
| *name* | Clears NBNS statistics for a specific context. |
| **all** | Clears NBNS statistics for all contexts. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Entering this command without any keywords or arguments clears all NBNS counters on the network device.

## Examples

The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

## Related Commands

| Command | Description |
|---|---|
| **clear webvpn session** | Clears remote users sessions on a SSL VPN gateway. |
| **clear webvpn stats** | Clears application and access counters on a SSL VPN gateway. |

# clear webvpn session

To clear SSL VPN remote user sessions, use the **clear webvpn session** command in privileged EXEC mode.

**clear webvpn session** [**user** *name*] **context** {*name* | **all**}

## Syntax Description

| | |
|---|---|
| **user** *name* | (Optional) Clears session information for a specific user. |
| **context** *name* \| **all** | Clears session information for a specific context or all contexts. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used to clear the session for either the specified remote user or all remote users in the specified context.

## Examples

The following example clears all session information:

```
Router# clear webvpn session context all
```

## Related Commands

| Command | Description |
|---|---|
| **clear webvpn nbns** | Clears the NBNS cache on a SSL VPN gateway. |
| **clear webvpn stats** | Clears application and access counters on a SSL VPN gateway. |

# clear webvpn stats

To clear (or reset) SSL VPN application and access counters, use the **clear webvpn stats** command in privileged EXEC mode.

**clear webvpn stats** [[**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**context** {*name* | **all**}]]

## Syntax Description

| | |
|---|---|
| **cifs** | (Optional) Clears Windows file share (CIFS) statistics. |
| **citrix** | (Optional) Clears Citrix application statistics. |
| **mangle** | (Optional) Clears URL mangling statistics. |
| **port-forward** | (Optional) Clears port forwarding statistics. |
| **sso** | (Optional) Clears statistics for Single SignOn (SSO) activities. |
| **tunnel** | (Optional) Clears Cisco AnyConnect VPN Client tunnel statistics. |
| **context** *name* \| **all** | (Optional) Clears information for either a specific context or all contexts. |

## Command Default

If no keywords are entered, all SSL VPN application and access counters are cleared.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(11)T | The **sso** keyword was added. |

## Usage Guidelines

This command is used to clear counters for Windows file shares, Citrix applications, URL mangling, application port forwarding, SSO, and Cisco AnyConnect VPN Client tunnels. The counters are cleared for either the specified context or all contexts on the SSL VPN gateway.

## Examples

The following example clears all statistics counters for all SSL VPN processes:

```
Router# clear webvpn stats
```

The following example clears statistics for SSO activities:

```
Router# clear webvpn stats sso
```

## Related Commands

| Command | Description |
|---|---|
| **clear webvpn nbns** | Clears the NBNS cache on a SSL VPN gateway. |
| **clear webvpn session** | Clears remote users sessions on a SSL VPN gateway. |

# clear xsm

To clear XML Subscription Manager (XSM) client sessions, use the **clear xsm** command in privileged EXEC mode.

**clear xsm** [**session** *number*]

## Syntax Description

| | |
|---|---|
| **session** | (Optional) Specifies an XSM client session to clear. |
| *number* | (Optional) ID number of the specific XSM client session to be cleared. |

## Command Default

No XSM client sessions are cleared.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(6)E | This command was introduced. |
| 12.2(9)YE | This command was integrated into Cisco IOS Release 12.2(9)YE. |
| 12.2(9)YO1 | This command was integrated into Cisco IOS Release 12.2(9)YO1. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command disconnects all active client sessions (such as with a VPN Device Manager [VDM]) on the XSM server, unless you state a specific session number. This command allows troubleshooting of the XSM server and its active clients by allowing individual clients to be disconnected. Use the **show xsm status** command to obtain specific session numbers.

When the optional **session** *number* keyword and argument are not used, the **clear xsm** command clears all XSM client sessions.

## Examples

The following example shows how to clear all XSM client sessions:

```
Router# clear xsm
```

The following example shows how to clear XSM client session 10:

```
Router# clear xsm session 10
```

## Related Commands

| Command | Description |
|---|---|
| **show xsm status** | Displays information and status about clients subscribed to the XSM server. |
| **xsm** | Enables XSM client access to the router. |

# clear zone-pair

To clear the policy map counters, inspect sessions, or the URL filter cache on a zone-pair, use the **clear zone-pair** command in privileged EXEC mode.

**clear zone-pair** [*zone-pair-name*] {**counter** | **inspect session** | **urlfilter cache**}

## Syntax Description

| | |
|---|---|
| *zone-pair-name* | (Optional) Name of the zone-pair on which counters, inspect sessions, or the uRL filter cache are cleared. |
| **counter** | Clears the policy-map counters. Resets the statistics of the inspect type policy map on the specified zone-pair. |
| **inspect session** | Deletes the inspect sessions on the specified zone-pair. |
| **urlfilter cache** | Clears the URL filter cache on the specified zone-pair. |

## Command Default

Disabled (it is not necessary to enter this command).

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(15)XZ | This command was implemented on the following platforms: Cisco 881 and Cisco 888. |

## Usage Guidelines

If you do not specify a zone-pair name, the policy map counters, sessions, or the URL filter cache are cleared for all the configured zone-pairs.

## Examples

The following example deletes the inspect sessions on the zp zone-pair:

```
Router# clear zone-pair zp inspect session
```

The following example clears the URL filter cache on the zp zone-pair.

```
Router# clear zone-pair zp urlfilter cache
```

# clid

To preauthenticate calls on the basis of the Calling Line IDentification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *password*]
**no clid** [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

## Syntax Description

| | |
|---|---|
| **if-avail** | (Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes. |
| **required** | (Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails. |
| **accept-stop** | (Optional) Prevents subsequent preauthentication elements such as ctype or dnis from being tried once preauthentication has succeeded for a call element. |
| **password** *password* | (Optional) Defines the password for the preauthentication element. The default password string is cisco. |

## Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

## Command Modes

AAA preauthentication configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |

## Usage Guidelines

You may configure more than one of the authentication, authorization and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

## Examples

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
 group radius
 clid required
```

## Related Commands

| Command | Description |
|---|---|
| **ctype** | Preauthenticates calls on the basis of the call type. |
| **dnis (RADIUS)** | Preauthenticates calls on the basis of the DNIS number. |
| **dnis bypass (AAA preauthentication configuration)** | Specifies a group of DNIS numbers that will be bypassed for preauthentication. |
| **group (RADIUS)** | Specifies the AAA RADIUS server group to use for preauthentication. |

# client

To specify a RADIUS client from which a device can accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

**client** {*hostname ip-address*} [**server-key** {**0** *string* | **6** *string* | **7** *string string*} | **vrf** *vrf-id*]
**no client** {*hostname ip-address*} [**server-key** {**0** *string* | **6** *string* | **7** *string string*} | **vrf** *vrf-id*]

## Syntax Description

| | |
|---|---|
| *hostname* | Hostname of the RADIUS client. |
| *ip-address* | IP address of the RADIUS client. |
| **server-key** | (Optional) Configures the RADIUS key to be shared between a device and a RADIUS client. |
| **0** *string* | Specifies that an unencrypted key follows.<br>• *string*—The unencrypted (clear text) shared key. |
| **6** *string* | Specifies that an encrypted key follows.<br>• *string*—The advanced encryption scheme [AES] encrypted key. |
| **7** *string* | Specifies that a hidden key follows.<br>• *string*—The hidden shared key. |
| *string* | The unencrypted (clear text) shared key. |
| **vrf** *vrf-id* | (Optional) Virtual routing and forwarding (VRF) ID of the client. |

## Command Default

CoA and disconnect requests are dropped.

## Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 15.4(1)T | This command was integrated into Cisco IOS Release 15.4(1)T. The **6** keyword was added. |

## Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the router can act as server.

## Examples

The following example shows how to configure the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

## Related Commands

| Command | Description |
|---|---|
| **aaa server radius dynamic-author** | Configures an ISG as a AAA server to facilitate interaction with an external policy server. |

# client authentication list

To configure Internet Key Exchange (IKE) extended authentication (Xauth) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list**command in ISAKMP profile configuration mode. To restore the default behavior, which is that Xauth is not enabled, use the **no** form of this command.

**client authentication list** *list-name*
**no client authentication list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration. |

## Command Default

No default behaviors or values

## Command Modes

ISAKMP profile configuration (config-isakmp-profile)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11.5) | Xauth no longer has to be disabled globally for it to be enabled on a profile basis. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Before configuring Xauth, you must set up an authentication list using AAA commands.

Xauth can be enabled on a profile basis if it has been disabled globally.

Effective with Cisco IOS Release 12.4(11.5), Xauth on either a server or client does not need to be disabled globally to enable it on profile basis.

## Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
 client authentication list xauthlist
```

The following example shows that Xauth has been disabled globally and enabled for the profile "nocerts":

```
no crypto xauth FastEthernet0/0
!
crypto isakmp policy 1
 encr aes
 group 14
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 14
crypto isakmp client configuration group HRZ
crypto isakmp client configuration group vpngroup
 key cisco123
 pool vpnpool
crypto isakmp profile cert_sig
   match identity group HRZ
   isakmp authorization list isakmpauth
   client configuration address respond
   client configuration group HRZ
crypto isakmp profile nocerts
   match identity group vpngroup
   client authentication list vpn-login
   isakmp authorization list isakmpauth
   client configuration address respond
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication login** | Sets AAA authentication at login. |

# client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address**command in ISAKMP profile configuration mode. To disable IKE configuraton mode, use the **no** form of this command.

**client configuration address** {**initiate** | **respond**}
**no client configuration address** {**initiate** | **respond**}

## Syntax Description

| | |
|---|---|
| **initiate** | Router will attempt to set IP addresses for each peer. |
| **respond** | Router will accept requests for IP addresses from any requesting peer. |

## Command Default

IKE configuration is not enabled.

## Command Modes

ISAKMP
profile configuration (config-isa-prof)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Before you can use this command, you must enter the **crypto isakmp profile** command.

## Examples

The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called “vpnprofile”:

```
crypto isakmp profile vpnprofile
 client configuration address initiate
 client configuration address respond
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp profile** | Defines an ISAKMP profile. |

# client configuration group

To associate a group with the peer that has been assigned an Internet Security Association Key Management Protocol (ISAKMP) profile, use the client configuration group command in crypto ISAKMP profile configuration mode. To disable this option, use the no form of this command.

**client configuration group** *group-name*
**no client configuration group** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the group to be associated with the peer. |

## Command Default

No default behavior or values

## Command Modes

Crypto ISAKMP profile configuration (conf-isa-prof)

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

The **client configuration group** command is used after the crypto map has been configured and the ISAKMP profiles have been assigned to them.

## Examples

The following example shows that the group “some_group” is to be associated with the peer:

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

## Related Commands

| Command | Description |
|---|---|
| **match certificate (ISAKMP)** | Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate. |

# client inside

To specify the inside interface for the FlexVPN client, use the **client inside** command in IKEv2 FlexVPN client profile configuration mode. To disable the inside interface, use the **no** form of this command.

**client inside** *interface-type number*
**no client inside** *interface type number*

## Syntax Description

| | |
|---|---|
| *interface-type number* | Interface type and number. |

## Command Default

The inside interface is not specified.

## Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Release 3.7S | This command was integrated into Cisco IOS XE Release 3.7S. |

## Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

You can specify more than one inside interface in a FlexVPN client profile. The inside interfaces can be shared across FlexVPN client profiles.



**Note** Enabling this command is optional. Any changes to this command terminates the active session.

## Examples

The following example shows how to specify the inside interface:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# peer 1 10.0.0.1
Router(config-ikev2-flexvpn)# client inside Ethernet 1
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 client flexvpn** | Defines an IKEv2 FlexVPN client profile. |

# client pki authorization list

To specify the authorization list of AAA servers that will be used to obtain per-user AAA attributes on the basis of the username that is constructed from the certificate, use the **client pki authorization list** command in crypto ISAKMP profile configuration mode. To disable the list name, use the **no** form of this command.

**client pki authorization list** *listname*
**no client pki authorization list** *listname*

## Syntax Description

| | |
|---|---|
| *listname* | Definition of the argument needed, including syntax-level defaults, if any. |

## Command Default

User attributes are not pushed to the remote device.

## Command Modes

Crypto ISAKMP profile configuration (config-isakmp-profile)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is used inside the crypto Internet Security Association and Key Management Protocol (ISAKMP) profile.

## Examples

The following example shows that user attributes are to be obtained from the AAA server (list name "usrgrp") and pushed to the remote device:

```
crypto isakmp profile ISA-PROF
   match certificate CERT-MAP
   isakmp authorization list usrgrp
   client pki authorization list usrgrp
   client configuration address respond
   client configuration group pkiuser
   virtual-template 2
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp profile** | Defines an ISAKMP profile and audits IPsec user sessions. |

# client recovery-check interval

To set the interval of time for the client group member (GM) to monitor for control-plane errors, use the **client recovery-check interval** command in GDOI group configuration mode. To remove the control-plane error monitoring, use the **no** form of this command.

**client recovery-check interval** *interval*
**no client recovery-check interval** *interval*

## Syntax Description

| | |
|---|---|
| *interval* | Specifies the waiting period in seconds between consecutive recovery registrations. The range is from 100 to 1000 seconds. |

## Command Default

Control-plane error monitoring is disabled.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

| Release | Modification |
|---|---|
| 15.3(3)M | This command was introduced. |

## Usage Guidelines

Use the **client recovery-check interval** command to ensure GMs reactively try to recover from data plane errors, such as invalid stateful packet inspection (SPI) and Time-Based Anti-Replay (TBAR) errors, by registering to the configured key servers (KSs) to obtain the latest policies.

## Examples

The following example shows how to enable the GM to monitor for control-plane errors every 300 seconds:

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# client recovery-check interval 300
```

## Related Commands

| Command | Description |
|---|---|
| **crypto gdoi group** | Creates a GDOI group and enters GDOI group configuration mode. |

# client connect

To assign a tunnel interface to the FlexVPN client, use the **client connect** command in IKEv2 FlexVPN client profile configuration mode. To remove the tunnel interface, use the **no** form of this command.

**client connect tunnel** *number*
**no client connect tunnel** *number*

## Syntax Description

| | |
|---|---|
| **tunnel** | Tunnel interface. |
| *number* | Tunnel interface number. |

## Command Default

A tunnel interface is not assigned to the FlexVPN client.

## Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Release 3.7S | This command was integrated into Cisco IOS XE Release 3.7S. |

## Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** and the **interface** command with the **tunnel** keyword.

You can configure only one tunnel interface for a FlexVPN client profile.

**Note** Any changes to this command terminates the active session.

## Examples

The following example shows how to assign the tunnel interface 1 to the FlexVPN client profile "client1":

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# client inside Ethernet 1
Router(config-ikev2-flexvpn)# client connect tunnel 1
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 client flexvpn** | Defines an IKEv2 FlexVPN client profile. |
| **interface** | Specifies an interface. |

# client rekey encryption

To set the client acceptable rekey ciphers for the key-encryption-key (KEK), use the **client rekey encryption** command in GDOI group configuration mode. To remove the client acceptable rekey ciphers, use the **no** form of this command.

**client rekey encryption** *cipher* [**...** [*cipher*]]
**no client rekey encryption**

## Syntax Description

| | |
|---|---|
| *cipher* | Any of the following ciphers:<br>• **3des-cbc** —Specifies triple Data Encryption Standard (3DES) in Cipher-block chaining (CBC) mode (no longer recommended).<br>• **aes 128** —Specifies 128-bit Advanced Encryption Standard (AES).<br>• **aes 192** —Specifies 192-bit AES.<br>• **aes 256** —Specifies 256-bit AES.<br>• **des-cbc** —Specifies DES in CBC mode (no longer recommended). |

## Command Default

Any cipher assigned by the key server is accepted.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.4.1 | This command was introduced. |
| Cisco IOS Release 15.1(1)T | This command was integrated into Cisco IOS Release 15.1(1)T. |

## Usage Guidelines



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use the **client rekey encryption** command to specify the acceptable ciphers for KEK. Multiple ciphers can be specified. If a cipher is not set using this command, the cipher assigned by the key server is accepted.

## Examples

The following example shows how to set the acceptable ciphers for KEK:

```
Router# configure terminal
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# identity number 1111
```

```
Router(config-gdoi-group)# server address ipv4 192.10.2.10
Router(config-gdoi-group)# client rekey encryption aes 128 aes 192 aes 256
```

## Related Commands

| Command | Description |
|---|---|
| **crypto gdoi group** | Identifies a GDOI group and enters GDOI group configuration mode. |

# client rekey hash

To set acceptable hash algorithms for rekey message signing, use the **client rekey hash** command in GDOI group configuration mode. To remove acceptable hash algorithms, use the **no** form of this command.

**client rekey hash**
*hash1* [...[*hash4*]]
**no client rekey hash**
*hash1* [...[*hash4*]]

## Syntax Description

| | |
|---|---|
| *hash* | Hash for rekey message signing. You can use any combination of the following values: **sha**, **sha256**, **sha384**, and **sha512**. |

## Command Default

Any hash selected by the key server (KS) is accepted.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.4.1 | This command was introduced. |
| 15.1(1)T | This command was integrated into Cisco IOS Release 15.1(1)T. |
| 15.2(4)M | This command was modified. The **sha256**, **sha384**, and **sha512** keywords were added. |

## Usage Guidelines

Use the **client rekey hash** command to select the acceptable hash for the rekey message signing. If a hash is not set using this command, the hash selected by the KS is accepted.

Suite B requires SHA-256, SHA-384, or SHA-512. Suite B is a set of cryptographic algorithms that includes Galois Counter Mode Advanced Encryption Standard (GCM-AES) as well as algorithms for hashing, digital signatures, and key exchange.

## Examples

The following example shows how to set the acceptable hash for rekey message signing:

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# identity number 1111
Device(config-gdoi-group)# server address ipv4 192.10.2.10
Device(config-gdoi-group)# client rekey hash sha512
```

## Related Commands

| Command | Description |
|---|---|
| **crypto gdoi group** | Identifies a GDOI group and enters GDOI group configuration mode. |

# client transform-sets

To specify up to 6 acceptable transform-set tags used by the traffic-encryption-key (TEK) for data encryption or authentication, use the **client transform-sets**command in GDOI group configuration mode. To remove the acceptable transform-set tags, use the **no** form of this command.

**client transform-sets** *transform-set-name1* [**. . .** [*transform-set-name6*]]
**no client transform-sets**

## Syntax Description

| | |
|---|---|
| *transform-set-name* | Transform-tags used by the TEK for data encryption or authentication. |

## Command Default

The transform-set selected by the key server is accepted.

## Command Modes

GDOI group configuration (config-gdoi-group)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.4.1 | This command was introduced. |
| Cisco IOS Release 15.1(1)T | This command was integrated into Cisco IOS Release 15.1(1)T. |

## Usage Guidelines

Use the **client transform-sets** command to specify up to 6 transform-set tags used by the TEK for data encryption or authentication. If this command is not issued, the transform-set selected by the key server is accepted. The security protocol configured in the transform set must be Encapsulating Security Payload (ESP), which is the only protocol supported by GETVPN in Cisco IOS XE Release 2.4.1.

## Examples

The following example shows how to set the transform-set tags used by TEK for data encryption or authentication:

```
Router# configure terminal
Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac
Router(cfg-crypto-trans)# exit
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# client transform-sets g1
```

## Related Commands

| Command | Description |
|---|---|
| **crypto gdoi group** | Identifies a GDOI group and enters GDOI group configuration mode. |
| **crypto ipsec transform-set** | Defines a transform set--an acceptable combination of security protocols and algorithms. |

# commands (view)

To add commands or an interface to a command-line interface (CLI) view, use the **commands**command in view configuration mode. To delete a command or an interface from a CLI view, use the **no** form of this command.

**Syntax for Adding and Deleting Commands to a View**
**commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]
**no commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

**Syntax for Adding and Deleting Interfaces to a View**
**commands** *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *name*] [*command*]
**no commands** *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *name*] [*command*]

## Syntax Description

| | |
|---|---|
| *parser-mode* | Mode in which the specified command exists. See the table in the "Usage Guidelines" section for a list of available options for this argument. |
| **include** | Adds a specified command or a specified interface to the view and allows the same command or interface to be added to a view. |
| **include-exclusive** | Adds a specified command or a specified interface to the view and excludes the same command or interface from being added to all other views. |
| **exclude** | Denies access to commands in the specified parser mode.<br>**Note**<br>This keyword is available only for command-based views. |
| **all** | (Optional) A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface within a specified interface to be part of the view. |
| *command* | (Optional) Command that is added to the view.<br>**Note**<br>If no commands are specified, all commands within the specified parser mode are included or excluded, as appropriate. |
| **interface** *name* | (Optional) Interface that is added to the view. |

## Command Default

If this command is not enabled, a view will not have adequate information to deny or allow access to users.

## Command Modes

View configuration (config-view)

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.3(11)T | The **exclude** keyword and the **interface** *interface-name* option were added. |

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

If a network administrator does not enter a specific command (via the *command* argument) or interface (via the **interface** *interface-name* option), users are granted access (via the **include** or **include-exclusive** keyword) or denied access (via the **exclude** keyword) to all commands within the specified parser mode.

### parser-mode Options

The table below shows some of the keyword options for the *parser-mode*argument in the **commands**command. The available mode keywords vary depending on your hardware and software version. To display a list of available mode options on your system, use the **commands ?**command.

***Table 19: parser-mode Argument Options***

| Command | Description |
|---|---|
| **accept-dialin** | VPDN accept-dialin group configuration mode |
| **accept-dialout** | VPDN accept-dialout group configuration mode |
| **address-family** | Address family configuration mode |
| **alps-ascu** | ALPS ASCU configuration mode |
| **alps-circuit** | ALPS circuit configuration mode |
| **atm-bm-config** | ATM bundle member configuration mode |
| **atm-bundle-config** | ATM bundle configuration mode |
| **atm-vc-config** | ATM virtual circuit configuration mode |
| **atmsig_e164_table_mode** | ATMSIG E164 Table |
| **cascustom** | Channel-associated signaling (cas) custom configuration mode |
| **config-rtr-http** | RTR HTTP raw request configuration mode |
| **configure** | Global configuration mode |
| **controller** | Controller configuration mode |
| **crypto-map** | Crypto map configuration mode |
| **crypto-transform** | Crypto transform configuration mode |
| **dhcp** | DHCP pool configuration mode |
| **dspfarm** | DSP farm configuration mode |

| Command | Description |
|---|---|
| **exec** | EXEC mode |
| **flow-cache** | Flow aggregation cache configuration mode |
| **gateway** | Gateway configuration mode |
| **interface** | Interface configuration mode |
| **interface-dlci** | Frame Relay DLCI configuration mode |
| **ipenacl** | IP named extended access-list configuration mode |
| **ipsnacl** | IP named simple access-list configuration mode |
| **ip-vrf** | Configure IP VRF parameters |
| **lane** | ATM Lan Emulation Lecs Configuration Table |
| **line** | Line configuration mode |
| **map-class** | Map-class configuration mode |
| **map-list** | Map-list configuration mode |
| **mpoa-client** | MPOA client |
| **mpoa-server** | MPOA server |
| **null-interface** | Null interface configuration mode |
| **preaut** | AAA Preauth definitions |
| **request-dialin** | VPDN accept-dialin group configuration mode |
| **request-dialout** | VPDN accept-dialout group configuration mode |
| **route-map** | Route-map configuration mode |
| **router** | Router configuration mode |
| **rsvp_policy_local** | RSVP local policy configuration mode |
| **rtr** | RTR entry configuration mode |
| **sg-radius** | RADIUS server group definition |
| **sg-tacacs+** | TACACS+ server group |
| **sip-ua** | SIP UA configuration mode |
| **subscriber-policy** | Subscriber policy configuration mode |
| **tcl** | Tcl mode |
| **tdm-conn** | TDM connection configuration mode |

| Command | Description |
|---|---|
| **template** | Template configuration mode |
| **translation-rule** | Translation Rule configuration mode |
| **vc-class** | VC class configuration mode |
| **voiceclass** | Voice class configuration mode |
| **voiceport** | Voice configuration mode |
| **voipdialpeer** | Dial peer configuration mode |
| **vpdn-group** | VPDN group configuration mode |

## Examples

The following example shows how to add the privileged EXEC command **show version** to both CLI views "first" and "second." Because the **include** keyword was issued, the **show version** command can be added to both views.

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include show version
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include show version
```

The following example shows how to allow users in the view "first" to execute all commands that start with the word "show" except the **show interfaces** command, which is excluded by the view "second":

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include all show
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include-exclusive show interfaces
```

## Related Commands

| Command | Description |
|---|---|
| **parser view** | Creates or changes a CLI view and enters view configuration mode. |
| **secret 5** | Associates a CLI view or a superview with a password. |

# configuration url

To specify on a server the URL that an Easy VPN remote device must use to get a configuration in a Mode Configuration Exchange, use the **configuration url** command in global configuration or IKEv2 authorization policy configuration mode. To delete the URL, use the **no** form of this command.

**configuration url** *url*
**no configuration url** *url*

## Syntax Description

| | |
|---|---|
| *url* | Specifies the URL the Easy VPN remote device must use to get the configuration from the server.<br>• The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file. |

## Command Default

An Easy VPN remote device cannot request a configuration from a server in a Mode Configuration Exchange.

## Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

After the server "pushes" the URL to a Cisco Easy VPN remote device, the remote device can download the content located at the URL site and apply the configuration content to its running configuration.

Before this command can be configured, the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command must already have been configured.

## Examples

The file served by the configuration URL should have a Cisco IOS command-line interface( CLI) listing. The listing can have an optional "transient" section. The keyword to begin the transient section is "!%transient," and the keyword should be on a single line. A persistent section can be optionally identified by the keyword "!%persistent," also shown on a single line. An example of a CLI listing follows:

```
ip cef
cdp advertise-v2
!%transient
ip domain-name example.com
ntp server 10.2.3.4
ntp update-calendar
```

In the above example, the first two lines stay in the configuration even after the tunnel is disconnected (but they are not written into the nonvolatile configuration). The last three lines are effective only as long as the tunnel is "up."

The following example shows that a server has specified the URL the Easy VPN remote device must use to download the URL:

```
crypto isakmp client configuration group group1
 configuration url http://10.10.8.8/easy.cfg
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 authorization policy** | Specifies an IKEv2 authorization policy group. |
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |

# configuration version

To specify on a server the version that a Cisco Easy VPN remote device must use to get a particular configuration in a Mode Configuration Exchange, use the **configuration version** command in global configuration or IKEv2 authorization policy configuration mode. To delete the version number, use the **no** form of this command.

**configuration version** *version-number*
**no configuration version** *version-number*

## Syntax Description

| | |
|---|---|
| *version-number* | Specifies the version of the configuration.<br>• The version number will be an unsigned integer in the range 1 through 32767. |

## Command Default

A version number is not sent.

## Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

Before this command can be configured, the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command must already have been configured.

## Examples

The following example shows that a server has specified the version number a Cisco Easy VPN remote device must use to obtain that particular configuration version:

```
crypto isakmp client configuration group group1
 configuration version 10
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 authorization policy** | Specifies an IKEv2 authorization policy group. |
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |

# config-exchange

To enable the configuration exchange options, use the **config-exchange** command in IKEv2 profile configuration mode. To disable sending, use the **no** form of this command.

**config-exchange** {**request** | **set** {**accept** | **send**}}
**no config-exchange** {**request** | **set** {**accept** | **send**}}

## Syntax Description

| | |
|---|---|
| **request** | Enables configuration exchange request. |
| **set** | Enables configuration exchange request set options. |
| **accept** | Accepts configuration exchange request set. |
| **send** | Enables sending of configuration exchange set. |

## Command Default

The configuration exchange options is enabled by default.

## Command Modes

IKEv2 profile configuration (config-ikev2-profile)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. This command replaces the **config-mode set** command. |

## Usage Guidelines

Before using this command, you must first configure the **crypto ikev2 profile** command. Use this command to enable the exchange of configuration options. The acceptance of configuration exchange options is enabled by default.

## Examples

The following example show how to set the acceptance of configuration exchange request for the IKEv2 profile “profile2”:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# config-exchange set accept
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 profile** | Defines an IKEv2 profile. |

# config-mode set



**Note** Effective with Cisco IOS Release 15.2(2)T, the **config-mode set** command is replaced by the **config-exchange** command. See the **config-exchange** command for more information.

To enable sending the configuration mode set, use the **config-mode set** command in IKEv2 profile configuration mode. To disable sending, use the **no** form of this command.

**config-mode set**
**no config-mode set**

## Syntax Description

This command has no keywords or arguments.

## Command Default

The configuration mode set is enabled by default.

## Command Modes

IKEv2 profile configuration (config-ikev2-profile)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| 15.2(2)T | This command was replaced by the **config-exchange** command. |

## Usage Guidelines

Before using this command, you must first configure the crypto ikev2 profile command. Use this command to enable sending of configuration mode set. The acceptance of configuration mode set is enabled by default.

## Examples

The following example show how to configure the configuration mode set for the IKEv2 profile "profile1":

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# config-mode set
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 profile** | Defines an IKEv2 profile. |

# connect

To connect the FlexVPN client to the tunnel, use the **connect** command in IKEv2 FlexVPN client profile configuration mode. To disable the connection, use the **no** form of this command.

**connect** {**manual** | **auto** | **track** *track-number* [**up** | **down**]}
**no connect** {**manual** | **auto** | **track**}

## Syntax Description

| | |
|---|---|
| **manual** | Manually establishes connection with the tunnel. |
| **auto** | Automatic connection. This is the default mode. |
| **track** *track-number* | Estalishes a connection based on state of the track object. |
| **up** | Establishes a connection when the state of the track object is up. |
| **down** | Establishes a connection when the state of the track object is down. |

## Command Default

The default connect mode is auto.

## Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Release 3.7S | This command was integrated into Cisco IOS XE Release 3.7S. |

## Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

**Note** Any changes to this command terminates the active session.

## Examples

The following examples shows how to set the tunnel connection to auto.

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# peer 1 10.0.0.1
Router(config-ikev2-flexvpn)# connect track 10 up
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 client flexvpn** | Defines an IKEv2 FlexVPN client profile. |

# content-length

To permit or deny HTTP traffic through the firewall on the basis of message size, use the **content-length** command in appfw-policy-http configuration mode. To remove message-size limitations from your configuration, use the **no** form of this command.

**content-length** {**min** *bytes* **max** *bytes* | **min** *bytes* | **max** *bytes*} **action** {**reset** | **allow**} [**alarm**]
**no content-length** {**min** *bytes* **max** *bytes* | **min** *bytes* | **max** *bytes*} **action** {**reset** | **allow**} [**alarm**]

## Syntax Description

| | |
|---|---|
| **min** *bytes* | Minimum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535. |
| **max** *bytes* | Maximum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535. |
| action | Messages whose size do not meet the minimum or exceed the maximum number of bytes are subject to the specified action (**reset** or **allow**). |
| **reset** | Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection. |
| **allow** | Forwards the packet through the firewall. |
| **alarm** | (Optional) Generates system logging (syslog) messages for the given action. |

## Command Default

If this command is not enabled, message size is not considered when permitting or denying HTTP messages.

## Command Modes

appfw-policy-http
configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

All messages exceeding the specified content-length range, will be subjected to the configured action (**reset** or **allow**).

## Examples

The following example, which shows how to define the HTTP application firewall policy “mypolicy,” will not permit HTTP messages longer than 1 byte. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
```

```
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

# content-scan out

**Note** Effective with Cisco IOS Release 15.4(2)T, the **content-scan out** command is replaced by the **cws out** command. See the **cws out** command for more information.

To enable content scanning on an egress interface, use the **content-scan out** command in interface configuration mode. To disable content scanning, use the **no** form of this command.

**content-scan out**
**no content-scan out**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Content scanning is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T1 | This command was introduced. |
| 15.4(2)T | This command was replaced by the **cws out** command. |

## Usage Guidelines

The content scanning process redirects client web traffic to ScanSafe. Content scanning is enabled on an Internet-facing WAN interface to protect the web traffic going out.

In case you enable content scanning on a interface that has Wide Area Application Services (WAAS) configured, you must not apply both the WAAS and the content scanning feature on the same TCP session.

## Examples

The following example shows how to enable content scanning on a Gigabit Ethernet interface:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# content-scan out
```

## Related Commands

| Command | Description |
|---|---|
| **content-scan whitelisting** | Enables content scan whitelisting and enters content-scan whitelisting configuration mode. |
| **interface** | Configures an interface and enters interface configuration mode. |

# content-scan whitelisting



**Note** Effective with Cisco IOS Release 15.4(2)T, the **content-scan whitelisting** command is replaced by the **cws whitelisting** command. See the **cws whitelisting** command for more information.

To enable approved listing of incoming traffic and to enter content-scan allowed listing configuration mode, use the **content-scan whitelisting** command in global configuration mode. To disable the approved listing of traffic, use the **no** form of this command.

**content-scan whitelisting**
**no content-scan whitelisting**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Allowed listing of traffic is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T1 | This command was introduced. |
| 15.4(2)T | This command was replaced by the **cws whitelisting** command. |

## Usage Guidelines

An approved list contains entities that are provided a particular privilege, service, mobility, access, or recognition. An approved list means to grant access.

The web traffic that you have configured for an approved list will bypass the content scanning by ScanSafe.

## Examples

The following example shows how to enable content scan to create an approved list and enter content-scan allowed listing configuration mode:

```
Device(config)# content-scan whitelisting
Device(config-cont-scan-wl)#
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type content-scan global** | Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode. |

# content-type-verification

To permit or deny HTTP traffic through the firewall on the basis of content message type, use the **content-type-verification** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

**content-type-verification** [**match-req-resp**] **action** {**reset** | **allow**} [**alarm**]
**no content-type-verification** [**match-req-resp**] **action** {**reset** | **allow**} [**alarm**]

## Syntax Description

| | |
|---|---|
| **match-req-resp** | (Optional) Verifies the content type of the HTTP response against the accept field of the HTTP request. |
| action | Messages that match the specified content type are subject to the specified action (**reset** or **allow**). |
| **reset** | Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection. |
| **allow** | Forwards the packet through the firewall. |
| **alarm** | (Optional) Generates system logging (syslog) messages for the given action. |

## Command Default

If this command is not issued, all traffic will be allowed.

## Command Modes

appfw-policy-http
configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

After the **content-type-verification** command is issued, all HTTP messages are subjected to the following inspections:

- Verify that the content type of the message header is listed as a supported content type. (See the table below.)
- Verify that the content type of the header matches the content of the message data or entity body portion of the message.

The table below contains a list of supported content types.

***Table 20: HTTP Header Supported Content Types***

| Supported Content Types |
|---|
| audio/* |
| audio/basic |

| Supported Content Types |
|---|
| audio/midi |
| audio/mpeg |
| audio/x-adpcm |
| audio/x-aiff |
| audio/x-ogg |
| audio/x-wav |
| application/msword |
| application/octet-stream |
| application/pdf |
| application/postscript |
| application/vnd.ms-excel |
| application/vnd.ms-powerpoint |
| application/x-gzip |
| application/x-java-arching |
| application/x-java-xm |
| application/zip |
| image/* |
| image/cgf |
| image/gif |
| image/jpeg |
| image/png |
| image/tiff |
| image/x-3ds |
| image/x-bitmap |
| image/x-niff |
| image/x-portable-bitmap |
| image/x-portable-greymap |
| image/x-xpm |

| Supported Content Types |
|---|
| text/* |
| text/css |
| text/html |
| text/plain |
| text/richtext |
| text/sgml |
| text/xmcd |
| text/xml |
| video/* |
| video/-flc |
| video/mpeg |
| video/quicktime |
| video/sgi |
| video/x-avi |
| video/x-fli |
| video/x-mng |
| video/x-msvideo |

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
```

```
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

# control

To configure the control interface type and number for a redundancy group, use the **control**command in redundancy application group configuration mode. To remove the control interface for the redundancy group, use the **no** form of this command.

**control** *interface-type interface-number* **protocol** *id*
**no control**

## Syntax Description

| | |
|---|---|
| *interface-type* | Interface type. |
| *interface-number* | Interface number. |
| **protocol** | Specifies redundancy group protocol media. |
| *id* | Redundancy group protocol instance. The range is from 1 to 8. |

## Command Default

The control interface is not configured.

## Command Modes

Redundancy application group configuration (config-red-app-grp)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.1S | This command was introduced. |

## Examples

The following example shows how to configure the redundancy group protocol media and instance for the control Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# control GigabitEthernet 0/0/0 protocol
 1
```

## Related Commands

| Command | Description |
|---|---|
| **application redundancy** | Enters redundancy application configuration mode. |
| **authentication** | Configures clear text authentication and MD5 authentication for a redundancy group. |
| **data** | Configures the data interface type and number for a redundancy group. |
| **group(firewall)** | Enters redundancy application group configuration mode. |
| **name** | Configures the redundancy group with a name. |
| **preempt** | Enables preemption on the redundancy group. |

| Command | Description |
| --- | --- |
| **protocol** | Defines a protocol instance in a redundancy group. |

# copy (consent-parameter-map)

To configure a consent page to be downloaded from a file server, use the **copy** command in parameter-map type consent configuration mode.

**copy** *src-file-name dst-file-name*

## Syntax Description

| | |
|---|---|
| *src-file-name* | Source file location in which the specified file will be retrieved. The source file location must b e TFTP; for example, tftp://10.1.1.1/username/myfile. |
| *dst-file-name* | Destination location in which a copy of the file will be stored. The destination file should be copied to Flash; for example, flash. username .html. |

## Command Default

The consent page that is specified via the default parameter-map will be used.

## Command Modes

Parameter-map-type consent (config-profile)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

Use the **copy** command to transfer a file (consent web page) from an external server to a local file system on a device. Thus, the file name specified via the **copy** command is retrieved from the destination file location and displayed to the end user as the consent page.

When a consent webpage is displayed to an end user, the filename specified via the **file** command is used. If the file command is not configured, the destination location specified via the **copy** command is used .

## Examples

In the following example, both parameter maps are to use the consent file "tftp://192.168.104.136/consent_page.html" and store it in "flash:consent_page.html":

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

## Related Commands

| Command | Description |
|---|---|
| **file (consent-parameter-map)** | Specifies a local filename that is to be used as the consent webpage. |

# copy idconf

To load a signature package in Cisco IOS Intrusion Prevention System (IPS), use the **copy idconf**command in EXEC mode.

**copy** *url* **idconf**

## Syntax Description

| | |
|---|---|
| *url* | Specifies the location from which the router loads the signature file.<br>Available URL locations are as follows:<br>• Local flash, such as flash:sig.xml<br>• FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml<br>• rcp, such as rcp://myuser@rcp_server/sig.xml<br>• TFTP server, such as tftp://tftp_server/sig.xml |

## Command Default

None

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Use the **copy** *url* **idconf**command to load a signature package into Cisco IOS IPS. You may wish to load a new signature package into Cisco IOS IPS if a signature (or signatures) with the current signature file is not providing your network with adequate protection from security threats. After the signature package has been loaded into the router, Cisco IOS IPS saves all signature information to the location specified via the **ip ips config location** command.

Signatures are loaded into the scanning table on the basis of importance. Parameters such as signature severity, signature fidelity rating, and time lapsed since signatures were released enable Cisco IOS IPS to compile the most important signatures first, followed by less important signatures, thereby, creating a load order and prioritizing which signatures are loaded first.



**Note** The **copy** *url* **idconf** command replaces the **copy ips-sdf** command.

## Examples

The following example shows how to load a signature package into Cisco IOS IPS from the location "flash:IOS-S258-CLI-kd.pkg":

```
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13
engines
```

```
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
 engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms - packets
 for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for this
 engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this signature
 is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets for
 this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets for
 this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
 this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
```

*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms

## Related Commands

| Command | Description |
|---|---|
| **ip ips config-location** | Specifies the location in which the router will save signature information. |

# copy ips-sdf

**Note** In Cisco IOS Release 12.4(11)T, the **copy ips-sdf** command was replaced with the **copy idconf** command. For more information, see the **copy idconf** command.

To load or save the signature definition file (SDF) in the router, use the **copy ips-sdf**command in EXEC mode.

**Syntax for Loading the SDF**
**copy** [**/erase**]*url* **ips-sdf**

**Syntax for Saving the SDF**
**copy ips-sdf** *url*

## Syntax Description

| | |
|---|---|
| **/erase** | (Optional) Erases the current SDF in the router before loading the new SDF.<br>**Note**<br>This option is typically available only on platforms with limited memory. |
| *url* | Description for the *url* argument is one of the following options:<br>• If you want to load the SDF in the router, the *url* argument specifies the location in which to search for the SDF.<br>• If you are saving the SDF, the *url* argument represents the location in which the SDF is saved after it has been generated.<br>Regardless of what option the URL is used for, available URL locations are as follows:<br>• local flash, such as flash:sig.xml<br>• FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml<br>• rcp, such as rcp://myuser@rcp_server/sig.xml<br>• TFTP server, such as tftp://tftp_server/sig.xml |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.4(11)T | This command was replaced with the **copy idconf** command. |

## Usage Guidelines

**Loading Signatures From the SDF**

Issue the **copy** *url* **ips-sdf** command to load the SDF in the router from the location specified via the *url* argument. When the new SDF is loaded, it is merged with the SDF that is already loaded in the router, unless the **/erase** keyword is issued, which overwrites the current SDF with the new SDF.

Cisco IOS Intrusion Prevention System (IPS) will attempt to retrieve the SDF from each specified location in the order in which they were configured in the startup configuration. If Cisco IOS IPS cannot retrieve the signatures from any of the specified locations, the built-in signatures will be used.

If the **no ip ips sdf built-in** command is used, Cisco IOS IPS will fail to load. IPS will then rely on the configuration of the **ip ips fail**command to either fail open or fail closed.

**Note** For Cisco IOS Release 12.3(8)T, the SDF should be loaded directly from Flash.

After the signatures are loaded in the router, the signature engines are built. Only after the signature engines are built can Cisco IOS IPS beginning scanning traffic.

**Note** Whenever signatures are replaced or merged, the router is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built. Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.

The **ip sdf ips location** command can also be used to load the SDF. However, unlike the **copy ips-sdf**command, this command does not force and immediately load the signatures. Signatures are not loaded until the router reboots or IPS is initially applied to an interface (via the **ip ips**command).

**Saving a Generated or Merges SDF**

Issue the **copy ips-sdf** *url* command to save a newly created SDF file to a specified location. The next time the router is reloaded, IPS can refer to the SDF from the saved location by including the **ip ips sdf location** command in the configuration.

**Tip** It is recommended that you save the SDF back out to Flash. Also, you should save the file to a different name than the original attack-drop.sdf file; otherwise, you risk loosing the original file.

## Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the reload command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
```

```
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
```

exit

## Related Commands

| Command | Description |
|---|---|
| **ip ips sdf location** | Specifies the location in which the router should load the SDF. |

# consent email

To request a user's e-mail address on the consent login web page, use the **consent email** command in parameter map webauth configuration mode. To remove the consent parameter file from the map, use the **no** form of this command.

**consent email**
**no consent email**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The e-mail address is not requested on the consent login page.

## Command Modes

Parameter map webauth configuration (config-params-parameter-map)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2SE | This command was introduced. |

## Usage Guidelines

Use the **consent email** command to display a text box on the consent login page prompting the user to enter his or her e-mail address for identification. The device sends this e-mail address to the authentication, authorization, and accounting (AAA) server instead of sending the client's MAC address.

The consent feature allows you to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent web page. This web page lists the terms and conditions under which the organization is willing to grant access to end users. Users can connect to the network only after they accept the terms on the consent web page.

If you create a parameter map with the **type** command set to consent, the device does not prompt the user for his or her username and password credentials. Users instead get a choice of two radio buttons: accept or do not accept. For accounting purposes, the device sends the client's MAC address to the AAA server if no username is available (because consent is enabled).

This command is supported in named parameter maps only.

## Examples

The following example shows how to enable the consent e-mail feature in a parameter map:

```
parameter-map type webauth PMAP_1
 type consent
 consent email
 banner file flash:consent_page.htm
```

## Related Commands

| Command | Description |
|---|---|
| **banner** (parameter-map webauth) | Displays a banner on the web-authentication login web page. |
| **custom-page** | Displays custom web pages during web authentication login. |
| **type** (parameter-map webauth) | Defines the methods supported by a parameter map. |

# crl

To specify the certificate revocation list (CRL) query and CRL cache options for the public key infrastructure (PKI) trustpool, use the **crl** command in ca-trustpool configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

**crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}
**no crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}

## Syntax Description

| | |
|---|---|
| **cache** | Specifies CRL cache options. |
| **delete-after** | Removes the CRL from cache after a timeout. |
| *minutes* | The number of minutes from 1 to 43200 to wait before deleting CRL from cache. |
| **none** | Specifies that CRLs are not cached. |
| **query** *url* | Specifies the URL published by the certification authority (CA) server to query the CRL. |

## Command Default

The CRL is not queried and no CRL cache parameters are configured.

## Command Modes

Ca-trustpool configuration (ca-trustpool)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

The **crl query** command is used if the CDP is in Lightweight Directory Access Protocol (LDAP) form, which means that the CDP location in the certificate indicates only where the CRL distribution point (CDP) is located in the directory; that is, the CDP does not indicate the actual query location for the directory.

The Cisco IOS software queries the CRL to ensure that the certificate has not been revoked in order to verify a peer certificate (for example, during Internet Key Exchange (IKE) or Secure Sockets Layer (SSL) handshake). The query looks for the CDP extension in the certificate, which is used to download the CRL. If this query is unsuccessful, then the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports the following CDP entries:

- HTTP URL with a hostname. For example: http://myurlname/myca.crl
- HTTP URL with an IPv4 address. For example: http://10.10.10.10:81/myca.crl
- LDAP URL with a hostname. For example: ldap://CN=myca, O=cisco
- LDAP URL with an IPv4 address. For example: ldap://10.10.10.10:3899/CN=myca, O=cisco

- LDAP/X.500 DN. For example: CN=myca, O=cisco

The Cisco IOS needs a complete URL in order to locate the CDP.

## Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# crl query http://www.cisco.com/security/pki/crl/crca2048.crl
```

## Related Commands

| Command | Description |
|---|---|
| **cabundle url** | Configures the URL from which the PKI trustpool CA bundle is downloaded. |
| **chain-validation** | Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool. |
| **crypto pki trustpool import** | Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle. |
| **crypto pki trustpool policy** | Configures PKI trustpool policy parameters. |
| **default** | Resets the value of a ca-trustpool configuration command to its default. |
| **match** | Enables the use of certificate maps for the PKI trustpool. |
| **ocsp** | Specifies OCSP settings for the PKI trustpool. |
| **revocation-check** | Disables revocation checking when the PKI trustpool policy is being used. |
| **show** | Displays the PKI trustpool policy of the router in ca-trustpool configuration mode. |
| **show crypto pki trustpool** | Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool. |

| Command | Description |
|---|---|
| **source interface** | Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool. |
| **storage** | Specifies a file system location where PKI trustpool certificates are stored on the router. |
| **vrf** | Specifies the VRF instance to be used for CRL retrieval. |

# crl (cs-server)

To specify the certificate revocation list (CRL) public key infrastructure (PKI) certificate server (CS), use the **crl** command in certificate server configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

**crl** *CRL-serial-number*
**no crl**

## Syntax Description

| | |
|---|---|
| *CRL-serial-number* | Specifies CRL serial number of the PKI CS. |

## Command Default

The CRL is not queried and no CRL cache parameters are configured.

## Command Modes

Certificate server configuration (cs-server)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The **crl** command is used with the *CRL-serial-number* argument to identify the serial number of the PKI CS. If the **crl** command is entered without this argument, then PKI hexmode is entered. In this mode, the hexidecimal data can be specified for the CS so that it can be appended to the parse buffer.

**Note** To exit this mode and return to global configuration mode, use the **quit** command.

## Examples

```
Router(config)# crypto pki server CA
Router(ca-server)# crl 0x0-0xFFFFFFFF
```

## Related Commands

| Command | Description |
|---|---|
| **auto-rollover** | Enables the automated CA certificate rollover functionality. |
| **cdp-url** | Specifies a CDP to be used in certificates that are issued by the certificate server. |
| **crypto pki server** | Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials |

| Command | Description |
|---|---|
| **database archive** | Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file. |
| **database level** | Controls what type of data is stored in the certificate enrollment database. |
| **database url** | Specifies the location where database entries for the CS is stored or published. |
| **database username** | Specifies the requirement of a username or password to be issued when accessing the primary database location. |
| **default (cs-server)** | Resets the value of the CS configuration command to its default. |
| **grant auto rollover** | Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA. |
| **grant auto trustpoint** | Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests. |
| **grant none** | Specifies all certificate requests to be rejected. |
| **grant ra-auto** | Specifies that all enrollment requests from an RA be granted automatically. |
| **hash (cs-server)** | Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA. |
| **issuer-name** | Specifies the DN as the CA issuer name for the CS. |
| **lifetime (cs-server)** | Specifies the lifetime of the CA or a certificate. |

| Command | Description |
|---|---|
| **mode ra** | Enters the PKI server into RA certificate server mode. |
| **mode sub-cs** | Enters the PKI server into sub-certificate server mode |
| **redundancy (cs-server)** | Specifies that the active CS is synchronized to the standby CS. |
| **serial-number (cs-server)** | Specifies whether the router serial number should be included in the certificate request. |
| **show (cs-server)** | Displays the PKI CS configuration. |
| **shutdown (cs-server)** | Allows a CS to be disabled without removing the configuration. |

# crl query

To query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked, use the **crl query** command in ca-trustpoint configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

**crl query** **ldap://***url:[port]*
**no crl query**

## Syntax Description

| | |
|---|---|
| **ldap://***url:[port]* | The Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server to query the CRL; for example, ldap://another_server.<br>**Note**<br>If a port number is not specified, then the default LDAP server port 389 is used.<br>The URL can be the LDAP server hostname, IPv4 address. |

## Command Default

The CRL is not queried.

## Command Modes

Ca-trustpoint configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(1)T | This command was introduced. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **crl query** command is disabled, the router checks the CRL distribution point (CDP) that is embedded in the certificate. The **crl query** command does not need to be configured if the CDP that is in the certificate is formatted as a URL (for example, **http://***url* or **ldap://***url*, including the fully qualified domain name (FQDN) of the host where the CRL is held.

The **crl query** command is used if the CDP is in LDAP form, which means that the CDP location in the certificate indicates only where the CDP is located in the directory; that is, the CDP does not indicate the actual query location for the directory.

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports the following CDP entries:

- HTTP URL with a hostname. For example: http://myurlname/myca.crl)
- HTTP URL with an IPv4 address. For example: http://10.10.10.10:81/myca.crl

- LDAP URL with a hostname. For example: ldap:///CN=myca, O=cisco)
- LDAP URL with an IPv4 address. For example: ldap://10.10.10.10:3899/CN=myca, O=cisco
- LDAP/X.500 DN. For example: CN=myca, O=cisco

To locate the CRL, a complete URL needs to be formed. The **ldap://** *hostname*:[*port*] keywords and arguments are used to provide this information.

**Note** The **crypto ca trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root command, the configuration mode and command is written back as ca-trustpoint.

**Note** The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all ca-identity and trusted-root configuration mode commands).

## Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named "bar":

```
crypto ca trustpoint mytp
 enrollment url http://bar.cisco.com
 crl query ldap://bar.cisco.com:3899
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca trustpoint** | Declares the CA that your router should use. |
| **enrollment url (ca-trustpoint)** | Specifies the enrollment parameters of a CA. |
| **ocsp url** | Specifies the URL of an OCSP server to override the OCSP server URL (if one exists) in the AIA extension of the certificate. |
| **revocation-check** | Checks the revocation status of a certificate. |

# crl best-effort

**Note** Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To download the certificate revocation list (CRL) but accept certificates if the CRL is not available, use the **crl best-effort**command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

## Syntax Description

This command has no arguments or keywords.

## Command Default

If this command is not configured, CRL checking is mandatory before your router can accept a certificate. That is, if CRL downloading is attempted and it fails, the certificate will be considered invalid and will be rejected.

## Command Modes

Ca-identity configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.3(2)T | This command was replaced by the **revocation-check** command. |

## Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the appropriate CRL is in the router memory, the CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.)

When a CA system uses multiple CRLs, the certificate of the peer will indicate which CRL applies in its CDP extension and should be downloaded by your router.

If your router does not have the applicable CRL in memory and is unable to obtain one, your router will reject the certificate of the peer--unless you include the **crl best-effort** command in your configuration. When the **crl best-effort** command is configured, your router will try to obtain a CRL, but if it cannot obtain a CRL, it will treat the certificate of the peer as not revoked.

When your router receives additional certificates from peers, the router will continue to attempt to download the appropriate CRL if it was previously unsuccessful. The **crl best-effort** command specifies only that when the router cannot obtain the CRL, the router will not be forced to reject the certificate of a peer.

## Examples

The following configuration example declares a CA and permits your router to accept certificates when CRLs are not obtainable:

```
crypto ca identity myid
enrollment url http://mycaserver
crl best-effort
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca identity** | Declares the CA your router should use. |

# crl optional

**Note** Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

**crl optional**
**no crl optional**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The router must have and check the appropriate CRL before accepting the certificate of another IP Security peer.

## Command Modes

Ca-identity configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.3(2)T | This command was replaced by the **revocation-check** command. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.) To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.

**Note** If the CRL already exists in the memory (for example, by using the **crypto ca crl request** command to manually download the CRL), the CRL will still be checked even if the **crl optional** command is configured.

## Examples

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
crypto ca identity myca
 enrollment url http://ca_server
 enrollment retry-period 20
 enrollment retry-count 100
 crl optional
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca identity** | Declares the CA your router should use. |

# crl-cache delete-after

To configure the maximum time a router will cache a certificate revocation list (CRL), use the **crl-cache delete-after** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

**crl-cache delete-after** *time*
**no crl-cache delete-after** *time*

## Syntax Description

| | |
|---|---|
| *time* | The maximum lifetime of a CRL in minutes. |

## Command Default

A CRL is deleted from the cache when the CRL default lifetime expires.

## Command Modes

Ca-trustpoint configuration (ca-trustpoint)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

Use this command to limit the amount of time a router will cache a CRL. You may use the **crl-cache delete-after** command to force a router to download a CRL before the existing CRL expires by configuring a value shorter than the default lifetime of the CRL.

By default, a new CRL will be downloaded after the currently cached CRL expires. The **crl-cache delete-after** command does not effect any currently cached CRLs. The configured lifetime will only effect CRLs downloaded after this command is configured.

When the maximum CRL time expires, the cached CRL will be deleted from the router cache. A new copy of the CRL will be downloaded from the issuing certificate authority (CA) the next time the router has to validate a certificate.



**Note** Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed to the user.

## Examples

The following example shows how to configure a maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration shown above:

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate
 time and the crl-cache delete-after
command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after
a maximum lifetime of 2 minutes.
You can verify that the CRL will be cached for 2 minutes by executing the show crypto pki
crls
 command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.
```

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 22:57:42 GMT Nov 26 2005
    NextUpdate: 22:59:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

## Related Commands

| Command | Description |
|---|---|
| **crl-cache none** | Disables CRL caching. |

# crl-cache none

To disable certificate revocation list (CRL) caching, use the **crl-cache none** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

**crl-cache none**
**no crl-cache none**

## Syntax Description

This command has no arguments or keywords.

## Command Default

CRL caching is enabled.

## Command Modes

Ca-trustpoint configuration (ca-trustpoint)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

Use this command to disable CRL caching for all CRLs associated with a trustpoint. By default, a new CRL is issued when the currently cached CRL expires.

The **crl-cache none** command does not effect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.

This functionality is useful is when a certification authority (CA) issues CRLs with no expiration date or with expiration dates far into the future-days or weeks.

**Note** Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

## Examples

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache none
```

The current CRL is still cached immediately after executing the example configuration shown above:

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
```

```
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
  ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate time. The **crl-cache none**command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the **show crypto pki crls** command. No output will be shown because there are no CRLs cached.

## Related Commands

| Command | Description |
|---|---|
| **crl-cache delete-after** | Configures the maximum lifetime of a CRL. |



# crypto aaa attribute list through crypto ipsec transform-set


- crypto aaa attribute list, on page 579
- crypto ca authenticate, on page 582
- crypto ca cert validate, on page 584
- crypto ca certificate chain, on page 585
- crypto ca certificate map, on page 587
- crypto ca certificate query (ca-trustpoint), on page 590
- crypto ca certificate query (global), on page 592
- crypto ca crl request, on page 593
- crypto ca enroll, on page 595
- crypto ca export pem, on page 598
- crypto ca export pkcs12, on page 601
- crypto ca identity, on page 603
- crypto ca import, on page 604
- crypto ca import pem, on page 605
- crypto ca import pkcs12, on page 607
- crypto ca profile enrollment, on page 609
- crypto ca trusted-root, on page 611
- crypto ca trustpoint, on page 612
- crypto call admission limit, on page 614
- crypto connect vlan, on page 616
- crypto ctcp, on page 618
- crypto dynamic-map, on page 620
- crypto-engine, on page 623
- crypto engine accelerator, on page 624
- crypto engine aim, on page 627
- crypto engine compliance shield disable, on page 628
- crypto engine em, on page 629
- crypto engine mode vrf, on page 630
- crypto engine nm, on page 632
- crypto engine onboard, on page 633
- crypto engine slot, on page 634

- crypto engine slot (interface), on page 635
- crypto gdoi ks, on page 638
- crypto gdoi gm, on page 640
- crypto gdoi group, on page 642
- crypto identity, on page 643
- crypto ikev2 authorization policy, on page 645
- crypto ikev2 certificate-cache, on page 647
- crypto ikev2 cluster, on page 648
- crypto ikev2 cookie-challenge, on page 650
- crypto ikev2 cts, on page 651
- crypto ikev2 diagnose, on page 656
- crypto ikev2 dpd, on page 657
- crypto ikev2 fragmentation, on page 659
- crypto ikev2 http-url, on page 660
- crypto ikev2 keyring, on page 661
- crypto ikev2 limit, on page 664
- crypto ikev2 name mangler, on page 666
- crypto ikev2 nat, on page 668
- crypto ikev2 policy, on page 669
- crypto ikev2 profile, on page 672
- crypto ikev2 proposal, on page 676
- crypto ikev2 redirect, on page 679
- crypto ikev2 window, on page 680
- crypto ipsec client ezvpn (global), on page 681
- crypto ipsec client ezvpn (interface), on page 686
- crypto ipsec client ezvpn connect, on page 689
- crypto ipsec client ezvpn xauth, on page 690
- crypto ipsec transform-set default, on page 692
- crypto ipsec df-bit (global), on page 694
- crypto ipsec df-bit (interface), on page 695
- crypto ipsec fragmentation (global), on page 697
- crypto ipsec fragmentation (interface), on page 698
- crypto ipsec ike sa-strength-enforcement, on page 700
- crypto ipsec ipv4-deny, on page 702
- crypto ipsec nat-transparency, on page 704
- crypto ipsec optional, on page 706
- crypto ipsec optional retry, on page 707
- crypto ipsec profile, on page 708
- crypto ipsec security-association dummy, on page 711
- crypto ipsec security-association idle-time, on page 712
- crypto ipsec security-association lifetime, on page 714
- crypto ipsec security-association multi-sn, on page 717
- crypto ipsec security-association replay disable, on page 718
- crypto ipsec security-association replay window-size, on page 719
- crypto ipsec server send-update, on page 720
- crypto ipsec transform-set, on page 721

# crypto aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list of per-user attributes on a local Easy VPN server, use the **crypto aaa attribute list**command in crypto isakmp group configuration mode. To remove the AAA attribute list, use the **no** form of this command.

**crypto aaa attribute list** *list-name*
**no crypto aaa attribute list** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Name of the local attribute list. |

## Command Default

A local attribute list is not defined.

## Command Modes

Crypto isakmp group configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

There is no limit to the number of lists that can be defined (except for NVRAM storage limits).

## Examples

The following example shows that per-user attributes have been defined on a local Easy VPN AAA server:

```
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login noAAA none
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
```

```
!
!
username example password 0 example
!
!
crypto isakmp policy 3
 encr aes
 authentication pre-share
 group 14
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
 key cisco
 pool dpool
 crypto aaa attribute list per-group
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
crypto ipsec transform-set set esp-aes esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny   icmp any any
logging alarm informational
logging trap debugging
!
```

```
control-plane
!
gatekeeper
 shutdown
!
line con 0
line aux 0
 stopbits 1
line vty 0 4
!
!
end
```

## Related Commands

| Command | Description |
|---|---|
| **crypto isakmp client configuration group** | Specifies to which group a policy profile will be defined. |

# crypto ca authenticate



**Note** This command was replaced by the **crypto pki authenticate** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto ca authenticate** command in global configuration mode.

**crypto ca authenticate** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command . |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the "RSA public key chain").

If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2038. If the validity period of the CA certificate is set to expire after the year 2038, the following error message will be displayed when authentication with the CA server is attempted:

error retrieving certificate :incomplete chain

The following messages are displayed when you attempt to debug the error:

CRYPTO_PKI: Unable to read CA/RA certificates.

PKI-3-GETCARACERT Failed to receive RA/CA certificates.

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2038, you must reduce the expiration date by a year or more.

## Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)#
crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
```

## Related Commands

| Command | Description |
|---|---|
| **debug crypto pki transactions** | Displays debug messages for the trace of interaction (message type) between the CA and the router. |
| **show crypto pki certificates** | Displays information about your certificate, the certificate of the CA, and any RA certificates. |

# crypto ca cert validate

**Note** This command was replaced by the **crypto pki cert validate** command effective with Cisco IOS Release 12.3(8)T and 12.2(18)SXE.

To determine if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid, use the **crypto ca cert validate** command in global configuration mode.

**crypto ca cert validate** *trustpoint*

## Syntax Description

| | |
|---|---|
| *trustpoint* | The trustpoint to be validated. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

The **crypto ca cert validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

## Examples

The following examples show the possible output from the **crypto ca cert validate** command:

```
Router(config)# crypto ca cert validate ka
Validation Failed: trustpoint not found for ka
Router(config)# crypto ca cert validate ka
Validation Failed: can't get local certificate chain
Router(config)# crypto ca cert validate ka
Certificate chain has 2 certificates.
Certificate chain for ka is valid
Router(config)# crypto ca cert validate ka
Certificate chain has 2 certificates.
Validation Error: no certs on chain
Router(config)# crypto ca cert validate ka
Certificate chain has 2 certificates.
Validation Error: unspecified error
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the certification authority that the router should use. |
| **show crypto pki trustpoints** | Displays the trustpoints that are configured in the router. |

# crypto ca certificate chain



**Note** This command was replaced by the **crypto pki certificate chain** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To enter the certificate chain configuration mode, use the **crypto ca certificate chain**command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

**crypto ca certificate chain** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint**command. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

## Examples

The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.

```
Router# show crypto ca certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
Router# configure terminal
Rrouter(config)# crypto ca certificate chain myca
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
```

**Related Commands**

| Command | Description |
|---|---|
| **certificate** | Adds certificates manually. |

# crypto ca certificate map



**Note** This command was replaced by the **crypto pki certificate map** command effective with Cisco IOS Release 12.3(7)T, 12.2(18)SXD, and 12.2(18)SXE.

To define certificate-based access control lists (ACLs), use the **crypto ca certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the no form of this command.

**crypto ca certificate map** *label sequence-number*
**no crypto ca certificate map** *label sequence-number*

## Syntax Description

| | |
|---|---|
| *label* | A user-specified label that is referenced within the **crypto ca trustpoint** command. |
| *sequence-number* | A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result. |

## Command Default

No default behavior or value.

## Command Modes

Ca-certificate-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |

## Usage Guidelines

Issuing this command places the router in CA certificate map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

```
field-name match-criteria match-value
```

The *field-name* in the above example is one of the certificate fields. Field names are similar to the names used in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.509 standard. The **name**field is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name, subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name** -- Case-insensitive string.
- **expires-on** --Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name** -- Case-insensitive string.
- **name** -- Case-insensitive string.
- **subject-name** --Case-insensitive string.
- **unstructured-subject-name** -- Case-insensitive string.
- **valid-start** --Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

**Note** The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* in the example is one of the following logical operators:

- **eq** --equal (valid for name and date fields)
- **ne** --not equal (valid for name and date fields)
- **co** --contains (valid only for name fields)
- **nc** --does not contain (valid only for name fields)
- **lt** --less than (valid only for date fields)
- **ge** --greater than or equal to (valid only for date fields)

The *match-value* is a case-insensitive string or a date.

## Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco, and the sequence is 10.

```
crypto ca certificate map Cisco 10
 issuer-name co Cisco Systems
 unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto ca certificate map Group 10
 issuer-name co Cisco Systems
 subject-name co DIAL
crypto ca certificate map Group 20
 issuer-name co Cisco Systems
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Cisco Systems” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Cisco Systems” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Cisco Systems” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o =Cisco,” and so on.

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |

# crypto ca certificate query (ca-trustpoint)



**Note** This command was replaced by the **crypto pki certificate query (ca-trustpoint)**command effective with Cisco IOS Release 12.3(7)T, 12.2(18)SXD, and 12.2(18)SXE.

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto ca certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the no form of this command.

**crypto ca certificate query**
**no crypto ca certificate query**

## Syntax Description

This command has no arguments or keywords.

## Command Default

CA trustpoints are stored locally in the router's NVRAM.

## Command Modes

Ca-trustpoint configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |

## Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto ca certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto pki trustpoint**command , which puts you in ca-trustpoint configuration mode.



**Note** This command replaces the **crypto ca certificate query**command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

## Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto ca trustpoint ka
 .
 .
```

```
.
crypto ca certificate query
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |

# crypto ca certificate query (global)

The **crypto ca certificate query**command in global configuration mode is replaced by the crypto ca certificate query command in ca-trustpoint configuration mode. See the **crypto ca certificate query** command for more information.

# crypto ca crl request

**Note** Effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE, this command was replaced by the **crypto pki crl request** command.

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto ca crl request**command in global configuration mode.

**crypto ca crl request** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto pki trustpoint**command. |

## Command Default

Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.3(7)T | This command was replaced by the **crypto pki crl request** command. |

## Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto ca crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.

**Note** This command should be used only after the trustpoint is enrolled.

## Examples

The following example immediately downloads the latest CRL to your router:

```
crypto ca crl request
```

# crypto ca enroll

**Note** This command was replaced by the **crypto pki enroll** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To obtain the certificate(s) of your router from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

**crypto ca enroll** *name*
**no crypto ca enroll** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint**command. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto ca enroll** command is not saved in the router configuration.

**Note** If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate(s), you must reissue the command.

### Responding to Prompts

When you issue the **crypto ca enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

**Note** This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

## Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: <mypassword>
Re-enter password: <mypassword>
% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

## Related Commands

| Command | Description |
|---|---|
| **debug crypto pki messages** | Displays debug messages for the details of the interaction (message dump) between the CA and the router. |
| **debug crypto pki transactions** | Displays debug messages for the trace of interaction (message type) between the CA and the router. |
| **show crypto pki certificates** | Displays information about your certificate, the certificate of the CA, and any RA certificates. |

# crypto ca export pem

**Note** This command was replaced by the **crypto pki export pem** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To export certificates and Rivest, Shamir, and Adelman (RSA) keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file, use the **crypto ca export pem**command in global configuration mode.

**crypto ca export** *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

## Syntax Description

| | |
|---|---|
| *trustpoint* | Name of the trustpoint that the associated certificate and RSA key pair will export.<br>The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command. |
| **terminal** | Certificate and RSA key pair that will be displayed in PEM format on the console terminal. |
| **url** *url* | URL of the file system where your router should export the certificate and RSA key pairs. |
| **3des** | Export the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm. |
| des | Export the trustpoint using the DES encryption algorithm. |
| *passphrase* | Passphrase that is used to encrypt the PEM file for import.<br>**Note**<br>The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The **crypto ca export pem**command allows you to export certificate and RSA key pairs in PEM-formatted files. The PEM files can then be imported back into the Cisco IOS router (via the **crypto pki import pem** command) or other public key infrastructure (PKI) applications.

## Examples

The following example shows how to generate and export the RSA key pair "aaa" and certificates of the router in PEM files that are associated with the trustpoint "mycs":

```
Router(config)# crypto key generate rsa general-keys label aaa exportable

The name for the keys will be:aaa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be:Router
% The subject name in the certificate will be:bizarro.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Request certificate from CA? [yes/no]:y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint: 8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto ca export aaa pem terminal 3des cisco123
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
    Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki import pem** | Imports certificates and RSA keys to a trustpoint from PEM-formatted files. |
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| enrollment | Specifies the enrollment parameters of a CA. |

# crypto ca export pkcs12



**Note** This command was replaced by the **crypto pki export pkcs12** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto ca export pkcs12** command in global configuration mode.

**crypto ca export** *trustpointname* **pkcs12** *destination url passphrase*

## Syntax Description

| | |
|---|---|
| *trustpointname* | Name of the trustpoint who issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name. |
| *destination url* | Location of the PKCS12 file to which a user wants to import the RSA key pair. |
| *passphrase* | Passphrase that is used to encrypt the PKCS12 file for export. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |

## Usage Guidelines

The **crypto ca export pkcs12**command creates a PKCS 12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

**Security Measures**

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS#12 file, the RSA key pair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the passphrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

## Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto ca export mytp pkcs12 flash:myexport mycompany
```

**Related Commands**

| Command | Description |
|---|---|
| **crypto pki import pkcs12** | Imports RSA keys. |

# crypto ca identity

The **crypto ca identity** command is replaced by the crypto ca trustpoint command. See the crypto ca trustpointcommand for more information.

# crypto ca import

**Note** This command was replaced by the **crypto pki import** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXD.

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto ca import**command in global configuration mode.

**crypto ca import** *name* **certificate**

## Syntax Description

| | |
|---|---|
| *name* **certificate** | Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

## Examples

The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto pki trustpoint MS
 enroll terminal
 crypto pki authenticate MS
!
crypto pki enroll MS
crypto ca import MS certificate
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| **enrollment** | Specifies the enrollment parameters of your CA. |
| **enrollment terminal** | Specifies manual cut-and-paste certificate enrollment. |

# crypto ca import pem



**Note** This command was replaced by the **crypto pki import pem** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To import certificates and Rivest, Shamir, and Adelman (RSA) keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files, use the **crypto ca import pem** command in global configuration mode.

**crypto ca import** *trustpoint* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*

## Syntax Description

| | |
|---|---|
| *trustpoint* | Name of the trustpoint that is associated with the imported certificates and RSA key pairs.<br>The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command. |
| **usage-keys** | (Optional) Specifies that two RSA special usage key pairs will be imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair. |
| **terminal** | Certificates and RSA key pairs will be manually imported from the console terminal. |
| **url** *url* | URL of the file system where your router should import the certificates and RSA key pairs. |
| **exportable** | (Optional) Specifies that the imported RSA key pair can be exported again to another Cisco device such as a router. |
| *passphrase* | Passphrase that is used to encrypt the PEM file for import.<br>**Note**<br>The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

The **crypto ca import pem**command allows you import certificates and RSA key pairs in PEM-formatted files.The files can be previously exported from another router or generated from other public key infrastructure (PKI) applications.

## Examples

The following example shows how to import PEM files to trustpoint “ggg” via TFTP:

```
Router(config)# crypto ca import ggg pem url tftp://10.1.1.2/johndoe/msca cisco1234
% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.ca]?
Reading file from tftp://10.1.1.2/johndoe/msca.ca
Loading johndoe/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]
% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.prv]?
Reading file from tftp://10.1.1.2/johndoe/msca.prv
Loading johndoe/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]
% Importing  certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.crt]?
Reading file from tftp://10.1.1.2/johndoe/msca.crt
Loading johndoe/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki export pem** | Exports certificates and RSA keys that are associated with a trustpoint in a PEM-formatted file. |
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| enrollment | Specifies the enrollment parameters of a CA. |

# crypto ca import pkcs12

**Note** This command was replaced by the **crypto pki import pkcs12** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To import Rivest, Shamir, and Adelman (RSA) keys, use the **crypto ca import pkcs12** command in global configuration mode.

**crypto ca import** *trustpointname* **pkcs12** *source url passphrase*

## Syntax Description

| | |
|---|---|
| *trustpointname* | Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name. |
| *source url* | The location of the PKCS12 file to which a user wants to export the RSA key pair. |
| *passphrase* | Passphrase that must be entered to undo encryption when the RSA keys are imported. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |

## Usage Guidelines

When you enter the **cyrpto ca import pkcs12** command, a ke pair and a trustpoint are generated. If you then decide you want to remove the key pair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto ca trustpoint** command to remove the trustpoint.

**Note** After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

## Examples

In the following example, an RSA key pair that has been associated with the trustpoint "forward" is to be imported:

```
Router(config)# crypto ca import forward pkcs12 flash:myexport mycompany
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki export pkcs12** | Exports RSA keys. |
| **crypto pki trustpoint** | Declares the CA that your router should use. |

| Command | Description |
|---|---|
| **crypto key zeroize rsa** | Deletes all RSA keys from your router. |

# crypto ca profile enrollment

**Note** This command was replaced with the **crypto pki profile enrollment** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To define an enrollment profile, use the **crypto ca profile enrollment**command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

**crypto ca profile enrollment** *label*
**no crypto ca profile enrollment** *label*

## Syntax Description

| | |
|---|---|
| *label* | Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command. |

## Command Default

An enrollment profile does not exist.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)ZH | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

## Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto ca profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command** --Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal** --Specifies manual cut-and-paste certificate authentication requests.
- **authentication url** --Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command** --Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal** --Specifies manual cut-and-paste certificate enrollment.
- **enrollment url** --Specifies the URL of the CA server to which to send enrollment requests.
- **parameter** --Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.



**Note** The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

## Examples

The following example shows how to define the enrollment profile named "E" and associated profile parameters:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca trustpoint** | Declares the CA that your router should use. |
| **enrollment profile** | Specifies that an enrollment profile can be used for certificate authentication and enrollment. |

# crypto ca trusted-root

The **crypto ca trusted-root** command is replaced by the crypto ca trustpoint command. See the **crypto ca trustpoint**command for more information.

# crypto ca trustpoint



**Note** Effective with Cisco IOS Release 12.3(8)T, 12.2(18)SXD, and 12.2(18)SXE, the **crypto ca trustpoint** command is replaced with the **crypto pki trustpoint** command. See the **crypto pki trustpoint** command for more information.

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

**crypto ca trustpoint** *name*
**no crypto ca trustpoint** *name*

## Syntax Description

| | |
|---|---|
| *name* | Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.) |

## Command Default

Your router does not recognize any CAs until you declare a CA using this command.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.2(15)T | The **match certificate** subcommand was introduced. |
| 12.3(7)T | This command was replaced by the **crypto pki trustpoint** command. You can still enter the **crypto ca trusted-root**or **crypto ca trustpoint** command, but the command will be written in the configuration as "crypto pki trustpoint." |

## Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto ca trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl** --Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)** --Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment** --Specifies enrollment parameters (optional).
- **enrollment http-proxy** --Accesses the CA by HTTP through the proxy server.
- **match certificate** --Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map**command.

- **primary** --Assigns a specified trustpoint as the primary trustpoint of the router.
- **root** --Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.



**Note** Beginning with Cisco IOS Release 12.2(8)T, the **crypto ca trustpoint** command unified the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, theconfiguration mode and command will be written in the configuration as **"crypto ca trustpoint**."

## Examples

The following example shows how to declare the CA named "ka" and specify enrollment and CRL parameters:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca | pki trustpoint** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

## Related Commands

| Command | Description |
|---|---|
| **crl** | Queries the CRL to ensure that the certificate of the peer has not been revoked. |
| **default (ca-trustpoint)** | Resets the value of a ca-trustpoint configuration subcommand to its default. |
| **enrollment** | Specifies the enrollment parameters of your CA. |
| **enrollment http-proxy** | Accesses the CA by HTTP through the proxy server. |
| **primary** | Assigns a specified trustpoint as the primary trustpoint of the router. |
| **root** | Obtains the CA certificate via TFTP. |

# crypto call admission limit

To specify the maximum number of Internet Key Exchange (IKE) security associations (SAs) that the device can establish before IKE begins rejecting new SA requests, use the **crypto call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

**crypto call admission limit ike** {**in-negotiation-sa** *number* | **sa** *number*}
**no crypto call admission limit ike** {**in-negotiation-sa** *number* | **sa** *number*}

## Syntax Description

| | |
|---|---|
| **ike** | Configures the crypto Call Admission Control active IKE SA limit. |
| **in-negotiation-sa** *number* | Specifies the maximum number of in-negotiation IKE SAs allowed. Range is from 10 to 99999. |
| **sa** *number* | Specifies the number of active IKE SAs allowed on the device. Range is from 0 to 99999. |

## Command Default

The maximum number of IKE SAs is not specified.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1 on the Cisco 6500 and Cisco 7600. |
| 12.4(6)T | This command was modified. The **in-negotiation-sa** *number* keyword-argument pair was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA on the Cisco 7600. The **in-negotiation-sa** *number* keyword-argument pair was not supported. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. The **in-negotiation-sa** *number* keyword-argument pair was not supported. |

## Usage Guidelines

Use this command to limit the number of IKE SAs permitted to or from a device. By limiting the number of IKE SAs that can be created on the device, you can prevent the device from being impacted due to sudden inflow of IKE SA requests. The ideal limit depends on the particular platform, the network topology, the application, and traffic patterns. When the specified limit is reached, IKE rejects all new SA requests. If you specify an IKE SA limit that is less than the current number of active IKE SAs, a warning is displayed, but SAs are not terminated. New SA requests are rejected until the active SA count is below the configured limit.

## Examples

The following example shows how to configure a maximum of 50 IKE SAs before IKE begins rejecting new SA requests.

```
Device(config)# crypto call admission limit ike sa 50
```

The following example shows how to configure a maximum of 100 in-negotiation IKE SAs before IKE begins rejecting new SA requests.

```
Device(config)# crypto call admission limit ike in-negotiation-sa 100
```

**Related Commands**

| Command | Description |
|---|---|
| **show crypto call admission statistics** | Monitors Crypto CAC statistics. |

# crypto connect vlan

To create an interface VLAN for an IPSec VPN SPA and enter crypto-connect mode, use the **crypto connect vlan** command in interface configuration mode. To remove the interface VLAN status from the VLAN, use the **no** form of this command.

**crypto connect vlan** *vlan-id*
**no crypto connect** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN ID number. |

## Command Default

No default behavior or values.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

You can enter the **crypto connect vlan** command only from the following:

- The associated port VLAN interface when the EtherChannel interface (port-channel interface) and participating interfaces are switch ports.
- The EtherChannel interface when the EtherChannel interface (port-channel interface) and participant interfaces are routed ports.

The **crypto engine subslot**command is only available for VLANs prior to the VLANs being made interface VLANs by the **crypto connect vlan** command.

When you enter the **crypto connect vlan** command, a target VLAN is made an interface VLAN if and only if the target VLAN is not currently an interface VLAN, and the target VLAN has been added to an inside trunk port using the **crypto engine subslot** command. If the VLAN has been added to more than one inside trunk port, the **crypto connect vlan** command is rejected.

The **no crypto engine subslot** command is allowed only after you enter the **no crypto connect vlan** command, or before you enter the **crypto connect vlan** command.

When you remove an interface VLAN from an inside trunk port and a corresponding crypto engine subslot configuration state exists, then that crypto engine subslot configuration state is not removed. If you remove a VLAN that has a crypto engine subslot configuration state, you need to manually add it back to recover. While in this inconsistent state, any attempt to enter the **no crypto connect vlan** command is rejected.

When you enter the **no crypto connect vlan** command, the interface VLAN status is removed from a VLAN. Any associated crypto engine subslot configuration state is not altered.

## Examples

The following example adds port 2/1 to the outside access port VLAN and connects the outside access port VLAN to the inside interface VLAN:

```
Router(config)# interface Vlan101
Router(config-if)# ip address 192.168.101.1 255.255.255.0
Router(config-if)# crypto map cmap
Router(config-if)# crypto engine subslot 3/0
Router(config-if)# interface GigabitEthernet2/1
Router(config-if)# crypto connect vlan 101
```

## Related Commands

| Command | Description |
|---|---|
| **crypto engine subslot** | Assign an interface VLAN that requires encryption to the IPSec VPN SPA. |
| **crypto map (interface IPSec)** | Applies a previously defined crypto map set to an interface. |
| **show crypto vlan** | Displays the VPN running state for an IPSec VPN SPA. |

# crypto ctcp

To configure Cisco Tunneling Control Protocol (cTCP) encapsulation for Easy VPN, use the **crypto ctcp**command in global configuration mode. To remove the cTCP encapsulation, use the **no** form of this command.

**crypto ctcp** [**keepalive** *number-of-seconds* | **port** *port-number*]
**no crypto ctcp** [**keepalive** *number-of-seconds* | **port** *port-number*]

## Syntax Description

| | |
|---|---|
| **keepalive** | (Optional) Sets the interval of cTCP keepalives that are sent by the remote device.<br>**Note**<br>This command is configured on the remote device. |
| *number-of-seconds* | (Optional) Number of seconds between the keepalives. Value = 5 through 3600. If the **keepalive** keyword is not configured, the default is 5. |
| **port** | (Optional) Port number that cTCP will listen to. Up to 10 numbers can be configured.<br>**Note**<br>This keyword is configured only on the server. |
| *port-number* | (Optional) Actual port number. Value = 1 through 65535. If the **port** keyword is not configured, the default port number is 10000. |

## Command Default

cTCP encapsulation is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | The **crypto ctcp** command was introduced. |
| 12.4(20)T | The **keepalive** keyword and *number-of-seconds* argument were added. |

## Usage Guidelines

If cTCP is enabled on a port, any application that uses that port will not function.

When cTCP encapsulation is enabled on the router, only packets less than or equal to 1407 in size can pass through the IPsec tunnel with the Don't Fragment (DF) bit set. If an attempt is made to send a larger size packet, the following syslog message is generated:

```
CRYPTO_ENGINE: locally-sourced pkt w/DF bit set is too big,ip->tl=1450, mtu=1407
```

**Note** If a Cisco IOS device is acting as a remote device, it has to send keepalives periodically to keep Network Address Translation (NAT) or firewall sessions from timing out.

## Examples

The following example shows that cTCP encapsulation has been configured on port 120:

```
Router (config)# crypto ctcp port 120
```

The following example shows that the cTCP keepalive interval has been set at 30 seconds:

```
Router (config)# crypto ctcp keepalive 30
```

## Related Commands

| Command | Description |
|---|---|
| clear crypto ctcp | Clears cTCP encapsulation. |
| ctcp port | Sets the port number for cTCP encapsulation for Easy VPN. |
| debug crypto ctcp | Displays information about a cTCP session. |
| show crypto ctcp | Displays information about a cTCP session. |

# crypto dynamic-map

To create a dynamic crypto map entry and enter crypto map configuration command mode, use the **crypto dynamic-map** command in global configuration mode. To delete a dynamic crypto map set or entry, use the **no** form of this command.

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
**no crypto dynamic-map** *dynamic-map-name* [*dynamic-seq-num*]

## Syntax Description

| | |
|---|---|
| *dynamic-map-name* | Specifies the name of the dynamic crypto map set. |
| *dynamic-seq-num* | Specifies the number of the dynamic crypto map entry. |

## Command Default

No dynamic crypto maps exist.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(15)T | This command was modified. All changes to PFS settings in the dynamic crypto map template are immediately passed on to the instantiated crypto map PFS settings. |

## Usage Guidelines

Use dynamic crypto maps to create policy templates that can be used when processing negotiation requests for new security associations from a remote IP security peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such as the peer's IP address). For example, if you do not know about all the IPsec remote peers in your network, a dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. (However, these requests are not processed until the Internet Key Exchange authentication has completed successfully.)

When a router receives a negotiation request via IKE from another IPsec peer, the request is examined to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, it will be rejected unless the crypto map set includes a reference to a dynamic crypto map.

The dynamic crypto map is a policy template; it will accept "wildcard" parameters for any parameters not explicitly stated in the dynamic crypto map entry. This allows you to set up IPsec security associations with a previously unknown IPsec peer. (The peer still must specify matching values for the nonwildcard IPsec security association negotiation parameters.)

If the router accepts the peer's request, at the point that it installs the new IPsec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the router performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary

crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is removed.

If changes are made to the Perfect Forward Secrecy (PFS) settings in the dynamic crypto map template,the changes are passed on to the PFS settings in the instantiated crypto map. During the next rekey process the new settings are used to negotiate with the remote peer.

Dynamic crypto map sets are not used for initiating IPsec security associations. However, they are used for determining whether or not traffic should be protected.

The only configuration required in a dynamic crypto map is the **set transform-set** command. All other configuration is optional.

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. After you define a dynamic crypto map set (which commonly contains only one map entry) using this command, you include the dynamic crypto map set in an entry of the "parent" crypto map set using the **crypto map** (IPsec global configuration) command. The parent crypto map set is then applied to an interface.

You should make crypto map entries referencing dynamic maps the lowest priority map entries, so that negotiations for security associations will try to match the static crypto map entries first. Only after the negotiation request does not match any of the static map entries do you want it to be evaluated against the dynamic map.

To make a dynamic crypto map the lowest priority map entry, give the map entry referencing the dynamic crypto map the highest *seq-num* of all the map entries in a crypto map set.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in an access list, and the corresponding crypto map entry is tagged as "IPsec," then the traffic is dropped because it is not IPsec protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPsec protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding security association (SA) is not yet established, the router will initiate new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).



**Note** Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include **deny** entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPsec protected.

## Examples

The following example shows how to configure an IPsec crypto map set.

Crypto map entry "mymap 30" references the dynamic crypto map set "mydynamicmap," which can be used to process inbound security association negotiation requests that do not match "mymap" entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in "mydynamicmap," for a flow "permitted" by the access list 103, IPsec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with "mydynamicmap 10" is also used as a filter. Inbound packets that match a **permit** statement in this list are dropped for not being IPsec protected. (The same is true for

access lists associated with static crypto maps entries.) Outbound packets that match a **permit** statement without an existing corresponding IPsec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

## Related Commands

| Command | Description |
|---|---|
| **crypto map (global IPsec)** | Creates or modifies a crypto map entry and enters the crypto map configuration mode. |
| **crypto map (interface IPsec)** | Applies a previously defined crypto map set to an interface. |
| **crypto map local-address** | Specifies and names an identifying interface to be used by the crypto map for IPsec traffic. |
| **match address (IPsec)** | Specifies an extended access list for a crypto map entry. |
| **set peer (IPsec)** | Specifies an IPsec peer in a crypto map entry. |
| **set pfs** | Specifies that IPsec should ask for PFS when requesting new security associations for this crypto map entry, or that IPsec requires PFS when receiving requests for new security associations. |
| **set security-association lifetime** | Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations. |
| **set transform-set** | Specifies which transform sets can be used with the crypto map entry. |
| **show crypto engine accelerator logs** | Displays a dynamic crypto map set. |
| **show crypto map (IPsec)** | Displays the crypto map configuration. |

# crypto-engine

To enter the QoS policy map configuration mode for the IPsec VPN module, use the **crypto-engine** command in interface configuration mode.

**crypto-engine**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command has no default settings.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | Support for this command was introduced. |

## Usage Guidelines

Once you enter the **crypto-engine** command, the prompt changes to the following:

Router(config-crypto-engine)#

The following crypto engine configuration commands are available when you enter the **crypto-engine** command:

- **default** --Sets a command to its defaults.
- **exit** --Exit service-flow submode.
- **no** --Negates a command or set its defaults.
- **service-policy output** *policy-map-name* --Configures the service policy by assigning a policy map to the output of an interface.

## Examples

The following example shows how to apply the policy map to tunnel egress traffic:

```
Router(config)# interface tunnel1

Router(config-if)# crypto-engine
Router(config-crypto-engine)# service-policy output crypto1
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the statistics and configurations of the QoS policies attached to the tunnel interface. |

# crypto engine accelerator

**Note** Effective with Cisco IOS Release 12.3(11)T, this command is replaced by the **crypto engine aim**, **crypto engine em**, **crypto engine nm**, **crypto engine onboard**, and **crypto engine slot** commands. See these commands for more information.

To enable the onboard hardware accelerator of the router for IP security (IPsec) encryption, use the **crypto engine accelerator** command in global configuration mode. To disable the use of the onboard hardware IPsec accelerator, and thereby perform IPsec encryption or decryption in software, use the **no** form of this command.

**crypto engine accelerator**
**no crypto engine accelerator**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The hardware accelerator for IPsec encryption is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPsec encryption. |
| 12.1(3)XL | Support was added for the Cisco uBR905 cable access router. |
| 12.2(2)XA | Support was added for the Cisco uBR925 cable access router. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745. |
| 12.2(15)ZJ | This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM. |
| 12.3(4)T | The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM. |
| 12.3(11)T | This command was replaced by the **crypto engine aim**, **crypto engine em**, **crypto engine nm**, **crypto engine onboard**, and **crypto engine slot** commands. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is not normally needed for typical operations because the onboard hardware accelerator of the router is enabled for IPsec encryption by default. The hardware accelerator should not be disabled except on instruction from Cisco Technical Assistance Center (TAC) personnel.

## Examples

The following example shows how to disable the onboard hardware accelerator of the router for IPsec encryption. This disabling is normally needed only after the accelerator has been disabled for testing or debugging purposes.

```
Router(config)# no crypto engine accelerator
Warning! all current connections will be torn down.
Do you want to continue? [yes/no]:
```

## Related Commands

| Command | Description |
|---|---|
| **clear crypto engine accelerator counter** | Resets the statistical and error counters for the hardware accelerator to zero. |
| **crypto ca** | Defines the parameters for the certification authority used for a session. |
| **crypto cisco** | Defines the encryption algorithms and other parameters for a session. |
| **crypto dynamic-map** | Creates a dynamic map crypto configuration for a session. |
| **crypto ipsec** | Defines the IPSec security associations and transformation sets. |
| **crypto isakmp** | Enables and defines the IKE protocol and its parameters. |
| **crypto key** | Generates and exchanges keys for a cryptographic session. |
| **crypto map** | Creates and modifies a crypto map for a session. |
| **debug crypto engine accelerator control** | Displays each control command as it is given to the crypto engine. |
| **debug crypto engine accelerator packet** | Displays information about each packet sent for encryption and decryption. |
| **show crypto engine accelerator ring** | Displays the contents of command and transmits rings for the crypto engine. |
| **show crypto engine accelerator sa database** | Displays the active (in-use) entries in the crypto engine SA database. |
| **show crypto engine accelerator statistic** | Displays the current run-time statistics and error counters for the crypto engine. |
| **show crypto engine brief** | Displays a summary of the configuration information for the crypto engine. |
| **show crypto engine configuration** | Displays the version and configuration information for the crypto engine. |

| Command | Description |
| --- | --- |
| **show crypto engine connections** | Displays a list of the current connections maintained by the crypto engine. |

# crypto engine aim

To reenable an advanced integration module (AIM), use the **crypto engine aim**command in global configuration mode. To disable an AIM encryption module, use the **no** form of this command.

**crypto engine aim** *aim-slot-number*
**no crypto engine aim** *aim-slot-number*

## Syntax Description

| | |
|---|---|
| *aim-slot-number* | Slot number to which an AIM is to be reenabled or disabled. |

## Command Default

An AIM is neither reenabled nor disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. This command replaces the **crypto engine accelerator** command. |

## Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine aim** command will be saved to the running and startup (nonvolatile memory) configuration.

## Examples

The following example shows that the AIM in slot 0 is to be reenabled:

```
crypto engine aim 0
```

The following example shows that the AIM in slot 0 is to be disabled:

```
no crypto engine aim 0
```

# crypto engine compliance shield disable

To effectively allow weak cryptographic algorithms such as Message Direct 5 (MD5), Data Encryption Standard (DES), or weak RSA keys to be enabled by various features, perform the **crypto engine compliance shield disable** command.

To prevent the weak crypto algorithms from being used by features, use the **no** form of this command.

**crypto engine compliance sheild disable**
**no crypto engine compliance sheild disable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Weak crypto algorithm check is enabled by default.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

## Usage Guidelines

Weak cryptographic algorithms are insecure and do not provide adequate protection from modern threats when used with features such as IPsec, SSH, etc.

Cisco does not recommend using this command to bypass a weak crypto algorithm check and should only be used as last resort.

For more information on which cryptographic algorithms are considered weak, please refer to the sections on algorithms with a status of “Avoid” or “Legacy” in the Next Generation Cryptography document.

Changing the compliance shield status will require a device reboot to take effect.

## Examples

The following example shows when the weak crypto algorithm check is disabled:

```
device(config)# crypto engine compliance shield disable
Disable compliance shield mode will take effect after reboot!
```

# crypto engine em

To enable the hardware accelerator of an expansion slot for IP security (IPsec) encryption, use the **crypto engine em**command in global configuration mode. To disable the hardware accelerator of the expansion slot, use the **no** form of this command.

**crypto engine em** *slot-number*
**no crypto engine em** *slot-number*

## Syntax Description

| | |
|---|---|
| *slot-number* | Slot number to which the hardware accelerator of the expansion slot is to be enabled or disabled (applies to slots 0 through 3). |

## Command Default

The hardware accelerator is neither enabled nor disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. This command replaces the **crypto engine accelerator** command. |

## Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine em** command will saved to the running and startup (nonvolatile memory) configuration.

## Examples

The following example shows that the hardware accelerator of expansion slot 1 is to be enabled:

```
crypto engine em 1
```

The following example shows that the hardware accelerator of expansion slot 1 is to be disabled:

```
no crypto engine em 1
```

# crypto engine mode vrf

To enable VRF-Aware mode for the IPSec VPN SPA, use the **crypto engine mode vrf**command in global configuration mode. To disable VRF-aware mode, use the **no** form of this command.

**crypto engine mode** *vrf*
**no crypto engine mode** *vrf*

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The VRF-Aware IPSec feature introduces IPSec tunnel mapping to Multiprotocol Label Switching (MPLS) VPNs.

Using the VRF-Aware IPSec feature, you can map IPSec tunnels to VPN routing and forwarding instances (VRFs) using a single public-facing address.

Unlike other IPSec VPN SPA feature configurations, when configuring VRF-Aware features, you do not use the **crypto connect vlan** command.

## Examples

The following example shows a VRF-Aware IPSec implementation:

```
ip vrf pepsi
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf coke
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
crypto engine mode vrf
interface vlan 100
 ip vrf forwarding pepsi
 ip address 10.2.1.1 255.255.255.0
 crypto engine subslot 3/0
 crypto map map100
interface vlan 200
 ip vrf forwarding coke
 ip address 10.2.1.1 255.255.255.0
 crypto engine subslot 3/0
 crypto map map200
interface gi1/1 (hidden VLAN 1000)
 ip address 171.1.1.1
 crypto engine subslot 3/0
! BASIC MPLS CONFIGURATION
```

```
mpls label protocol ldp
tag-switching tdp router-id Loopback0
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
!
! CONFIGURE THE INTERFACE CONNECTED TO THE MPLS BACKBONE WITH LABEL/TAG SWITCHING
interface GigabitEthernet2/12
 ip address 20.1.0.34 255.255.255.252
 logging event link-status
 speed nonegotiate
 mpls label protocol ldp
tag-switching ip
```

## Related Commands

| Command | Description |
|---|---|
| **crypto engine subslot** | Assigns an interface VLAN that requires encryption to the IPSec VPN SPA. |
| **ip vrf** | Configures a VRF routing table and enters VRF configuration mode. |
| **ip vrf forwarding** | Associates a VRF with an interface or subinterface. |
| **vrf** | Defines the VRF to which the IPSec tunnel will be mapped. |

# crypto engine nm

To enable the onboard hardware accelerator of a network module for IP security (IPsec) encryption, use the **crypto engine nm**command in global configuration mode. To disable the accelerator of the network module, use the **no** form of this command.

**crypto engine nm** *slot-number*
**no crypto engine nm** *slot-number*

## Syntax Description

| | |
|---|---|
| *slot-number* | Slot number to which the hardware accelerator of a network module is to be enabled or disabled (applies to slots 0 through 5). |

## Command Default

The hardware accelerator is neither enabled nor disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. This command replaces the **crypto engine accelerator** command. |

## Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine nm** command will saved to the running and startup (nonvolatile memory) configuration.

## Examples

The following example shows that the hardware accelerator of the network module in slot 0 is to be enabled:

```
crypto engine nm 0
```

The following example shows that the hardware accelerator of the network module in slot 0 is to be disabled:

```
no crypto engine nm 0
```

# crypto engine onboard

To enable the hardware accelerator of an onboard module for IP security (IPsec) encryption, use the **crypto engine onboard**command in global configuration mode. To disable the hardware accelerator of the onboard module, use the **no** form of this command.

**crypto engine onboard** *slot-number*
**no crypto engine onboard** *slot-number*

## Syntax Description

| | |
|---|---|
| *slot-number* | Slot number to which the hardware accelerator of the onboard module is to be enabled or disabled (applies to slots 0 and 1). |

## Command Default

The hardware accelerator is neither enabled nor disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. This command replaces the **crypto engine accelerator** command. |

## Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine onboard** command will saved to the running and startup (nonvolatile memory) configuration.

## Examples

The following example shows that the hardware accelerator of the onboard module in slot 1 is to be enabled:

```
crypto engine onboard 1
```

The following example shows that the hardware accelerator of the onboard module in slot 1 is to be disabled:

```
no crypto engine onboard 1
```

# crypto engine slot

To enable a hardware accelerator, such ISM-VPN (supported by ISR G2 routers) in a service adapter, use the **crypto engine slot** command in global configuration mode. To disable the hardware accelerator in the service adapter, use the **no** form of this command.

**crypto engine slot** *slot-number*
**no crypto engine slot** *slot-number*

## Syntax Description

| | |
|---|---|
| *slot-number* | Slot number to which the hardware accelerator in a service adapter is to be reenabled or disabled (applies to slots 0 through 6). |

## Command Default

The hardware accelerator is neither enabled nor disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. This command replaces the **crypto engine accelerator** command. |

## Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine slot** command will be saved to the running and startup (nonvolatile memory) configuration.

## Examples

The following example shows how to enable the hardware accelerator of the service adaptor in slot 2:

```
crypto engine slot 2
```

The following example shows how to disable the hardware accelerator of the service adaptor in slot 2:

```
no crypto engine slot 2
```

The following example shows how to enable ISM VPN in slot 0:

```
crypto engine slot 0
```

# crypto engine slot (interface)

To assign an interface VLAN, Virtual Routing and Forwarding (VRF) tunnel interface, or Front-door VRF (FVRF) interface that requires encryption to the IPSec VPN Shared Port Adapter (SPA), use the **crypto engine slot** command in interface configuration mode. The command usage and syntax varies based on whether you are in crypto-connect mode or VRF mode. In crypto-connect mode, the command is applied to interface VLANs and only the *slot*/*subslot* arguments are specified; in VRF-mode, the command is applied to interface VLANs, tunnel interfaces, or FVRF interfaces and either the **inside** or **outside** keyword must also be specified. To remove the interface, use the corresponding **no** form of this command.

**Crypto-Connect Mode Syntax**
**crypto engine slot** *slot*
**no crypto engine slot** *slot*

**VRF Mode Syntax**
**crypto engine slot** *slot* {**inside** | **outside**}
**no crypto engine slot** *slot* {**inside** | **outside**}

## Syntax Description

| | |
|---|---|
| *slot* | Chassis slot number where the Cisco 7600 SSC-400 card is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. |
| **inside** | (VRF Mode Only) Identifies the interface as an interface VLAN or tunnel interface. |
| **outside** | (VRF Mode Only) Identifies the interface as an FVRF interface. |

## Command Default

No interface is assigned.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced into Cisco IOS Release 12.2(33)SRA to support the IPSec VPN SPA on Cisco 7600 series routers and Catalyst 6500 series switches. |
| 12.2(33)SRE | This command was modified. The *subslot* argument was removed. |

## Usage Guidelines

Usage guidelines vary based on whether you are in crypto-connect mode or VRF mode:

**Crypto-Connect Mode Usage Guidelines**

With this command, you do not need to explicitly add interface VLANs to the IPSec VPN SPA inside trunk port.

It is strongly recommended that you use the **crypto engine slot** command instead of manually adding and removing VLANs from the inside trunk port.

When you add an interface VLAN to an inside trunk port and that interface VLAN is not already added to another inside trunk port, the crypto engine slot configuration state on the interface VLAN is combined. If the interface VLAN is already added to another inside trunk port, the command is rejected.

You should not try to add all VLANs at one time (If you attempt this, you can recover by manually removing the VLANs from the inside trunk port.)

In crypto-connect mode, the **crypto engine slot** command is used in conjunction with the **crypto connect vlan** command.

In crypto-connect mode, the **crypto engine slot** command is only available for VLANs prior to the VLANs being made interface VLANs by the **crypto connect vlan** command.

The **crypto engine slot** command is rejected if you enter it on a crypto-connected interface VLAN whose current crypto engine slot configuration is different from the subslot specified in the **crypto engine slot** command. To change the crypto engine slot configuration on an interface VLAN, you must ensure that the VLAN is not crypto-connected.

If you change the crypto engine slot configuration on an interface VLAN, any IPSec and IKE SAs that are currently active on that interface VLAN are deleted.

If you enter the **no crypto engine slot** command and the interface VLAN is crypto-connected, the **no crypto engine slot** command is rejected. The **no crypto engine slot** command is allowed only after you enter the **no crypto connect vlan** command, or before you enter the **crypto connect vlan** command.

When you remove an interface VLAN from an inside trunk port and a corresponding crypto engine slot configuration state exists, then that crypto engine slot configuration state is not removed. If you remove a VLAN that has a crypto engine slot configuration state, you need to manually add it back to recover. While in this inconsistent state, any attempt to enter the **no crypto connect vlan** command is rejected.

When you enter the **no crypto connect vlan** command, the interface VLAN status is removed from a VLAN. Any associated crypto engine slot configuration state is not altered.

When you **write** the configuration or **show** the configuration, the crypto engine slot configuration state is expressed in the context of the associated interface VLAN. The interface VLAN is also shown as having been added to the appropriate inside trunk port. This is the case even if the configuration was loaded from a legacy (pre-crypto engine slot) configuration file, or if VLANs were manually added instead of being added through the **crypto engine slot** command.

By editing the **crypto engine slot** commands and inside trunk port VLANs, it is possible to produce an inconsistent configuration file.

**VRF Mode Usage Guidelines**

When configuring an interface VLAN or tunnel interface in VRF mode, the **crypto-engine slot inside** command must be specified.

When configuring an FVRF interface in VRF mode, the **crypto-engine slot outside** command must be specified.

In VRF mode, the **crypto-connect vlan** command is not used.

In Cisco IOS Release 12.2(33)SRE and later releases the *subslot* argument was removed.

## Examples

The following crypto-connect mode example shows how to assign VLAN interface 101 to the IPSec VPN SPA in slot 3, subslot 0:

```
Router(config)# interface Vlan101
Router(config-if)# ip address 192.168.101.1 255.255.255.0
```

```
Router(config-if)# crypto map cmap
Router(config-if)# crypto engine slot 3/0
Router(config)# interface GigabitEthernet2/1
Router(config-if)# crypto connect Vlan101
```

The following VRF mode example shows how to assign VLAN interface 101 to the IPSec VPN SPA in slot 3, subslot 0:

```
Router(config)# interface Vlan101
Router(config-if)# ip vrf forwarding abc
Router(config-if)# ip address 10.2.1.1 255.255.255.0
Router(config-if)# crypto engine slot 3/0 inside
Router(config-if)# crypto map map100
```

The following VRF mode example shows how to assign Tunnel interface 1 to the IPSec VPN SPA in slot 4, subslot 0:

```
Router(config)# interface Tunnel1
Router(config)# ip vrf forwarding abc
Router(config-if)# ip address 10.1.1.254 255.255.255.0
Router(config-if)# tunnel source 172.1.1.1
Router(config-if)# tunnel destination 100.1.1.1
Router(config-if)# tunnel mode ipsec profile tp
Router(config-if)# crypto engine slot 4/0 inside
```

The following VRF mode example assigns the WAN-side interface GigabitEthernet1/1 to the IPSec VPN SPA in slot 3, subslot 0:

```
Router(config)# interface GigabitEthernet1/1
Router(config-if)# ip address 171.1.1.1 255.255.255.0
Router(config-if)# crypto engine slot 3/0 outside
```

## Related Commands

| Command | Description |
|---|---|
| **crypto connect vlan** | Creates an interface VLAN for an IPSec VPN SPA and enters crypto-connect mode. |
| **crypto map (interface IPSec)** | Applies a previously defined crypto map set to an interface. |
| ip vrf forwarding | Associates a VRF with an interface. |
| **show crypto vlan** | Displays the VPN running state for an IPSec VPN SPA. |
| tunnel vrf | Associates a VRF instance with a specific tunnel interface. |

# crypto gdoi ks

To trigger a rekey of group members in a GET VPN network, use the **crypto gdoi ks** command in privileged EXEC mode.

**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

## Syntax Description

| | |
|---|---|
| **group** *group-name* | (Optional) Name of the group. |
| **rekey** | Sends a rekey message based on the latest security policy in the running configuration. |
| **replace-now** | (Optional) Removes the old TEKs and KEK from group members (GMs) immediately and installs the new TEKs and KEK. |

## Command Default

No rekey is triggered.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Release 3.8S | This command was integrated into Cisco IOS XE Release 3.8S. |

## Usage Guidelines

When you change the policy (for example, from DES to AES) on the key server (KS) and exit from global configuration mode, a syslog message appears on the primary KS indicating that the policy has changed and a rekey is needed. You can enter the **crypto gdoi ks** command to send a rekey based on the latest security policy in the running configuration.

When each GM receives this triggered rekey, it installs the new SAs (for example, for AES) and shortens the lifetimes of the old SAs (for example, for DES). The GM continues to encrypt and decrypt traffic using the old SAs until their shortened lifetimes expire.

For GMs that are running older versions that do not yet support the **crypto gdoi ks** command, the primary KS uses the software versioning feature to detect those versions and only triggers a rekey without sending instruction for policy replacement. Therefore, when a GM receives the rekey, it installs the new SAs but does not shorten the lifetimes of the old SAs. (This behavior is the same as the prior rekey method and ensures backward compatibility for devices that cannot support policy replacement.)

If the **replace-now** keyword is used, the GM that receives the rekey will immediately remove the old TEKs and KEK and install the new TEKs and KEK. Therefore, the new policy takes effect immediately without waiting for existing policy SAs to expire.

You must use this command on the KS or primary KS. If you try to use this command on the secondary KS, it rejects the command as shown below:

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```



**Note** The **replace-now** keyword could cause a temporary traffic discontinuity, because all GMs may not receive the rekey message at the same time.

## Examples

The following example shows how to trigger a rekey on all GMs:

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

The following example shows how to remove the old TEKs and KEK from GMs immediately and install the new TEKs and KEK:

```
Device# crypto gdoi ks rekey replace-now
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto gdoi feature** | Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether each device is running a version that supports GM removal, rekey triggering with policy replacement, or the GDOI MIB. |

# crypto gdoi gm

For group members to change the IP security (IPsec) security association (SA) status, use the **crypto gdoi gm**command in privileged EXEC mode.

**crypto gdoi gm group** *group-name* {**ipsec direction inbound optional** | **ipsec direction inbound only** | **ipsec direction both**}

## Syntax Description

| | |
|---|---|
| **group** *group-name* | Name of the group. |
| **ipsec direction inbound optional** | Allows a group member to change the IPsec SA status to inbound optional. IPsec SA will accept cipher or plain text or both and will encrypt the packet before forwarding it. |
| **ipsec direction inbound only** | Allows a group member to change the IPsec SA status to inbound only. IPsec SA will accept cipher or plain text or both and will forward the packet in clear text. |
| **ipsec direction both** | Allows a group member to change the IPsec SA status to both inbound and outbound. IPsec SA will accept only cipher text and will encrypt the packet before forwarding it. |

## Command Default

If the **sa receive-only**command is specified on the key server, the group member remains in receive-only mode.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

This command is executed on group members. This command and its various keywords aid in testing individual group members and verifies that the group members are encrypting or decrypting traffic. This command and its keywords can be used only after the **sa receive-only** command has been configured on the key server.

The **ipsec direction inbound optional**keyword is used for situations in which all group members have been instructed to install the IPsec SAs as inbound only but for which a group member wants to install the IPsec SAs as inbound optional.

The **ipsec direction inbound only** keyword is used when a group member wants to change a previously set IPsec SA status to inbound only.

The **ipsec direction both**keyword is used when a group member has to change a previously set IPsec SA status to both inbound and outbound. In this setting, the group member accepts only cipher text.

## Examples

The following example shows how to determine whether a group member can accept cipher text.

On Group Member 1, configure the following:

```
crypto gdoi gm group groupexample ipsec direction inbound only
```

On Group Member 2, configure the following:

```
crypto gdoi gm group groupexample ipsec direction inbound optional
```

Then Ping Group Member 1.

Group Member 2 will have encrypted the packet and will send an encrypted packet to Group Member 1, which then decrypts that packet. If the traffic is from Group Member 1 to Group Member 2, Group Member 1 will forward the packet in clear text, and Group Member will accept it.

## Related Commands

| Command | Description |
|---|---|
| **sa receive-only** | Specifies that an IPsec SA is to be installed by a group member as “inbound only.” |

# crypto gdoi group

To create a Group Domain of Interpretation (GDOI) group and enter GDOI group configuration mode, use the **crypto gdoi group** command in global configuration mode. To disable a GDOI group, use the **no** form of this command.

**crypto gdoi group [ipv6]***group-name*
**no crypto gdoi group [ipv6]** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the group. You can use up to 80 characters. |
| **ipv6** | Creates an IPv6 group. |

## Command Default

A GDOI group is not defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 15.2(3)T | This command was modified. The **ipv6** keyword was added. |

## Usage Guidelines

There are more options for configuring a group on a key server than there are for configuring a group member. The group is identified by an identity and by the server. If the GDOI group is a group member, the address of the server is specified. If the GDOI group is a key server, “server local” is specified, which indicates that this is the key server.

## Examples

The following example shows how to configure an IPv4 GDOI group for a key server:

```
crypto gdoi group mygroup
 identity number 4444
 server local
```

The following example shows how to configure an IPv6 GDOI group for a key server:

```
crypto gdoi group ipv6 mygroup2
 identity number 4444
 server local
```

The following example shows how to configure an IPv4 GDOI group for a group member:

```
crypto gdoi group mygroup3
 identity number 3333
 server address ipv4 10.0.5.2
```

# crypto identity

To configure the identity of the router with a given list of distinguished names (DNs) in the certificate of the router, use the **crypto identity** command in global configuration mode. To delete all identity information associated with a list of DNs, use the **no** form of this command.

**crypto identity** *name*
**no crypto identity** *name*

## Syntax Description

| | |
|---|---|
| *name* | Identity of the router, which is associated with the given list of DNs. |

## Command Default

If this command is not enabled, the IP address is associated with the identity of the router.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(20)T | Support for IPv6 was added. |

## Usage Guidelines

The crypto identity command allows you to configure the identity of a router with a given list of DNs. Thus, when used with the dn and fqdn commands, you can set restrictions in the router configuration that prevent peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

**Note** The identity of the peer must be the same as the identity in the exchanged certificate.

## Examples

The following example shows how to configure a DN-based crypto map:

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
```

```
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

## Related Commands

| Command | Description |
|---|---|
| **crypto mib ipsec flowmib history failure size** | Associates the identity of the router with the DN in the certificate of the router. |
| **fqdn** | Associates the identity of the router with the hostname that the peer used to authenticate itself. |

# crypto ikev2 authorization policy

To configure an IKEv2 authorization policy, use the **crypto ikev2 authorization policy** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command. To return the authorization policy to its default value, use the **default** form of this command.

**crypto ikev2 authorization policy** *policy-name*
**no crypto ikev2 authorization policy** *policy-name*
**default crypto ikev2 authorization policy**

## Syntax Description

| | |
|---|---|
| *policy-name* | Group definition that identifies which policy is enforced for users. |

## Command Default

The default IKEv2 authorization policy is used.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |

## Usage Guidelines

Use the **crypto ikev2 authorization policy** command to specify the group for which a policy profile must be defined and the group policy information that needs to be defined or changed. You may wish to change the group policy on your router if you decide to connect to the client using a group ID that does not match the *policy-name* argument. The authorization policy is referred from the IKEv2 profile using the **aaa authorization group** command where the group name can be directly specified or derived from the remote identities using a name mangler.

If AAA authorization is configured as local, AAA derives the authorization attributes from IKEv2 client configuration group through the callback to crypto component.

After enabling this command, which puts the networking device in IKEv2 group authorization policy mode, you can specify the characteristics for the authorization policy using the following commands:

- **dhcp--** Configures an IP address on the remote access client for the Dynamic Host Configuration Protocol (DHCP) to use**.**
- **dns** --Specifies the primary and secondary Domain Name Service (DNS) servers for the group.
- **netmask** --Subnet mask to be used by the client for local connectivity.
- **pool** --Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **subnet-acl** --Configures split tunneling.
- **wins** --Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

You can modify the default authorization policy using the **crypto ikev2 authorization policy default** command. You can either modify the entire authorization policy or modify one of the above commands.

You can disable the default authorization policy using the **no crypto ikev2 authorization policy default** command. When disabled, the values in the default authorization policy are copied and the default proposal remains inactive.

## Examples

The following example shows how the client configuration group is referred from IKEv2 profile using the **aaa authorization group** command where the group name is specified directly. In this example, the policy is enforced for users that matches the group name “abc.”

```
aaa new-model
aaa authorization network aaa-group-list default local
!
crypto ikev2 authorization policy
abc
  pool pool1
  dns 198.51.100.1 198.51.100.100
  wins 203.0.113.1 203.0.113.115
  dhcp server 3.3.3.3
  dhcp giaddr 192.0.2.1
  dhcp timeout 10
  netmask 255.255.255.0
  subnet-acl acl-123
!
crypto ikev2 profile profile1
  authentication remote eap
aaa authorization group aaa-group-list abc
!
ip access-list extended acl-123
permit ip 209.165.200.225 0.0.0.31 any
permit ip 209.165.201.1 255.255.255.224 any
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization group** | Sets parameters that restrict user access to a network. |
| **dhcp** | Configures an IP address for the DHCP to use. |
| **dns** | Specifies the primary and secondary DNS servers for the group. |
| **netmask** | Specifies the netmask of the subnet address that is assigned to the client. |
| **pool** | Defines a local pool address for assigning IP addresses. |
| **subnet-acl** | Defines ACL for split tunneling. |
| **wins** | Specifies the internal WINS server addresses. |

# crypto ikev2 certificate-cache

To set the cache size to store certificates, use the **crypto ikev2 certificate-cache** command in global configuration mode. To delete the cache size, use the **no** form of this command.

**crypto ikev2 certificate-cache** *number-of-certificates*
**no crypto ikev2 certificate-cache**

## Syntax Description

| | |
|---|---|
| *number-of-certificates* | The maximum number of certificates that can be stored in the cache. |

## Command Default

The cache size is not set.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to set the cache to store the maximum number of certificates fetched from the HTTP URLs.

## Examples

The following example sets the cache size to store 500 certificates:

```
Router(config)# crypto ikev2 certificate-cache 500
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 cluster

To configure an Internet Key Exchange Version 2 (IKEv2) cluster policy in a Hot Standby Router Protocol (HSRP) cluster, use the **crypto ikev2 cluster** command in global configuration mode. To remove this command and all associated commands from your configuration, use the **no** form of this command.

**crypto ikev2 cluster**
**no crypto ikev2 cluster**

## Syntax Description

This command has no keywords or arguments.

## Command Default

An IKEv2 cluster policy is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |

## Usage Guidelines

Use the **crypto ikev2 cluster** command to define an IKEv2 cluster policy and to enter IKEv2 cluster configuration mode.

After enabling this command, you can specify the characteristics for the cluster policy by using the following commands:

- **holdtime**
- **master**
- **port**
- **slave**
- **standby-group**

To view the cluster configuration, use the **show crypto ikev2 cluster** command.

## Examples

The following example shows how to configure an IKEv2 cluster policy:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# master crypto-load 10
Device(config-ikev2-cluster)# slave priority 90
```

## Related Commands

| Command | Description |
|---|---|
| **holdtime** | Specifies the time interval to receive messages. |
| **master (IKEv2)** | Defines settings for the primary gateway in the HSRP cluster. |
| **port (IKEv2)** | Specifies port settings for the HSRP cluster. |

| Command | Description |
|---|---|
| **show crypto ikev2 cluster** | Displays the cluster policy configuration. |
| **slave (IKEv2)** | Defines settings for the secondary gateways in the HSRP cluster. |
| **standby-group** | Defines HSRP cluster settings. |

# crypto ikev2 cookie-challenge

To enable a cookie challenge for Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 cookie-challenge** command in global configuration mode. To disable the cookie challenge, use the **no** form of this command.

**crypto ikev2 cookie-challenge** *number*
**no crypto ikev2 cookie-challenge**

## Syntax Description

| | |
|---|---|
| *number* | Enables the IKEv2 cookie challenge when the number of half-open security associations (SAs) crosses the configured number. The range is 1 to 1000. |

## Command Default

The cookie challenge is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to enable the IKEv2 cookie challenge. A cookie challenge mitigates the effect of a DoS attack when an IKEv2 responder is flooded with session initiation requests from forged IP addresses.

## Examples

The following example sets the cookie challenge to 450:

```
Router(config)# crypto ikev2 cookie-challenge 450
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 cts

To enable IPsec inline tagging globally, use the **crypto ikev2 cts** command in global configuration mode. To disable the SGT inline tagging, use the **no** form of this command.

**crypto ikev2 cts sgt**
**no crypto ikev2 cts sgt**

## Syntax Description

| | |
|---|---|
| **sgt** | Enables Security Group Tag (SGT) IPsec inline tagging. |

## Command Default

IPsec inline tagging is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

This command applies to all sessions on the router. If IPsec inline tagging is disabled, the new negotiated sessions do not negotiate the vendor ID (VID). However, the current SA and the subsequent SA rekey are enabled with the feature until the lifetime of the SA. This applies to the new IPsec SA and the rekey of the IPsec SA established using the parent or rekeyed IKE SA.

## Examples

The following example shows how to enable IPsec inline tagging on an sVTI initiator and dVTI responder.

```
crypto ikev2 proposal p1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address ::/0
  pre-shared-key cisco
 !
 peer v4
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
```

```
!
!
crypto ikev2 profile prof3
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
!
crypto ikev2 cts sgt
!
crypto ipsec transform-set trans1 esp-aes esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set trans
 set ikev2-profile prof3
 match address ipv4acl
!
!
interface Loopback1
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001::4:1/112
!
interface Loopback2
 ip address 209.165.200.1 255.255.255.224
 ipv6 address 2001::40:1/112
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.210.74 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.240.0.0
 duplex auto
 speed auto
 ipv6 address 2001::5:1/112
 ipv6 enable
 crypto map cmap
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.16.0.2
ip route 10.12.255.200 255.0.0.0 172.31.255.254
!
ip access-list extended ipv4acl
 permit ip host 209.165.201.1host 192.168.12.125
 permit ip host 209.165.200.1 host 172.18.0.1
 permit ip host 172.28.0.1 host 10.10.10.1
 permit ip host 10.12.255.200 host 192.168.14.1
!
logging esm config
ipv6 route ::/0 2001::5:2
!
!
!
!
```

```
!!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000


crypto ikev2 proposal p1
 encryption aes-cbc-192
 integrity sha1
 group 15
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address 172.160.1.1 255.240.0.0
  pre-shared-key cisco
 !
 peer v4_p2
  address 172.31.255.1 255.240.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
 virtual-template 25
!
crypto ikev2 cts sgt
!
crypto ipsec transform-set trans esp-null esp-sha-hmac
!
crypto ipsec profile prof_ipv4
 set transform-set trans
 set ikev2-profile prof1_ipv4
!
!
interface Loopback0
 ip address 192.168.12.1 255.255.0.0
!
interface Loopback1
 no ip address
!
interface Loopback2
 ip address 172.18.0.1 255.240.0.0
!
```

```
interface Loopback10
 no ip address
 ipv6 address 2001::8:1/112
!
interface Loopback11
 no ip address
 ipv6 address 2001::80:1/112
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.0.0.0
 duplex auto
 speed auto
 ipv6 address 2001::7:1/112
 ipv6 enable
!
interface GigabitEthernet0/1
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.210.144 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 no ip address
 shutdown
!
interface FastEthernet0/0/1
 no ip address
!
interface FastEthernet0/0/2
 no ip address
!
interface FastEthernet0/0/3
 no ip address
!
!
interface Virtual-Template25 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof_ipv4
!
interface Vlan1
 no ip address
!
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 172.17.0.0 255.240.0.0 10.10.10.1
!
logging esm config
ipv6 route ::/0 2001::7:2
!
control-plane
```

```
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

# crypto ikev2 diagnose

To enable Internet Key Exchange Version 2 (IKEv2) error diagnostics, use the **crypto ikev2 diagnose** command in global configuration mode. To disable the error diagnostics, use the **no** form of this command.

**crypto ikev2 diagnose error** *number*
**no crypto ikev2 diagnose error**

## Syntax Description

| | |
|---|---|
| **error** | Enables the IKEv2 error path tracing. |
| *number* | Specifies the maximum number of errors allowed in the exit path entry. The range is 1 to 1000. |

## Command Default

IKEv2 error diagnostics is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to enable IKEv2 error path tracing and to specify the number of entries in the exit path database. When the number exceeds the specified number, new entries replace the old entries.

## Examples

The following example sets the maximum number of entries that can be logged:

```
Router(config)# crypto ikev2 diagnose error 500
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 dpd

To configure Dead Peer Detection (DPD) for Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 dpd**command in global configuration mode. To delete DPD, use the **no** form of this command.

**crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**}
**no crypto ikev2 dpd**

## Syntax Description

| | |
|---|---|
| *interval* | Specifies the keepalive interval in seconds. |
| *retry-interval* | Specifies the retry interval in seconds when there is no reply from the peer. |
| **on-demand** | Specifies the on-demand mode to send keepalive only in the absence of any incoming data traffic, to check the liveness of the peer before sending any data. |
| **periodic** | Specifies the periodic mode to send keepalives regularly at a specified interval. |

## Command Default

DPD is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to configure DPD globally for all peers. The DPD configuration in a Internet Key Exchange Version 2 (IKEv2) profile overrides the global DPD configuration.

## Examples

The following example shows how to configure the periodic mode for DPD. In the example in this step, the first DPD is sent after 30 seconds when there is no incoming ESP traffic. After waiting for 6 seconds (which is the specified retry interval), DPD retries are sent agressively 5 times in intervals of 6 seconds each. So, a total of 66 seconds (30 + 6 + 6 * 5 = 66) elapses before a crypto session is torn down because of DPD.

```
Router(config)# crypto ikev2 dpd 30 6 on-demand
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |

| Command | Description |
|---|---|
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 fragmentation

To configure Internet Key Exchange Version 2 (IKEv2) fragmentation, use the **crypto ikev2 fragmentation** command in global configuration mode. To disable the fragmentation, use the **no** form of this command.

**crypto ikev2 fragmentation mtu** *mtu-size*
**no crypto ikev2 fragmentation**

## Syntax Description

| | |
|---|---|
| **mtu** *mtu-size* | Specifies the maximum transmission unit in bytes. The range is from 68 to 1500 bytes. |

## Command Default

IKEv2 fragmentation is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |

## Usage Guidelines

Use this command to fragment the IKEv2 packets at IKEv2 layer and to avoid fragmentation after encryption. The MTU size refers to the IP or UDP encapsulated IKEv2 packets. The formula for fragmenting a packet is calculated as follows:

Specified MTU - UDP header - IP header = fragment packet size.

Using the above formula, if the MTU size is 100, specified in the command as **crypto ikev2 fragmentation mtu 100**, an IKE packet is fragmented if the packet size is greater than 72 bytes.

100 (specified MTU) - 8 (UDP header) - 20 (IP header) = 72 bytes.

## Examples

The following example shows how to configure IKEv2 fragmentation:

```
Router# enable
Router(config)# crypto ikev2 fragmentation mtu 200
```

# crypto ikev2 http-url

To enable lookup based on HTTP URL, use the **crypto ikev2 http-url**command in global configuration mode. To disable the lookup based on HTTP URL, use the **no** form of this command.

**crypto ikev2 http-url cert**
**no crypto ikev2 http-url cert**

## Syntax Description

| | |
|---|---|
| **cert** | Enable certificate lookup based on the HTTP URL. |

## Command Default

HTTP CERT is enabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1.(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to enable certificate lookup based on the HTTP URL. HTTP CERT indicates that the node is capable of looking up certificates based on the URL. This avoids the fragmentation that results when transferring large certificates.

## Examples

The following example shows how to configure HTTP CERT:

```
Router(config)# crypto ikev2 http-url cert
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 keyring

To configure an Internet Key Exchange version 2 (IKEv2) key ring, use the **crypto ikev2 keyring** command in the global configuration mode. To delete an IKEv2 keyring, use the **no** form of this command.

**crypto ikev2 keyring** *keyring-name*
**no crypto ikev2 keyring** *keyring-name*

## Syntax Description

| | |
|---|---|
| *keyring-name* | Name of the keyring. |

## Command Default

There is no default key ring.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

IKEv2 keyrings are independent of IKEv1 keyrings. The key differences are as follows:

- IKEv2 keyrings support symmetric and asymmetric preshared keys.
- IKEv2 keyrings do not support Rivest, Shamir and Adleman (RSA) public keys.
- IKEv2 keyrings are specified in the IKEv2 profile and are not looked up, unlike IKEv1 where keys are looked up on receipt of MM1 to negotiate the preshared key authentication method. The authentication method is not negotiated in IKEv2.
- IKEv2 keyrings are not associated with VPN routing and forwarding (VRF) during configuration. The VRF of an IKEv2 keyring is the VRF of the IKEv2 profile that refers the keyring.
- A single keyring can be specified in an IKEv2 profile, unlike an IKEv1 profile, which can specify multiple keyrings.
- A single keyring can be specified in more than one IKEv2 profile, if the same keys are shared across peers matching different profiles.
- An IKEv2 keyring is structured as one or more peer subblocks.

On an IKEv2 initiator, IKEv2 keyring key lookup is performed using the peer's hostname or the address, in that order. Use the hostname (ikev2 keyring) and address (ikev2 keyring) commands to configure the hostname and address in the IKEv2 keyring peer configuration mode.

On an IKEv2 responder, the key lookup is performed using the peer's IKEv2 identity or the address, in that order. Use the address (ikev2 keyring) and **identity**(ikev2 keyring) command to configure the address and identity in IKEv2 keyring peer configuration mode.

**Note** You cannot configure the same identity in more than one peer.

The best match is only performed for address configurations and a key lookup is performed for the remaining peer identification, including identity address.

## Examples

The following example shows how to configure a keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description example.com
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0

Router(config-ikev2-keyring-peer)# pre-shared-key xyz-key
```

The following example shows how a keyring match is performed. In the example, the key lookup for peer 10.0.0.1 would first match the wildcard key abc-key, then the prefix key abc-key and finally the host key host1-abc-key and the best match host1-abc-key is used.

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description example.com
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0

Router(config-ikev2-keyring-peer)# pre-shared-key xyz-key
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description abc.example.com
Router(config-ikev2-keyring-peer)# address 10.0.0.0 255.255.0.0

Router(config-ikev2-keyring-peer)# pre-shared-key abc-key
Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1@abc.example.com
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key host1-abc-key
```

In the following example, the key lookup for peer 10.0.0.1 would first match the host key host1-abc-key. Because, this is a specific match, no further lookup is performed.

```
Router(config)# crypto ikev2 keyring keyring-2
Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1 in abc.example.com sub-domain
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key host1-abc-key
Router(config-ikev2-keyring)# peer host2
Router(config-ikev2-keyring-peer)# description example domain
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key xyz-key
```

## Related Commands

| Command | Description |
|---|---|
| address (ikev2 keyring) | Specifies the IPv4 address or the range of the peers in IKEv2 keyring. |
| **description (ikev2 keyring)** | Describes an IKEv2 peer or a peer group for the IKEv2 keyring. |
| hostname (ikev2 keyring) | Specifies the hostname for the peer in the IKEv2 keyring. |

| Command | Description |
|---|---|
| **identity (ikev2 keyring)** | Identifies the peer with IKEv2 types of identity. |
| **peer** | Defines a peer or a peer group for the keyring. |
| pre-shared-key **(ikev2 keyring)** | Defines a preshared key for the IKEv2 peer. |

# crypto ikev2 limit

To enable call admission control in Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 limit** command in the global configuration mode. To disable call admission control, use the **no** form of this command.

**crypto ikev2 limit** {**max-in-negotiation-sa** *limit* [**incoming** | **outgoing**] | **max-sa** *limit* | **queue sa-init** *limit*}
**no crypto ikev2 limit** {**max-in-negotiation-sa** *limit* [**incoming** | **outgoing**] | **max-sa** *limit* | **queue sa-init**}

## Syntax Description

| | |
|---|---|
| **max-in-negotiation-sa** *limit* | Limits the total number of in-negotiation IKEv2 security associations (SAs) on the node. |
| **incoming** | (Optional) Limits the total number of in-negotiation IKEv2 SAs on the incoming node. |
| **outgoing** | (Optional) Limits the total number of in-negotiation IKEv2 SAs on the outgoing node. |
| **max-sa** *limit* | Limits the total number of IKEv2 SAs on the node. |
| **queue sa-init** *limit* | Limits the incoming SA_INIT requests size. |

## Command Default

By default, there is no configured limit on the number of IKEv2 SAs.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |
| Cisco IOS XE Release 3.12S | This command was modified. The **incoming** and **outgoing** keywords were added. |
| Cisco IOS XE Everest 16.5.1 | This command was modified. The **queue sa-init** *limit* keyword-argument pair was added. |
| Cisco IOS XE Everest 16.6.1 | The default **queue sa-init** *limit* of 5000 from being nvgen was stopped. |

## Usage Guidelines

Call admission control limits the in-negotiation and total number of IKEv2 SA on a node.



**Note** In IKEv2, rekey is not a new security association (SA) unlike in IKEv1. Hence, the rekey SA is not counted.

The **queue sa-init** *limit* keyword-argument pair limits the queue size to improve performance if you encounter packet drops from the initiating client due to response timeout. The packets are dropped when a source device sends IKEv2 INIT packets to a destination device to establish a tunnel, and the destination device is unable to process IKEv2 INIT packets faster due to a large queue of packets for processing on the responder device.

## Examples

The following example shows how to enable call admission control:

```
Device(config)# crypto ikev2 max-in-negotiation-sa limit 5000
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| **crypto logging ikev2** | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 name mangler

To configure the Internet Key Exchange version 2 (IKEv2) name mangler, use the **crypto ikev2 name mangler** command in global configuration mode. To delete the name mangler, use the **no** form of this command.

**crypto ikev2 name mangler** *mangler-name*
**no crypto ikev2 name mangler** *mangler-name*

## Syntax Description

| | |
|---|---|
| *mangler-name* | IKEv2 mangler name. |

## Command Default

IKEv2 name mangler is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |

## Usage Guidelines

The IKEv2 name mangler is used to derive a name for the AAA group or user authorization requests. The name mangler contains multiple statements--one for each identity type. The name mangler is derived from the specified portions of different forms of remote IKE identities or EAP identity. The name mangler is referred in the IKEv2 profile using the **aaa authorization** command.

**After enabling this command, which puts the networking device in** IKEv2 **name mangler configuration mode, you can specify the characteristics for the name mangler using the following commands:**

- **dn--** Derives the name from the remote identity of type distinguished name (DN)**.**
- **eap** --Derives the name from remote identities of type Extensible Authentication Protocol (EAP).
- **email** --Derives the name from the remote identity of type e-mail.
- **fqdn** --Derives the name from the remote identity of type Fully Qualified Domain Name (FQDN).

## Examples

The following example shows how to define name manglers based on identity of type FQDN:

```
crypto ikev2 name-mangler mangler1
 fqdn domain
crypto ikev2 name-mangler mangler2
 fqdn hostname
crypto ikev2 name-mangler mangler3
 fqdn all
```

The following example shows how to define name manglers based on identity of type e-mail:

```
crypto ikev2 name-mangler mangler1
 email domain
crypto ikev2 name-mangler mangler2
```

```
 email username
crypto ikev2 name-mangler mangler3
 email all
```

The following example shows how to define name manglers based on identity of type DN:

```
crypto ikev2 name-mangler mangler2
  DN country
crypto ikev2 name-mangler mangler3
  DN state
crypto ikev2 name-mangler mangler4
  DN organization
crypto ikev2 name-mangler mangler5
  DN organization-unit
```

The following example shows how to define name manglers based on identity of type EAP:

```
crypto ikev2 name-mangler mangler1
  eap all
crypto ikev2 name-mangler mangler2
  eap prefix user123 delimiter @
crypto ikev2 name-mangler mangler3
  eap suffix cisco delimiter
crypto ikev2 name-mangler mangler4
 eap DN common-name
```

## Related Commands

| Command | Description |
|---|---|
| **dn (IKEv2)** | Derives the name from identity of type DN. |
| **eap (IKEv2)** | Derives the name from identity of type EAP. |
| **email** | Derives the name from identity of type e-mail. |
| **fqdn** | Derives the name from identity of type FQDN. |

# crypto ikev2 nat

To configure Network Address Translation (NAT) keepalive for Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 nat**command in global configuration mode. To delete NAT keepalive configuration, use the **no** form of this command.

**crypto ikev2 nat keepalive** *interval*
**no crypto ikev2 nat keepalive** *interval*

## Syntax Description

| | |
|---|---|
| **keepalive** *interval* | Specifies the NAT keepalive interval in seconds. |

## Command Default

NAT keepalive is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to configure NAT keepalive globally for all peers. The NAT keepalive configuration specified in the IKEv2 profile overrides the global configuration. NAT keepalive prevents the deletion of NAT translation entries in the absence of any traffic, when NAT is between IKEv2 peers.

## Examples

The following example shows how to specify a NAT keepalive interval of 500 seconds:

```
Router(config)# crypto ikev2 nat keepalive 500
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ikev2 policy

To configure an Internet Key Exchange Version 2 (IKEv2) policy, use the **crypto ikev2 policy** command in global configuration mode. To delete a policy, use the **no** form of this command. To return the policy to its default value, use the **default** form of this command.

**crypto ikev2 policy** *name*
**no crypto ikev2 policy** *name*
**default crypto ikev2 policy**

## Syntax Description

| | |
|---|---|
| *name* | Name of the IKEv2 policy. |

## Command Default

A default IKEv2 policy is used only in the absence of any user-defined IKEv2 policy. The default IKEv2 policy will have the default IKEv2 proposal and will match all local addresses in a global VPN Routing and Forwarding (VRF).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

An IKEv2 policy contains the proposals that are used to negotiate the encryption, integrity, Psuedo-Random Function (PRF) algorithms and Diffie-Hellman (DH) group in SA_INIT exchange. IKEv2 policy can have match statements, which are used as selection criteria to select a policy for negotiation.

An IKEv2 policy must contain at least one proposal to be considered as complete, and can have more proposals and match statements.

A policy can have similar or different match statements. Match statements that are similar are logically ORed and match statements that are different are logically ANDed. There is no precedence between match statements of different types. Policy check will happen in a sequential order. To avoid unexpected or unpredictable behavior during IKEv2 policy selection, overlapping match statements must not be configured.

A policy is matched as follows:

- If no IKEv2 policy is configured, the default policy is used for negotiating a SA that uses any local address in a global VRF.
- If IKEv2 policies are configured, the policy with the best match is selected.
- If none of the configured policies matches, the SA_INIT exchange does not start.

You can modify the default policy using the **crypto ikev2 policy default** command. You can modify the entire policy or one of the statements in the policy.

You can disable the default policy using the **no crypto ikev2 policy default** command. When disabled, the values in the default policy are copied and the default policy remains inactive.

## Examples

The following examples show how to configure a policy and how a policy match is performed:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal pro1
Router(config-ikev2-policy)# match fvrf green
Router(config-ikev2-policy)# match address local 10.0.0.1
```

The policy policy1 is selected and proposal pro1 is used for negotiating IKEv2 SA with the local address as 10.0.0.1 and the FVRF as green:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal pro1
Router(config-ikev2-policy)# match address local 10.0.0.1
```

The policy policy1 is selected and proposal pro1 is used for negotiation of the IKEv2 SA that is negotiatied with the local address as 10.0.0.1 and the FVRF as global:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal pro1
Router(config-ikev2-policy)# match fvrf green
```

The policy policy1 is selected and proposal pro1 is used for negotiation of the IKEv2 SA that is negotiatied with any local address and the FVRF as green.

### How a Policy Match Is Performed

The following example shows how a policy is chosen out of two policies:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal1
Router(config-ikev2-policy)# match fvrf green
Router(config)# crypto ikev2 policy policy2
Router(config-ikev2-policy)# proposal1
Router(config-ikev2-policy)# match fvrf green
Router(config-ikev2-policy)# match local address 10.0.0.1
```

To negotiate the SA for local address 10.0.0.1 and FVRF as green, policy 2 is selected because policy 2 is the best match:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal2
Router(config-ikev2-policy)# match local address 10.0.0.1
Router(config-ikev2-policy)# match fvrf green
Router(config)# crypto ikev2 policy policy2
Router(config-ikev2-policy)# proposal1
Router(config-ikev2-policy)# match fvrf green
Router(config-ikev2-policy)# match local address 10.0.0.1
```

In this case, even though both the policies are the best match, policy1 is selected, because it was configured first.

## Related Commands

| Command | Description |
|---|---|
| **match (ikev2 policy)** | Matches an IKEv2 policy based on the parameters. |
| **proposal** | Specifies the proposals that must be used in the IKEv2 policy. |

| Command | Description |
| --- | --- |
| **show crypto ikev2 policy** | Displays the default or user-defined IKEv2 policy. |

# crypto ikev2 profile

To configure an Internet Key Exchange Version 2 (IKEv2) profile, use the **crypto ikev2 profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

**crypto ikev2 profile** *profile-name*
**no crypto ikev2 profile** *profile-name* **dynamic**

## Syntax Description

| | |
|---|---|
| *profile-name* | The name of the IKEv2 profile. |

## Command Default

There is no default IKEv2 profile. However, there are default values for some commands under the profile, such as lifetime.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |
| 17.2.1 | The dynamic keyword was introduced. |

## Usage Guidelines

Use this command to define an IKEv2 profile. An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE security associations (SAs) (such as local/remote identities and authentication methods) and the services that will be available to the authenticated peers that match the profile. The following are the characteristics of an IKEv2 profile:

- It must be attached to either a crypto map or an IPsec profile on the IKEv2 initiator and responder.
- It must contain a match identity or match certificate statement; otherwise the profile is considered incomplete and is unused.
- The statements match VRF, local or remote authentication methods are optional.

The table below describes the differences between IKEv1 and IKEv2 profiles.

***Table 21: Differences between IKEv1 and IKEv2 Profiles***

| IKEv1 | IKEv2 |
|---|---|
| The authentication method is a negotiable parameter and must be specified in the ISAKMP policy. | The authentication method is not a negotiable parameter, can be asymmetric, and must be specified in the profile. |
| Multiple keyrings can be specified in the profile. | A single keyring can be specified in the profile and is optional also. |

The IKEv2 profile applied on the crypto interface must be the same as IKEv2 profile that matches the peer identity received in the IKE_AUTH exchange.

## Examples

The following examples show an IKEv2 profile matched on a remote identity and an IKEv2 profile catering to two peers using different authentication method.

### IKEv2 Profile Matched on Remote Identity

The following profile caters to peers that identify using fqdn example.com and authenticate with rsa-signature using trustpoint-remote. The local node authenticates with pre-share using keyring-1.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

### IKEv2 Profile Catering to Two Peers Using Different Authentication Method

The following profile caters to two peers: user1@example.com that authenticate with pre-share using keyring-1, and user2@example.com authenticates with rsa-signature using trustpoint-remote. However, the local peer authenticates the remote peers with rsa-signature using trustpoint-local.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote email user1@example.com
Router(config-ikev2-profile)# match identity remote email user2@example.com
Router(config-ikev2-profile)# identity local email router2@abc.com
Router(config-ikev2-profile)# authentication local rsa-sig
Router(config-ikev2-profile)# authentication remote pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-local sign
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

### EAP Authentication with External EAP Server

The following example shows how to configure the remote access server using the remote EAP authentication method with an external EAP server:

```
aaa new-model
aaa authentication login aaa-eap-list default group radius
!
crypto ikev2 profile profile2
 authentication remote eap
 aaa authentication eap aaa-eap-list
```

### EAP Authentication with Local and External EAP

The following example shows how to configure the remote access server with local and external EAP server using the remote EAP authentication method:

```
aaa new-model
aaa authentication login aaa-eap-list default group radius
aaa authentication login aaa-eap-local-list default group tacacs
!
crypto ikev2 profile profile2
 authentication remote eap
 authentication remote eap-local
 aaa authentication eap aaa-eap-list
 aaa authentication eap-local aaa-eap-local-list
```

### Configuring the Local Policy

This example shows how to configure the AAA authorization for a local group policy:

```
aaa new-model
aaa authorization network aaa-group-list default local
!
 crypto ikev2 client configuration group cisco
  pool addr-pool1
  dns 198.51.100.1 198.51.100.100
  wins 203.0.113.1 203.0.113.115
 !
 crypto ikev2 profile profile1
  authentication remote eap
  aaa authorization group aaa-group-list abc
```

The aaa-group-list specifies that the group authorization is local and that the AAA username is abc. The authorization list name corresponds to the group policy defined in the **crypto ikev2 client configuration group** command.

### External AAA-based Group Policy

This example shows how to configure an external AAA-based group policy. The aaa-group-list specifies that the group authorization is RADIUS based. The name mangler derives the group name from the domain part of ID-FQDN, which is abc.

```
 aaa new-model
 aaa authorization network aaa-group-list default group radius
 !
 crypto ikev2 name-mangler mangler1
  fqdn domain
  !
 crypto ikev2 profile profile1
  identity remote fqdn host1.abc
  authentication remote eap
  aaa authorization group aaa-group-list name-mangler mangler1
```

### External AAA-based User Policy

This example shows how to configure an external AAA-based group policy. The aaa-user-list specifies that the user authorization is RADIUS based. The name mangler derives the username from the hostname part of ID-FQDN, which is host1.

```
aaa new-model
aaa authorization network aaa-user-list default group radius
!
crypto ikev2 name-mangler mangler2
 fqdn hostname
!
crypto ikev2 profile profile1
 match identity remote fqdn host1.abc
  authentication remote eap
 aaa authorization user aaa-user-list name-mangler mangler2
```

## Related Commands

| Command | Description |
|---|---|
| aaa authentication (IKEv2 profile) | Defines the AAA authentication list for EAP authentication. |
| aaa authorization (IKEv2 profile) | Defines the AAA authorization for a local or group policy. |
| authentication (IKEv2 profile) | Defines the local and remote authentication methods. |
| dynamic (IKEv2 profile) | Configures the IKEv2 profile settings to be dynamic. |
| **crypto ikev2 keyring** | Defines an IKEv2 keyring. |
| **show crypto ikev2 profile** | Displays the IKEv2 profile. |

# crypto ikev2 proposal

To configure an Internet Key Exchange Version 2 (IKEv2) proposal, use the **crypto ikev2 proposal** command in global configuration mode. To delete an IKEv2 proposal, use the **no** form of this command. To return the proposal to its default value, use the **default** form of this command.

**crypto ikev2 proposal** *name*
**no crypto ikev2 proposal** *name*
**default crypto ikev2 proposal**

## Syntax Description

| | |
|---|---|
| *name* | Name of the proposal. The proposals are attached to IKEv2 policies using the **proposal** command. |

## Command Default

The default IKEv2 proposal is used.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

An IKEv2 proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in negotiation.

You can modify the default proposal using the **crypto ikev2 proposal default** command. You can modify the entire proposal or one of the transforms namely, the encryption algorithm, the integrity algorithm and the DH group.

You can disable the default proposal using the **no crypto ikev2 proposal default** command. When disabled, the values in the default proposal are copied and the default proposal remains inactive.

Although this command is similar to the **crypto isakmp policy** command, the IKEv2 proposal differs as follows:

- An IKEv2 proposal allows configuration of one or more transforms for each transform type.
- An IKEv2 proposal does not have any associated priority.

**Note** The IKEv2 proposals must be attached to the IKEv2 policies for using the proposals in negotiation. If a proposal is not configured, then the default IKEv2 proposal is used with the default IKEv2 policy.

When multiple transforms are configured for a transform type, the order of priority is from left to right.

A proposal with multiple transforms for each transform type translates to all possible combinations of transforms. If only a subset of these combinations is required, then they must be configured as individual proposals.

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption aes-cbc-128, aes-cbc-192
Router(config-ikev2-proposal)# integrity sha, sha256
Router(config-ikev2-proposal)# group 14
```

For example, the commands shown translates to the following transform combinations:

```
aes-cbc-128, sha, 14
aes-cbc-192, sha, 14
aes-cbc-128, sha256, 14
aes-cbc-192, sha256, 14
```

To configure the first and last transform combinations, the commands are as follows:

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption aes-cbc-128
Router(config-ikev2-proposal)# integrity sha
Router(config-ikev2-proposal)# group 14
Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption aes-cbc-192
Router(config-ikev2-proposal)# integrity sha256
Router(config-ikev2-proposal)# group 14
```

## Examples

The following examples show how to configure a proposal:

### IKEv2 Proposal with One Transform for Each Transform Type

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity sha1
Device(config-ikev2-proposal)# group 14
```

### IKEv2 Proposal with Multiple Transforms for Each Transform Type

```
Device(config)# crypto ikev2 proposal proposal-2
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-192
Device(config-ikev2-proposal)# integrity sha2 sha256
Device(config-ikev2-proposal)# group 14 15
```

The IKEv2 proposal **proposal-2** shown translates to the following prioritized list of transform combinations:

- aes-cbc-128, sha1, 14
- aes-cbc-128, sha1, 15
- aes-cbc-128, sha256, 14
- aes-cbc-128, sha256, 15
- aes-cbc-192, sha1, 14
- aes-cbc-192, sha1, 15
- aes-cbc-192, sha256, 14
- aes-cbc-192, sha256, 15

### IKEv2 Proposals on the Initiator and Responder

The proposal of the initiator is as follows:

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-196
Device(config-ikev2-proposal)# integrity sha1 sha256
Device(config-ikev2-proposal)# group 14 16
```

The proposal of the responder is as follows:

```
Device(config)# crypto ikev2 proposal proposal-2
Device(config-ikev2-proposal)# encryption aes-cbc-196 aes-cbc-128
Device(config-ikev2-proposal)# integrity sha256 sha1
Device(config-ikev2-proposal)# group 16 14
```

In the scenario shown, the initiator choice of algorithms is preferred and the selected algorithms are as follows:

```
encryption aes-cbc-128
integrity sha1
group 14
```

## Related Commands

| Command | Description |
|---|---|
| **encryption (ikev2 proposal)** | Specifies the encryption algorithm in an IKEv2 proposal. |
| **group (ikev2 proposal)** | Specifies the Diffie-Hellman group identifier in an IKEv2 proposal. |
| **integrity (ikev2 proposal)** | Specifies the integrity algorithm in an IKEv2 proposal. |
| **show crypto ikev2 proposal** | Displays the parameters for each IKEv2 proposal. |

# crypto ikev2 redirect

To configure an Internet Key Exchange Version 2 (IKEv2) redirect mechanism on a gateway and a client, use the **crypto ikev2 redirect** command in global configuration mode. To remove the redirect mechanism, use the **no** form of this command.

**crypto ikev2 redirect** {**client** [**max-redirects** *number*] | **gateway** {**auth** | **init**}}
**no crypto ikev2 redirect** {**client** | **gateway**}

## Syntax Description

| | |
|---|---|
| **client** | Enables the redirect mechanism on a FlexVPN client. |
| **max-redirects** *number* | (Optional) Specifies the maximum number of redirects that can be configured per session on a FlexVPN client for redirect loop detection. The range is from 1 to 255. The default is 5. |
| **gateway** | Enables the redirect mechanism on a gateway. |
| **auth** | Enables the redirects mechanism on a gateway when a security association (SA) is authenticated. |
| **init** | Enables the redirect mechanism on a gateway when an SA is initiated. |

## Command Default

The redirects mechanism is disabled (on a gateway and a client).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |

## Usage Guidelines

A thorough security analysis shows that redirect during IKE_AUTH is neither more nor less secure than redirect during IKE_INIT. However, for performance and scalability reasons, we recommend redirect during IKE_INIT.

## Examples

The following example shows how to enable the redirects mechanism on the client and the gateway during initiation:

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 redirect client
Device(config)# crypto ikev2 redirect gateway init
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 cluster** | Defines an IKEv2 cluster policy in an HSRP cluster. |

# crypto ikev2 window

To configure the Internet Key Exchange Version 2 (IKEv2) window size, use the **crypto ikev2 window**command in global configuration mode. To delete IKEv2 window configuration, use the **no** form of this command.

**crypto ikev2 window** *window-size*
**no crypto ikev2 window**

## Syntax Description

| | |
|---|---|
| *window-size* | Size of the window that can range from 1 to 20. |

## Command Default

The default window size is 5.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Window size allows multiple IKEv2 request-response pairs in transit. Use this command to specify the IKEv2 window size to have multiple IKEv2 request-response pairs in transit.

## Examples

The following example shows how to configure a window size of 10:

```
Router(config)# crypto ikev2 window size 10
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| crypto logging ikev2 | Enables IKEv2 syslog messages on a server. |

# crypto ipsec client ezvpn (global)

To create a Cisco Easy VPN remote configuration and enter the Cisco Easy VPN remote configuration mode, use the **crypto ipsec client ezvpn** command in global configuration mode. To delete the Cisco Easy VPN remote configuration, use the **no** form of this command.

**crypto ipsec client ezvpn** *name*
**no crypto ipsec client ezvpn** *name*



**Note** A separate **crypto ipsec client ezvpn** command in interface configuration mode assigns a Cisco Easy VPN remote configuration to the interface.



**Note** For network extension mode, the dynamic NAT rule is not inserted by EZVPN client when a duplicate split tunnel (ACE has same source address but different destination address) entry is pushed from EZVPN server for network extension mode.

## Syntax Description

| | |
|---|---|
| *name* | Identifies the Cisco Easy VPN remote configuration with a unique, arbitrary name. |

## Command Default

Newly created Cisco Easy VPN remote configurations default to **client** mode.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)YA | This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(8)YJ | This command was enhanced to enable you to manually establish and terminate an IPsec VPN tunnel on demand for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.3(4)T | The **username** command was added, and the **pee**command was changed so that the command may now be input multiple times. |
| 12.3(7)XR | The **acl** and **backup** commands were added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.3(11)T | The **acl** command was integrated into Cisco IOS Release 12.3(11)T. However, the **backup** command was not integrated into Cisco IOS Release 12.3(11)T. |

| Release | Modification |
|---|---|
| 12.4(2)T | The **virtual-interface** command was added. |
| 12.4(4)T | The **default** keyword was added to the **peer** command, and the **flow allow acl** and **idle-time** commands were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | The **nat acl** and **nat allow** commands were added. |

## Usage Guidelines

The **crypto ipsec client ezvpn** command creates a Cisco Easy VPN remote configuration and then enters the Cisco Easy VPN remote configuration mode, at which point you can enter the following commands:

- **acl** {*acl-name* | *acl-number*}--Specifies multiple subnets in a Virtual Private Network (VPN) tunnel. Up to 50 subnets may be configured.
  - The *acl-name* argument is the name of the access control list (ACL).
  - The *acl-number* argument is the number of the ACL.

**Note** Use the **acl** command in the Network Extension Mode (NEM) to expand the networks that are being extended. The **permit** statements in the ACL allow you to add additional networks to the list of extended networks. Without an ACL, the VPN only provides connectivity with the directly connected network of the inside interface.

- **backup** {*ezvpn-config-name*} **track** {*tracked-object-number*}--Specifies the Easy VPN configuration that will be activated when the backup is triggered.
  - **backup** {*ezvpn-config-name*}--Specifies the Easy VPN configuration that will be activated when the backup is triggered.
  - **track** {*tracked-object-number*}--Specifies the link to the tracking system so that the Easy VPN state machine can get the notification to trigger the backup.
- **connect** [**auto** | **manual | acl**]--Manually establishes and terminates an IP Security (IPsec) tunnel on demand.
  - The **auto** keyword is the default setting, because it was the initial Cisco Easy VPN remote functionality. The IPsec VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface.
  - The **manual** keyword specifies the manual setting to direct the Cisco Easy VPN remote to wait for a command or application programming interface (API) call before attempting to establish the Cisco Easy VPN remote connection. When the tunnel times out or fails, subsequent connections have to wait for the command to reset to manual or to an API call.
  - The **acl** keyword specifies the ACL-triggered setting, which is used for transactional-based applications and dial backup. Using this option, you can define the "interesting" traffic that triggers the tunnel to be established.
- **default**--Sets the following command to its default values.
- **exit**--Exits the Cisco Easy VPN configuration mode and returns to global configuration mode.

- **flow allow acl** [*name* | *number*]--Restricts the client from sending traffic in clear text when the tunnel is down. The *name* argument is the access list name. The *number* argument is the access list number, which can be 100 through 199.
- **flow restrict**—Restricts the traffic coming from Cisco Easy VPN inside interface to goout in clear text when a VPN tunnel is down.
- **group** *group-name* **key** *group-key*--Specifies the group name and key value for the VPN connection.
- **idletime**--(Optional) Sets the idle time after which an Easy VPN tunnel is brought down.
- **local-address** *interface-name*--Informs the Cisco Easy VPN remote which interface is used to determine the public IP address, which is used to source the tunnel. This command applies only to the Cisco uBR905 and Cisco uBR925 cable access routers.
  - The value of the *interface-name* argument specifies the interface used for tunnel traffic.

After specifying the local address used to source tunnel traffic, the IP address can be obtained in two ways:

- - The **local-address** command can be used with the **cable-modem dhcp-proxy** {**interface loopback** *number} command to obtain a public IP address and automatically assign it to the loopback interface.*
  - The IP address can be manually assigned to the loopback interface.
- **mode** {**client** | **network-extension | network extension plus**}--Specifies the VPN mode of operation of the router:
  - The **client** keyword (default) automatically configures the router for Cisco Easy VPN client mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations. When the Cisco Easy VPN remote configuration is assigned to an interface, the router automatically creates the NAT or PAT and access list configuration needed for the VPN connection.
  - The **network-extension** keyword specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the address space of the enterprise network.
  - The **network extension plus** keyword is identical to network extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec security associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).
- nat acl {*acl-name* | *acl-number*}--Enables split-tunneling for the traffic specified by the ACL name or the ACL number.
  - The *acl-name* argument is the name of the ACL.
  - The *acl-number* argument is the number of the ACL.
- nat allow--Allows NAT to be integrated with Cisco Easy VPN.
- **no**--Removes the command or sets it to its default values.
- **peer** {*ipaddress* | *hostname* } [**default**]--Sets the peer IP address or hostname for the VPN connection. A hostname can be specified only when the router has a Domain Name System (DNS) server available for hostname resolution.

The **peer** command may be input multiple times.

The **default** keyword defines the given peer as the primary peer. When Phase 1 SA negotiations fail and Easy VPN fails over from the primary peer to the next peer on its backup list and the primary peer is again available, the current connection is torn down and the primary peer is reconnected.

- **username** *name* **password** {**0** | **6**} {*password*}--Allows you to save your extended authentication (Xauth) password locally on the PC. On subsequent authentications, you may activate the save-password tick box on the software client or add the username and password to the Cisco IOS hardware client profile. The setting remains until the save-password attribute is removed from the server group profile.
  - **0** specifies that an unencrypted password will follow.
  - **6** specifies that an encrypted password will follow.
  - *password specifies an unencrypted (cleartext) user password.*

The save-password option is useful only if the user password is static, that is, it is not a one-time password (OTP), such as a password generated by a token.

- **virtual-interface** [*virtual-template-number*]--Specifies a virtual interface for an Easy VPN remote device. If a virtual template number is specified, the virtual interface is derived from the virtual template that is configured. If a virtual template number is not specified, a generic virtual-access interface of the type tunnel is created. If the creation is successful, Easy VPN makes the virtual-access interface its outside interface (that is, the crypto map and NAT are applied on the virtual-access interface). If the creation is a failure, Easy VPN prints an error message and remains in the IDLE state.

After configuring the Cisco Easy VPN remote configuration, use the **exit** command to exit the Cisco Easy VPN remote configuration mode and return to global configuration mode.



**Note** You cannot use the **no crypto ipsec client ezvpn** command to delete a Cisco Easy VPN remote configuration that is assigned to an interface. You must remove that Cisco Easy VPN remote configuration from the interface before you can delete the configuration.

## Examples

The following example shows a Cisco Easy VPN remote configuration named “telecommuter-client” being created on a Cisco uBR905 or Cisco uBR925 cable access router and being assigned to cable interface 0:

```
Router# configure terminal

Router(config)# crypto ipsec client ezvpn telecommuter-client

Router(config-crypto-ezvpn)# group telecommute-group
 key secret-telecommute-key

Router(config-crypto-ezvpn)# peer telecommuter-server

Router(config-crypto-ezvpn)# mode client

Router(config-crypto-ezvpn)# exit

Router(config)# interface c0

Router(config-if)# crypto ezvpn telecommuter-client

Router(config-if)# exit
```



**Note** Specifying the **mode client** option as shown above is optional because this is a default configuration for these options.

The following example shows the Cisco Easy VPN remote configuration named "telecommuter-client" being removed from the interface and then deleted:

```
Router# configure terminal

Router(config)# interface e1

Router(config-if)# no crypto ipsec client ezvpn telecommuter-client

Router(config-if)# exit

Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

The following example shows that a virtual IPsec interface has been configured for the Easy VPN remote device:

```
crypto ipsec client ezvpn EasyVPN1
 virtual-interface 3
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec client ezvpn (interface)** | Assigns a Cisco Easy VPN remote configuration to an interface. |

# crypto ipsec client ezvpn (interface)

To assign a Cisco Easy Virtual Private Network (VPN) remote configuration to an interface other than a virtual interface, to specify whether the interface is outside or inside, and to configure multiple outside and inside interfaces, use the **crypto ipsec client ezvpn** command in interface configuration mode. To remove the Cisco Easy VPN remote configuration from the interface, use the **no** form of this command.

**crypto ipsec client ezvpn** *name* [**outside** | **inside**]
**no crypto ipsec client ezvpn** *name* [**outside** | **inside**]

## Syntax Description

| | |
|---|---|
| *name* | Specifies the Cisco Easy VPN remote configuration to be assigned to the interface.<br>**Note**<br>The interface specified cannot be a virtual interface. |
| **outside** | (Optional) Specifies the outside interface of the IP Security (IPsec) client router. You can add up to four outside tunnels for all platforms, one tunnel per outside interface. |
| **inside** | (Optional) Specifies the inside interface of the IPsec client router. The Cisco 1700 series has no default inside interface, and any inside interface must be configured. The Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers have default inside interfaces. However, you can configure any inside interface and add up to three inside interfaces for all platforms. |

## Command Default

The default inside interface is the Ethernet interface on Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)YA | This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(8)YJ | This command was enhanced to enable you to configure multiple outside and inside interfaces for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

The **crypto ipsec client ezvpn** command assigns a Cisco Easy VPN remote configuration to an interface, enabling the creation of a VPN connection over that interface to the specified VPN peer. If the Cisco Easy VPN remote configuration is configured for the client mode of operation, the router is also automatically

configured for network address translation (NAT) or port address translation (PAT) and for an associated access list.

**Note** The **crypto ipsec client ezvpn** command is not supported on virtual interfaces.

**Release 12.2(8)YJ**

The **crypto ipsec client ezvpn** command was enhanced to allow you to configure multiple outside and inside interfaces. To configure multiple outside and inside interfaces, you must use the **interface** *interface-name* command to first define the type of interface on the IPsec client router.

- In client mode for the Cisco Easy VPN client, a single security association (SA) connection is used for encrypting and decrypting the traffic coming from all the inside interfaces. In network extension mode, one SA connection is established for each inside interface.
- When a new inside interface is added or an existing one is removed, all established SA connections are deleted and new ones are initiated.
- Configuration information for the default inside interface is shown with the **crypto ipsec client ezvpn name inside** command. All inside interfaces, whether they belong to a tunnel, are listed in interface configuration mode as an inside interface, along with the tunnel name.

**Release 12.2(4)YA**

The following restrictions apply to the **crypto ipsec client ezvpn** command:

- The Cisco Easy VPN remote feature supports only one tunnel, so the **crypto ipsec client ezvpn** command can be assigned to only one interface. If you attempt to assign it to more than one interface, an error message is displayed. You must use the **no** form of this command to remove the configuration from the first interface before assigning it to the second interface.
- The **crypto ipsec client ezvpn** command should be assigned to the outside interface of the NAT or PAT. This command cannot be used on the inside NAT or PAT interface. On some platforms, the inside and outside interfaces are fixed.

For example, on Cisco uBR905 and Cisco uBR925 cable access routers, the outside interface is always the cable interface. On Cisco 1700 series routers, the FastEthernet interface defaults to being the inside interface, so attempting to use the **crypto ipsec client ezvpn** command on the FastEthernet interface displays an error message.

**Note** A separate **crypto ipsec client ezvpn** command exists in global configuration mode that creates a Cisco Easy VPN remote configuration. You must first use the global configuration version of the **crypto ipsec client ezvpn** command to create a Cisco Easy VPN remote configuration before assigning it to an interface.

## Examples

The following example shows a Cisco Easy VPN remote configuration named " telecommuter-client" being assigned to the cable interface on a Cisco uBR905 or a Cisco uBR925 cable access router:

```
Router# configure terminal
Router(config)# interface c0
```

```
Router(config-if)# crypto ipsec client ezvpn telecommuter-client

Router(config-if)# exit
```

The fo llowing example first shows an attempt to delete the Cisco Easy VPN remote configuration named “telecommuter-client, ” but the configuration cannot be deleted because it is still assigned to an interface. The configuration is then removed from the interface and deleted.

```
Router# configure terminal

Router(config)# no crypto ipsec client ezvpn telecommuter-client
Error: crypto map in use by interface; cannot delete
Router(config)# interface e1

Router(config-if)# no crypto ipsec client ezvpn telecommuter-client

Router(config-if)# exit

Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec client ezvpn (global)** | Creates and modifies a Cisco Easy VPN remote configuration. |
| **interface** | Configures an interface type. |

# crypto ipsec client ezvpn connect

To connect to a specified IPSec Virtual Private Network (VPN) tunnel in a manual configuration, use the **crypto ipsec client ezvpn connect** command in privileged EXEC mode. To disable the connection, use the **no** form of this command.

**crypto ipsec client ezvpn connect** *name*
**no crypto ipsec client ezvpn connect** *name*

## Syntax Description

| | |
|---|---|
| *name* | Identifies the IPSec VPN tunnel with a unique, arbitrary name. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(8)YJ | This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is used with the **connect** [**auto** | **manual** | **acl**] subcommand. After the manual setting is designated, the Cisco Easy VPN remote waits for a command or application programming interface (API) call before attempting to establish the Cisco Easy VPN remote connection.

If the configuration is manual, the tunnel is connected only after the **crypto ipsec client ezvpn connect** name command is entered in privileged EXEC mode, and after the **connect** [**auto**] | **manual** subcommand is entered.

## Examples

The following example shows how to connect an IPSec VPN tunnel named ISP-tunnel on a Cisco uBR905/uBR925 cable access router:

```
Router# crypto ipsec client ezvpn connect
 ISP-tunnel
```

## Related Commands

| Command | Description |
|---|---|
| **connect** | Manually establishes and terminates an IPSec VPN tunnel on demand. |
| **crypto ipsec client ezvpn (global)** | Creates and modifies a Cisco Easy VPN remote configuration. |

# crypto ipsec client ezvpn xauth

To respond to a pending Virtual Private Network (VPN) authorization request, use the **crypto ipsec client ezvpn xauth** command in privileged EXEC mode.

**crypto ipsec client ezvpn xauth** *name*

## Syntax Description

| | |
|---|---|
| *name* | Identifies the IP Security (IPSec) VPN tunnel with a unique, arbitrary name. This name is required. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)YA | This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(8)YJ | This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(8)YJ | This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

If the tunnel name is not specified, the authorization request is made on the active tunnel. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

When making a VPN connection, individual users might also be required to provide authorization information, such as a username or password. When the remote end requires this information, the router displays a message on the console of the router instructing the user to enter the **crypto ipsec client ezvpn xauth**command. The user then uses command-line interface (CLI) to enter this command and to provide the information requested by the prompts that follow after the command has been entered.



**Note** If the user does not respond to the authentication notification, the message is repeated every 10 seconds.

## Examples

The following example shows an example of the user being prompted to enter the **crypto ipsec client ezvpn xauth** command. The user then enters the requested information and continues.

```
Router#
```

```
20:27:39: EZVPN: Pending XAuth Request, Please enter the following command:
20:27:39: EZVPN: crypto ipsec client ezvpn xauth
Router> crypto ipsec client ezvpn xauth
Enter Username and Password: userid
Password: ************
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec client ezvpn (interface)** | Assigns a Cisco Easy VPN Remote configuration to an interface. |

# crypto ipsec transform-set default

To enable default IP Security (IPsec) transform sets, use the **crypto ipsec transform-set default** command in global configuration mode. To disable the default IPsec transform sets, use the **no** form of this command.

**crypto ipsec transform-setdefault**
**no crypto ipsec transform-setdefault**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default IPsec transform sets are enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

A default transform set will be used by any crypto map or ipsec profile where no other transform set has been configured if the following is true:

- The default transform sets have not been disabled with the **no crypto ipsec default transform-set** command.
- The crypto engine in use supports the encryption algorithm.

Each default transform set defines both an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type as shown in the table below.

***Table 22: Default Transform Sets and Parameters***

| Default Transform Name | ESP Encryption Transform and Description | ESP Authentication Transform and Description |
|---|---|---|
| #$!default_transform_set_0 | esp-3des<br>(ESP with the 168-bit Triple Data Encryption Standard [3DES or Triple DES] encryption algorithm) | esp-sha-hmac<br>(ESP with the Secure Hash Algorithm [SHA-1, HMAC variant] authentication algorithm) |

| Default Transform Name | ESP Encryption Transform and Description | ESP Authentication Transform and Description |
|---|---|---|
| #$!default_transform_set_1 | esp-aes<br>(ESP with the 128-bit Advanced Encryption Standard [AES] encryption algorithm) | esp-sha-hmac |

## Examples

```
The following example displays output from the show crypto ipsec transform-set default
 command when the default transform sets are enabled, the default setting.
Router# show crypto ipsec transform-set default

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
The following example displays output from the show crypto ipsec transform-set default
 command when the default transform sets have been disabled with the no crypto ipsec default
 transform-set
command.
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec transform-set default
! There is no output.
Router#
```

The following is example system log message that is generated whenever IPsec security associations (SAs) have negotiated with a default transform set.

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPSec transform-set
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto isakmp default policy** | Displays the default IKE policies currently in use. |

# crypto ipsec df-bit (global)

To set the DF bit for the encapsulating header in tunnel mode to all interfaces, use the **crypto ipsec df-bit** command in global configuration mode.

**crypto ipsec df-bit** [**clear** | **set** | **copy**]

## Syntax Description

| | |
|---|---|
| **clear** | Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation. |
| **set** | Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared. |
| **copy** | The router will look in the original packet for the outer DF bit setting. The **copy** keyword is the default setting. |

## Command Default

The default is **copy**

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |

## Usage Guidelines

Use the **crypto ipsec df-bit** command in global configuration mode to configure your router to specify the DF bit in an encapsulated header.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.



**Note** In Cisco IOS Release 15.2(1)T and later releases, either wait till the next rekey/SA installation or enter the **clear crypto session** command for the **crypto ipsec df-bit clear** command to take effect.

If this command is enabled without a specified setting, the router will use the **copy** setting as the default.

## Examples

The following example shows how to clear the DF bit on all interfaces:

```
crypto ipsec df-bit clear
```

# crypto ipsec df-bit (interface)

To set the DF bit for the encapsulating header in tunnel mode to a specific interface, use the **crypto ipsec df-bit** command in interface configuration mode.

**crypto ipsec df-bit** [**clear** | **set** | **copy**]

## Syntax Description

| | |
|---|---|
| **clear** | Outer IP header has the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation. |
| **set** | Outer IP header has the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared. |
| **copy** | The router looks in the original packet for the outer DF bit setting. |

## Command Default

The default setting is the same as the **crypto ipsec df-bit** command setting in global configuration mode.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |

## Usage Guidelines

Use the **crypto ipsec df-bit** command in interface configuration mode to configure your router to specify the DF bit in an encapsulated header. This command overrides any existing DF bit global settings.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

**Note** In Cisco IOS Release 15.2(1)T and later releases, either wait till the next rekey/SA installation or enter the **clear crypto session** command for the **crypto ipsec df-bit clear** command to take effect.

If this command is enabled without a specified setting, the router uses the **crypto ipsec df-bit** command setting in global configuration mode.

## Examples

In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces except Ethernet0 allows the router to send packets larger than the available MTU size; Ethernet0 allows the router to fragment the packet.

```
crypto isakmp policy 1
 encr aes
 hash sha
 authentication pre-share
 group 14
crypto isakmp key Delaware address 192.168.10.66
```

```
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-sha-hmac esp-aes
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102
!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```

# crypto ipsec fragmentation (global)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on a global basis, use the **crypto ipsec fragmentation**command in global configuration mode. To disable a manually configured command, use the **no** form of this command.

**crypto ipsec fragmentation** {**before-encryption** | **after-encryption**}
**no crypto ipsec fragmentation** {**before-encryption** | **after-encryption**}

## Syntax Description

| | |
|---|---|
| **before-encryption** | Enables prefragmentation for IPSec VPNs. The default is that prefragmentation is enabled. |
| **after-encryption** | Disables prefragmentation for IPSec VPNs. |

## Command Default

If you do not enter this command, prefragmentation is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(11b)E | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Use the **before-encryption**keywordto enable prefragmentation for IPSec VPNs; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of the output interface, the packet is fragmented before encryption.



**Note** This command does not show up in the a running configuration if the default global command is enabled. It shows in the running configuration only when you explicitly enable the command on an interface.

## Examples

The following example shows how to globally enable prefragmentation for IPSec VPNs:

```
crypto ipsec fragmentation before-encryption
```

# crypto ipsec fragmentation (interface)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on an interface, use the **crypto ipsec fragmentation**command in interface configuration mode. To disable a manually configured command, use the **no** form of this command.

**crypto ipsec fragmentation** {**before-encryption** | **after-encryption**}
**no crypto ipsec fragmentation** {**before-encryption** | **after-encryption**}

## Syntax Description

| | |
|---|---|
| **before-encryption** | Enables prefragmentation for IPSec VPNs. |
| **after-encryption** | Disables prefragmentation for IPSec VPNs. |

## Command Default

If no other prefragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(11b)E | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs per interface; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of output interface, the packet is fragmented before encryption.

## Examples

The following example shows how to enable prefragmentation for IPSec VPNs on an interface and then how to display the output of the show running configuration command:



**Note** This command shows in the running configuration only when you explicitly enable it on the interface.

```
Router(config-if)# crypto ipsec fragmentation before-encryption
Router(config-if)# exit
Router# show running-config
crypto isakmp policy 10
```

```
 encryption aes
 authentication pre-share
 group 14
crypto isakmp key abcd123 address 209.165.202.130
!
crypto ipsec transform-set fooprime esp-aes esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
 set peer 209.165.202.130
 set transform-set fooprime
 match address 102
```

# crypto ipsec ike sa-strength-enforcement

To ensure that the strength of the IKE encryption cipher is higher than the strength of its child IPsec SA's encryption ciphers, use the **crypto ipsec ike sa-strength-enforcement** command. To disable this feature, use the **no** form of this command.

**crypto ipsec ike sa-strength-enforcement**
**no crypto ipsec ike sa-strength-enforcement**

## Command Default

Enforcement is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 17.13 | This command was introduced. |

## Usage Guidelines

It is a good security practice to configure IPSec such that the strength of the IKE SA encryption cipher is greater than or equal to the strength of its child IPsec SA encryption cipher. The strength enforcement only affects the encryption cipher. It does not alter the integrity or key exchange algorithms. The encryption cipher strength comparison is done during session negotiation or establishment. It is not enforced during the configuration of IKE or IPsec. The number of bits in the encryption key determines the strength of the encryption cipher.

When this command is enabled, the IKEv1 and IKEv2 sessions compare the relative strength of each child SA's selected encryption cipher. If the child SA's encryption algorithm is stronger than the IKEv1 or IKEv2 encryption algorithms, the child SA negotiation will be aborted, and a new high-severity syslog and debug message will be issued to identify the cause of the failed negotiation.

The following table lists the supported encryption ciphers in order of strength (from highest to lowest). The encryption ciphers on the same line have equivalent strength for purposes of this check.

***Table 23: Supported Encryption Ciphers***

| ISAKMP/IKEv1 | IKEv2 | IPSec |
|---|---|---|
| AES-256 | AES-CBC-256 (default), AES-GCM-256 | ESP-AES-256 |
| AES-192 | AES-CBC-192 | ESP-AES-192 |
| | | ESP-SEAL-160 |
| AES-128 (default) | AES-CBC-128, AES-GCM-128 | ESP-AES-128 (default), ESP-GCM-128 |

## Examples

The following example shows how to configure Security Association Strength Enforcement.

```
Router(config) #crypto ipsec ike sa-strength-enforcement
% Warning: Please make sure IKE SA encryption keysize configured, is greater than or equal
```

```
 to IPSec SA encryption keysize.
Please run "clear crypto session" to enforce stronger IKE SA encryption immediately.
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto session detail** | Display the status of the crypto session. |
| **show running-config ipsec** | Displays the IPSec configuration details. |

# crypto ipsec ipv4-deny

To configure deny address ranges at the global (IPSec VPN SPA) level, use the **crypto ipsec ipv4 deny-policy** command in global configuration mode.

**crypto ipsec ipv4-deny** {**jump** | **clear** | **drop**}

## Syntax Description

| | |
|---|---|
| **jump** | Causes the search to jump to the beginning of the ACL associated with the next sequence in the crypto map and continues the search when a deny address is hit. |
| **clear** | Allows traffic to pass through in the clear (unencrypted) state when a deny address is hit. |
| **drop** | Causes traffic to be dropped when a deny address is hit. |

## Command Modes

The default behavior is **jump**.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Use this command to prevent repeated address ranges from being programmed in the hardware, resulting in more efficient TCAM space utilization.

Specifying a deny address range in an ACL results in “jump” behavior. When a denied address range is hit, it forces the search to “jump” to the beginning of the ACL associated with the next sequence in a crypto map and continue the search.

The **clear** keyword allows a deny address range to be programmed in hardware. The deny addresses are then filtered out for encryption and decryption. If the voice private network (VPN) mode is crypto-connect, when a deny address is hit, the search is stopped and traffic is allowed to pass in the clear (unencrypted) state.

If the VPN mode is VRF mode, the deny address matching traffic is dropped.

If you want to pass clear traffic on an address, you must insert a deny address range for each sequence in a crypto map.

Each permit list of addresses inherits all the deny address ranges specified in the ACL. A deny address range causes the software to do a subtraction of the deny address range from a permit list, and creates multiple permit address ranges that need to be programmed in hardware. This behavior can cause repeated address ranges to be programmed in the hardware for a single deny address range, resulting in multiple permit address ranges in a single ACL.

If you apply the specified keyword **(jump**, **clear**, or **drop**) when crypto maps are already configured on the IPSec VPN SPA, all existing IPSec sessions are temporarily removed and restarted, which impacts traffic on your network.

The number of deny entries that can be specified in an ACL are dependent on the keyword specified:

- **jump** --Supports up to 8 deny entries in an ACL.
- **clear** --Supports up to 1000 deny entries in an ACL.
- **drop** --Supports up to 1000 deny entries in an ACL.

## Examples

The following example shows a configuration using the deny-policy **clear** option. In this example, when a deny address is hit, the search will stop and traffic will be allowed to pass in the clear (unencrypted) state:

```
Router(config)# crypto ipsec ipv4-deny clear
```

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Defines a standard or extended IP access list. |

# crypto ipsec nat-transparency

To enable security parameter index (SPI) matching or User Datagram Protocol (UDP) encapsulation between two Virtual Private Network (VPN) devices, use the **crypto ipsec nat-transparency**command on both devices in global configuration mode. To disable both SPI matching and UDP encapsulation, use the **no** form of this command with each keyword.

**crypto ipsec nat-transparency** {**spi-matching** | **udp-encaps**}
**no crypto ipsec nat-transparency** {**spi-matching** | **udp-encaps**}

## Syntax Description

| | |
|---|---|
| **spi-matching** | Enables SPI matching on both endpoints. |
| udp-encaps | Enables UDP encapsulation on both endpoints. |

## Command Default

When this command is entered, UDP encapsulation is enabled by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(15)T | The command syntax was modified to add the **spi-matching**keyword**.** |

## Usage Guidelines

You can use this command to resolve issues that arise when Network Address Translation (NAT) is configured in an IP Security (IPsec)-aware network. This command has two mutually exclusive options:

- The default option is UDP encapsulation of the IPsec protocols.
- The alternative is to match the inbound SPI to the outbound SPI.

When you enter the **crypto ipsec nat-transparency** command, UDP encapsulation is configured unless you either specifically disable it or configure SPI matching. You can disable both options, but doing so might cause problems if the device you are configuring uses NAT and is part of a VPN.

To disable SPI matching, configure UDP encapsulation or use the **no** form of this command with the keyword **spi-matching**. To disable UDP encapsulation, configure SPI matching or use the **no** form of this command with the keyword **udp-encaps**. To disable both SPI matching and UDP encapsulation, first disable UDP encapsulation, and then disable SPI matching. If you disable both options, the **show running-config** command displays: **no crypto ipsec nat-transparency udp-encaps.**

## Examples

The following example enables SPI matching on the endpoint routers:

```
crypto ipsec nat-transparency spi-matching
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip nat translation** | Clears dynamic NAT translations from the translation table. |

| Command | Description |
|---|---|
| **ip nat** | Designates that traffic originating from or destined for the interface is subject to NAT. |
| **ip nat inside destination** | Enables NAT of the inside destination address. |
| **ip nat inside source** | Enables NAT of the inside source address. |
| **ip nat outside source** | Enables NAT of the outside source address. |
| **show ip nat statistics** | Displays NAT statistics. |
| **show ip nat translations** | Displays active NAT translations. |
| **show crypto isakmp sa detail nat** | Displays NAT translations of source and destination addresses. |

# crypto ipsec optional

To enable IP Security (IPSec) passive mode, use the **crypto ipsec optional** command in global configuration mode. To disable IPSec passive mode, use the **no** form of this command.

**crypto ipsec optional**
**no crypto ipsec optional**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IPSec passive mode is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **crypto ipsec optional**command to implement an intermediate mode (IPSec passive mode) that allows a router to accept unencrypted and encrypted data. IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec because all routers will continue to interact with routers that encrypt data (that is, that have been upgraded with IPSec) and also with routers that have yet to be upgraded.

After this feature is disabled, all active connections that are sending unencrypted packets are cleared, and a message that reminds the user to enter the **write memory** command is sent.



**Note** Because a router in IPSec passive mode is insecure, ensure that no routers are accidentally left in this mode after upgrading a network.

## Examples

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
 set peer 209.165.202.145
 set transform-set xauthtransform
 match address 192
!
crypto ipsec optional
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

# crypto ipsec optional retry

To adjust the amount of time that a packet can be routed in the clear (unencrypted), use the **crypto ipsec optional retry**command in global configuration mode. To return to the default setting (5 minutes), use the **no** form of this command.

**crypto ipsec optional retry** *seconds*
**no crypto ipsec optional retry** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Time a connection can exist before another attempt is made to establish an encrypted IP Security (IPSec) session. The default value is 5 minutes. |

## Command Default

5 minutes

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

You must enable the **crypto ipsec optional** command, which enables IPSec passive mode, before you can use this command.

## Examples

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
 set peer 209.165.202.145
 set transform-set xauthtransform
 match address 192
!
crypto ipsec optional
crypto ipsec optional retry 60
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec optional** | Enables IPSec passive mode. |

# crypto ipsec profile

To define the IP Security (IPsec) parameters that are to be used for IPsec encryption between two IPsec routers and to enter IPsec profile configuration mode, use the **crypto ipsec profile** command in global configuration mode. To delete an IPsec profile, use the **no** form of this command. To return the IPsec profile to its default value, use the **default** form of this command.

**crypto ipsec profile** *name*
**no crypto ipsec profile** *name*
**default crypto ipsec profile**

## Syntax Description

| | |
|---|---|
| *name* | Profile name. |

## Command Default

The default IPsec profile is used.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

An IPsec profile abstracts the IPsec policy settings into a single profile that can be used in other parts of the Cisco IOS configuration.

The IPsec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPsec profile. Only commands that pertain to an IPsec policy can be issued under an IPsec profile; you cannot specify the IPsec peer address or the access control list (ACL) to match the packets that are to be encrypted.

After this command has been enabled, the following commands can be configured under an IPsec profile:

- **default** —Sets the command to its defaults.
- **description** —Describes the crypto map statement policy.

- **dialer** —Specifies dialer-related commands.
- **exit**—Exits crypto map configuration mode.
- **no**—Negates a command or sets its defaults.
- **redundancy** —Configure stateless HA for this ipsec profile.
- **responder-only**—Do not initiate SAs from this device.
- **reverse-route**—Reverse Route Injection.
- **set**—Sets values for encryption/decryption.

After enabling this command, the only parameter that must be defined under the profile is the transform set via the **set transform-set** command.

You can modify the default IPsec profile using the **crypto ipsec profile default** command. You can disable the default IPsec profile using the **no crypto ipsec profile default** command.

For more information on transform sets, refer to the section "Defining Transform Sets" in the chapter "Configuring IPSec Network Security" in the *Cisco IOS Security Configuration Guide*.



**Note** Any changes in configurations under an IPsec profile, when its already applied on an interface, will not reflect on the interface. To reflect the changes, do one of the following:

- perform a shut/no shut on the tunnel interface, or
- remove the IPsec profile from the interface, and reapply it

## Examples

The following example shows how to configure a crypto map that uses an IPsec profile:

```
crypto ipsec transform-set cat-transforms esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile cat-profile
 set transform-set cat-transforms
 set pfs group14
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source FastEthernet2/0
 tunnel destination 10.13.7.67
 tunnel protection ipsec profile cat-profile
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec transform-set** | Defines a transform set. |
| **set pfs** | Specifies that IPsec should ask for PFS when requesting new security associations for a crypto map entry. |
| **set transform-set** | Specifies which transform sets can be used with the crypto map entry. |

| Command | Description |
|---|---|
| **tunnel protection** | Associates a tunnel interface with an IPsec profile. |

# crypto ipsec security-association dummy

To enable the generation and transmission of dummy packets in an IPsec traffic flow, use the **crypto ipsec security-association dummy** command in global configuration mode. To disable this generation and transmission, use the **no** form of this command.

**crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
**no crypto ipsec security-association dummy**

## Syntax Description

| | |
|---|---|
| **pps** *rate* | Packets per second rate. The range is 0 to 25. |
| **seconds** *seconds* | Delay, in seconds, between packets. The range is 1 to 3600. |

## Command Default

Generating and transmitting dummy packets is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M3 | This command was introduced. |
| Cisco IOS XE Release 3.10S | This command was integrated into Cisco IOS XE Release 3.10S. |

## Usage Guidelines

RFC 4303 specifies a method to hide packet data in an IPsec traffic flow by adding dummy packets in the traffic flow. Use the **crypto ipsec security-association dummy** command to generate and transmit dummy packets to hide data in the IPsec traffic flow. The dummy packet is designated by setting the next header field in the Encapsulating Security Payload (ESP) packet to a value of 59. When a crypto engine receives such packets, it discards them.

Use the **pps** *rate* keyword/argument pair to specify a rate greater than one packet per second.

## Examples

The following example generates dummy packets in the traffic flow every five seconds:

```
Device# configure terminal
Device(config)# crypto ipsec security-association dummy seconds 5
```

## Related Commands

| Command | Description |
|---|---|
| **set security-association dummy** | Enables the generation and transmission of dummy packets for an IPsec traffic flow in a crypto map. |

# crypto ipsec security-association idle-time

To configure the IP Security (IPSec) security association (SA) idle timer, use the **crypto ipsec security-association idle-time** command in global configuration mode or crypto map configuration mode. To inactivate the IPSec SA idle timer, use the **no** form of this command.

**crypto ipsec security-association idle-time** *seconds*
**no crypto ipsec security-association idle-time**

## Syntax Description

| | |
|---|---|
| *seconds* | Time, in seconds, that the idle timer allows an inactive peer to maintain an SA. The range is 60 to 86400 seconds. |

## Command Default

IPSec SA idle timers are disabled.

## Command Modes

Global configuration
Crypto map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **crypto ipsec security-association idle-time** command to configure the IPSec SA idle timer. This timer controls the amount of time that an SA will be maintained for an idle peer.

Use the **crypto ipsec security-association lifetime**command to configure global lifetimes for IPSec SAs. There are two lifetimes: a timed lifetime and a traffic-volume lifetime. A security association expires after the first of these lifetimes is reached.

The IPSec SA idle timers are different from the global lifetimes for IPSec SAs. The expiration of the global lifetimes is independent of peer activity. The IPSec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPSec SA idle timers are not configured with the **crypto ipsec security-association idle-time** command, only the global lifetimes for IPSec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.



**Note** If the last IPSec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.

**Release 12.2(33)SRA or later releases Release 12.2(33)SXH or later releases**

In a system using the IPSec VPN SPA with these software releases, the configured value for the *seconds* argument is rounded up to the next multiple of 600 seconds (ten minutes), and the rounded value becomes

the polling interval for SA idle detection. Because the SA idle condition must be observed in two successive pollings, the period of inactivity may last up to twice the polling period before the SAs are deleted.

## Examples

The following example configures the IPSec SA idle timer to drop SAs for inactive peers after at least 750 seconds:

```
Router# configure terminal
Router(config)# crypto ipsec security-association idle-time 750
```

With Cisco IOS Release 12.2(15)T or later releases, the SA will be deleted after an inactivity period of 750 seconds.

With Cisco IOS Release 12.2(33)SRA or 12.2(33)SXH or later releases, the configured value of 750 seconds will be rounded up to 1200 seconds (the next multiple of 600), which becomes the idle polling interval. The SA will be deleted after two successive idle pollings, resulting in an inactivity period of between 1200 and 2400 seconds before deletion.

## Related Commands

| Command | Description |
|---|---|
| **clear crypto sa** | Deletes IPSec SAs. |
| **crypto ipsec security-association lifetime** | Changes global lifetime values used when negotiating IPSec SAs. |

# crypto ipsec security-association lifetime

To change global lifetime values used when negotiating IPsec security associations, use the **crypto ipsec security-association lifetime**command in global configuration mode. To reset a lifetime to the default value, use the **no** form of this command.

**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}
**no crypto ipsec security-association lifetime** {**seconds** | **kilobytes** | **kilobytes disable**}

## Syntax Description

| | |
|---|---|
| **seconds** *seconds* | Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour). |
| **kilobytes** *kilobytes* | Specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes. |
| **kilobytes disable** | Disables the Internet Key Exchange (IKE) rekey based on volume only on the router on which it is configured.<br>• If the **no** form is used with this keyword, lifetime settings switch back to the default settings. |

## Command Default

3600 seconds (one hour) and 4,608,000 kilobytes (10 megabits per second for one hour).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3T | This command was introduced. |
| 12.2(13)T | The security association negotiation changed. Prior to Cisco IOS Release 12.2(13)T, the new security association was negotiated either 30 seconds before the **seconds** lifetime expired or when the volume of traffic through the tunnel reached 256 kilobytes less than the **kilobytes** lifetime. Effective with Cisco IOS Release 12.2(13)T, the negotiation is either 30 seconds before the **seconds** lifetime expires or when the volume of traffic through the tunnel reaches 90 percent of the **kilobytes** lifetime. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SXI | The **disable** keyword was added.<br>**Note**<br>This keyword addition is for only Cisco IOS Release 12.2(33)SXI. |
| 15.0(1)M | The **disable** keyword was added. |

## Usage Guidelines

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its global lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The security association expires after the first of these lifetimes is reached.

If you change a global lifetime, the change is only applied when the crypto map entry does not have a lifetime value specified. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more details.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** form of the command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the key of the security association.

Shorter lifetimes can make it harder to mount a successful key recovery attack, since the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The lifetime values are ignored for manually established security associations (security associations installed using an **ipsec-manual** crypto map entry).

### How The Lifetimes Work

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds**keyword) or after the amount of traffic in kilobytes has passed (specified by the **kilobytes** keyword).

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The **seconds**lifetime and the **kilobytes**lifetime each have a jitter mechanism to avoid security association rekey collisions. The new security association is negotiated either (30 plus a random number of) seconds before the **seconds** lifetime expires or when the traffic volume reaches (90 minus a random number of) percent of the **kilobytes**lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPsec sees another packet that should be protected.

### Disabling the Volume Lifetime

The **crypto ipsec security-association lifetime kilobytes disable** form of the command disables the volume lifetime. Using this command form should result in a significant improvement in performance and reliability, and this option can be used to reduce packet loss in high traffic environments. It can be used to prevent frequent rekeys that are triggered by reaching the volume lifetimes.

**Note** The volume lifetime can also be disabled using the **set security-association lifetime kilobytes disable** command.

## Examples

The following example shortens both lifetimes, because the administrator feels there is a higher risk that the keys could be compromised. The timed lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 kilobytes (10 megabits per second for one half hour).

```
crypto ipsec security-association lifetime seconds 2700
crypto ipsec security-association lifetime kilobytes 2304000
```

The following example shows that the **kilobytes disable** keyword has been used to disable the volume lifetime.

```
crypto ipsec security-association lifetime kilobytes disable
```

## Related Commands

| Command | Description |
|---|---|
| **set security-association lifetime** | Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations. |
| **show crypto ipsec security-association lifetime** | Displays the security-association lifetime value configured for a particular crypto map entry. |

# crypto ipsec security-association multi-sn

To enable multiple sequence number space per IPSec SA (security association), use the **crypto ipsec security-association multi-sn** command in global configuration mode. To disable multiple sequence number space, use the **no** form of the command.

**crypto ipsec security-association multi-sn**
**no crypto ipsec security-association multi-sn**

## Syntax Description

This command has no keywords or arguments

## Command Default

Multiple sequence number space is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 16.6.1 | This command was introduced. |

## Usage Guidelines

All existing sessions need to be cleared before configuring this feature. Else, traffic from the existing sessions will be dropped.

This feature needs to be configured on both the tunnel routers in an IPSec connection. If this featues is only enabled on one router, the other router will drop packets.

### Example

The following example shows how to enable multiple sequence number space on a device:

```
Device(config)# crypto ipsec security-association multi-sn
Warning: Existing sessions if any, might experience traffic drop due to SPI not found
```

**Note** This command is not supported on Cisco ISR44xx series devices.

# crypto ipsec security-association replay disable

To disable anti-replay checking globally, use the **crypto ipsec security-association replay disable** command in global configuration mode. To reset the configuration to enable anti-replay checking, use the **no** form of this command.

**crypto ipsec security-association replay disable**
**no crypto ipsec security-association replay disable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Anti-replay checking is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)SXF6 | This command was integrated into Cisco IOS Release 12.2(18)SXF6. |

## Examples

The following example shows that anti-replay checking has been disabled globally:

```
crypto map mymap 10
exit
crypto ipsec security-association replay disable
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec security-association replay window-size** | Sets the size of the SA anti-replay window. |

# crypto ipsec security-association replay window-size

To set the size of the security association (SA) anti-replay window globally, use the **crypto ipsec security-association replay window-size**command in global configuration mode. To reset the window size to the default of 64, use the **no** form of this command.

**crypto ipsec security-association replay window-size** [*N*]
**no crypto ipsec security-association replay window-size**

## Syntax Description

| | |
|---|---|
| *N* | (Optional) Size of the window. Values can be 64, 128, 256, 512, or 1024. This value becomes the default value.<br>**Note**<br>The window size is significant only if anti-replay checking is enabled. |

## Command Default

If a window size is not entered, the default is 64.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)SXF6 | This command was integrated into Cisco IOS Release 12.2(18)SXF6. |

## Examples

The following example shows that the size of the SA anti-replay window has been set globally to 128:

```
crypto map mymap 20
exit
crypto ipsec security-association replay window-size 128
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec security-association replay disable** | Disables anti-replay checking. |

# crypto ipsec server send-update

To send auto-update notifications any time after an Easy VPN connection is "up," use the **crypto ipsec server send-update** command in privileged EXEC mode.

**crypto ipsec server send-update** *group-name*
**no crypto ipsec server send-update** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of group to which to send auto-update notifications. |

## Command Default

Auto-update notifications are not sent.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(2T) | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is configured on a server. By configuring the command, the auto update notification is sent manually after the tunnel is "up."

## Examples

The following example shows that automatic update notifications are to be sent to GroupA:

```
crypto ipsec server send-update GroupA
```

# crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command. To return the transform-set to its default value, use the **default** form of this command.

**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
**no crypto ipsec transform-set** *transform-set-name*
**default crypto ipsec transform-set**

## Syntax Description

| | |
|---|---|
| *transform-set-name* | Name of the transform set to create (or modify). |
| *transform1 transform2 transform3 transform4* | Type of transform set. You may specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are described in the table below. |

## Command Default

The default transform-set is used.

## Command Modes

Global configuration

This command invokes the crypto transform configuration mode.

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(13)T | The following transform set options were added: **esp-aes**, **esp-aes 192**, and **esp-aes 256**. |
| 12.3(7)T | The **esp-seal** transform set option was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS release 12.(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(2)T | This command was modified in Cisco IOS Release 15.1(2)T. The **esp-gcm** and **esp-gmac transforms were added.** |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by the access list of that crypto map entry. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of the IPSec SAs of both peers.

When Internet Key Exchange (IKE) is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry, it must be defined using this command.

Although this command is similar to the **crypto isakmp policy** command, the IKEv2 proposal differs as follows:

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. The AH and ESP IPSec security protocols are described in the "*Allowed Transform Combinations*" section.

To define a transform set, you specify one to four "transforms"--each transform represents an IPSec security protocol (AH or ESP) plus the algorithm you want to use. When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set you can specify the AH protocol, the ESP protocol, or both. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform set or both an ESP encryption transform set and an ESP authentication transform set.

The table below lists the acceptable transform set combination selections for the AH and ESP protocols.

***Table 24: Allowed Transform Combinations***

| Transform Type | Transform | Description |
|---|---|---|
| **AH Transform** *>Pick only one.* | **ah-md5-hmac** | AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm. (No longer recommended). |
| | **ah-sha-hmac** | AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm. |

| Transform Type | Transform | Description |
|---|---|---|
| **ESP Encryption Transform** ( *>Pick only one.* | **esp-aes** | ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm. |
| | **esp-gcm**<br>**esp-gmac** | The **esp-gcm** and **esp-gmac** transforms are ESPs with either a 128 or 256 bit encryption algorithm. The default for either of these transforms is 128 bits.<br>**Note**<br>Both the **esp-gcm** and **esp-gmac** transforms cannot be configured together with any other ESP transform within the same crypto IPsec transform set using the crypto ipsec transform-set command. |
| | **esp-aes 192** | ESP with the 192-bit AES encryption algorithm. |
| | **esp-aes 256** | ESP with the 256-bit AES encryption algorithm. |
| | **esp-des** | ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm. (No longer recommended). |
| | **esp-3des** | ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). (No longer recommended). |
| | **esp-null** | Null encryption algorithm. |
| | **esp-seal** | ESP with the 160-bit SEAL encryption algorithm. (No longer recommended). |
| **ESP Authentication Transform** (*Pick only one.* ) | **esp-md5-hmac** | ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended). |
| | **esp-sha-hmac** | ESP with the SHA (HMAC variant) authentication algorithm. |
| **IP Compression Transform** | **comp-lzs** | IP compression with the Lempel-Ziv-Stac (LZS) algorithm.<br>**Note**<br>The IP Compression Transform is not supported on Cisco IOS XE software. |

Examples of acceptable transform set combinations are as follows:

- **ah-sha-hmac**
- **esp-gcm 256**
- **esp-aes**
- **esp-aes** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-aes** and **esp-sha-hmac**
- **comp-lzs** and **esp-sha-hmac** and **esp-aes** (In general, the **comp-lzs** transform set can be included with any other legal combination that does not already include the **comp-lzs** transform.)
- **esp-seal** and **esp-md5-hmac**

The parser will prevent you from entering invalid combinations; for example, after you specify an AH transform set, it will not allow you to specify another AH transform set for the current transform set.

**IPSec Protocols: AH and ESP**

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data--either a full IP datagram (or only the payload)--with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates or protects the payload of an IP datagram. For more information about modes, see the **mode**(IPSec) command description.

**The esp-seal Transform**

There are three limitations on the use of the **esp-seal** transform set:

- The **esp-seal** transform set can be used only if no crypto accelerators are present. This limitation is present because no current crypto accelerators implement the SEAL encryption transform set, and if a crypto accelerator is present, it will handle all IPSec connections that are negotiated with IKE. If a crypto accelerator is present, the Cisco IOS software will allow the transform set to be configured, but it will warn that it will not be used as long as the crypto accelerator is enabled.
- The **esp-seal** transform set can be used only in conjunction with an authentication transform set, namely one of these: **esp-md5-hmac**, (not recommended) **esp-sha-hmac**, **ah-md5-hmac** (not recommended), or **ah-sha-hmac**. This limitation is present because SEAL encryption is especially weak when it comes to protecting against modifications of the encrypted packet. Therefore, to prevent such a weakness, an authentication transform set is required. (Authentication transform sets are designed to foil such attacks.) If you attempt to configure an IPSec transform set using SEAL but without an authentication transform set, an error is generated, and the transform set is rejected.
- The **esp-seal** transform set cannot be used with a manually keyed crypto map. This limitation is present because such a configuration would reuse the same keystream for each reboot, which would compromise security. Because of the security issue, such a configuration is prohibited. If you attempt to configure a manually keyed crypto map with a SEAL-based transform set, an error is generated, and the transform set is rejected.

**Selecting Appropriate Transform Sets**

The following tips may help you select transform sets that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform set.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform set. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform set, also consider including an ESP authentication transform set or an AH transform set to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH), you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slower.
- Note that some transform sets might not be supported by the IPSec peer.

**Note** If a user enters an IPSec transform set that the hardware does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform set but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform set combinations follow:

- **esp-aes** and **esp-sha-hmac**
- **esp-aes 256** and **esp-sha-hmac**

### The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, see the **match address** (IPSec) and **mode** (IPSec) command descriptions.

### Changing Existing Transform Sets

If one or more transform sets are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transform sets will replace the existing transform sets for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

### Default Transform Set

You can modify the default transform-set using the **crypto ipsec transform-set default** command. You can disable the default transform-set using the **no crypto ipsec transform-set default** command.

If you do not specify a transform-set, the default transform-set is used with the default profile.

## Examples

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that supports only the older transforms.

```
Router (config)# crypto ipsec transform-set newer esp-aes esp-sha-hmac
Router (config)# crypto ipsec transform-set older ah-md5-hmac esp-des
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform set that the hardware does not support:

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-sha-hmac
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

The following output example shows that SEAL encryption has been correctly configured with an authentication transform set:

```
Router (config)# crypto ipsec transform-set seal esp-seal esp-sha-hmac
```

The following example is a warning message that is displayed when SEAL encryption has been configured with a crypto accelerator present:

```
Router (config)# show running-config
crypto ipsec transform-set seal esp-seal esp-sha-hmac
! Disabled because transform not supported by encryption hardware
```

The following example is an error message that is displayed when SEAL encryption has been configured without an authentication transform set:

```
Router (config)# crypto ipsec transform seal esp-seal
ERROR: Transform requires either ESP or AH authentication.
```

The following example is an error message that is displayed when SEAL encryption has been configured within a manually keyed crypto map:

```
Router (config)# crypto map green 10 ipsec-manual
%Note: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router (config-crypto-map)# set transform seal
ERROR: transform seal illegal for a manual crypto map.
```

## Related Commands

| Command | Description |
|---|---|
| **clear crypto sa** | Deletes IPSec security associations. |
| **crypto ipsec transform-set** | Defines a transform set--an acceptable combination of security protocols and algorithms. |
| **match address** | Specifies an extended access list for a crypto map entry. |
| **mode (IPSec)** | Changes the mode for a transform set. |
| **set transform-set** | Specifies which transform sets can be used with the crypto map entry. |
| **show crypto ipsec transform-set** | Displays the configured transform sets. |



# crypto isakmp aggressive-mode disable through crypto mib topn


- crypto isakmp aggressive-mode disable, on page 729
- crypto isakmp client configuration address-pool local, on page 730
- crypto isakmp client configuration browser-proxy, on page 731
- crypto isakmp client configuration group, on page 732
- crypto isakmp client firewall, on page 737
- crypto isakmp default policy, on page 739
- crypto isakmp enable, on page 742
- crypto isakmp fragmentation, on page 744
- crypto isakmp identity, on page 745
- crypto isakmp invalid-spi-recovery, on page 747
- crypto isakmp keepalive, on page 748
- crypto isakmp key, on page 751
- crypto isakmp nat keepalive, on page 754
- crypto isakmp peer, on page 756
- crypto isakmp policy, on page 758
- crypto isakmp profile, on page 761
- crypto key decrypt rsa, on page 764
- crypto key encrypt rsa, on page 765
- crypto key export ec, on page 767
- crypto key export rsa pem, on page 770
- crypto key generate ec keysize, on page 773
- crypto key generate rsa, on page 775
- crypto key import ec, on page 781
- crypto key import rsa pem, on page 783
- crypto key lock rsa, on page 787
- crypto key move rsa, on page 789
- crypto key pubkey-chain rsa, on page 791
- crypto key storage, on page 793
- crypto key unlock rsa, on page 795
- crypto key zeroize ec, on page 797
- crypto key zeroize pubkey-chain, on page 799

- crypto key zeroize rsa, on page 800
- crypto keyring, on page 802
- crypto logging ezvpn, on page 803
- crypto logging ikev2, on page 804
- crypto logging session, on page 805
- crypto map (global IPsec), on page 806
- crypto map (interface IPsec), on page 813
- crypto map (Xauth), on page 816
- crypto map client configuration address, on page 818
- crypto map gdoi fail-close, on page 819
- crypto map (isakmp), on page 821
- crypto map isakmp-profile, on page 823
- crypto map local-address, on page 824
- crypto map redundancy replay-interval, on page 826
- crypto mib ipsec flowmib history failure size, on page 828
- crypto mib ipsec flowmib history tunnel size, on page 829
- crypto mib topn, on page 830

# crypto isakmp aggressive-mode disable

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the **crypto isakmp aggressive-mode disable** command in global configuration mode. To disable the blocking, use the **no** form of this command.

**crypto isakmp aggressive-mode disable**
**no crypto isakmp aggressive-mode disable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections. In addition, if the device has been configured with the **crypto isakmp peer address** and the **set aggressive-mode password**or **set aggressive-mode client-endpoint**commands, the device will initiate aggressive mode if this command is not configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(1) | This command was introduced on all Cisco IOS platforms that support IP Security (IPSec). |

## Usage Guidelines

If you configure this command, all aggressive mode requests to the device and all aggressive mode requests made by the device are blocked, regardless of the ISAKMP authentication type (preshared keys or Rivest, Shamir, and Adelman [RSA] signatures).

If a request is made by or to the device for aggressive mode, the following syslog notification is sent:

```
Unable to initiate or respond to Aggressive Mode while disabled
```



**Note** This command will prevent Easy Virtual Private Network (Easy VPN) clients from connecting if they are using preshared keys because Easy VPN clients (hardware and software) use aggressive mode.

## Examples

The following example shows that all aggressive mode requests to and from a device are blocked:

```
Router (config)# crypto isakmp aggressive-mode disable
```

# crypto isakmp client configuration address-pool local

To configure the IP address local pool to reference Internet Key Exchange (IKE) on your router, use the **crypto isakmp client configuration address-pool local**command in global configuration mode. To restore the default value, use the **no** form of this command.

**crypto isakmp client configuration address-pool local** *pool-name*
**no crypto isakmp client configuration address-pool local**

## Syntax Description

| | |
|---|---|
| *pool-name* | Specifies the name of a local address pool. |

## Command Default

IP address local pools do not reference IKE.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(4)XE | This command was introduced. |
| 12.0(7)T | This command was integrated into Cisco IOS release 12.0(7)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example references IP address local pools to IKE on your router, with “ire” as the *pool-name*:

```
crypto isakmp client configuration address-pool local ire
```

## Related Commands

| Command | Description |
|---|---|
| **ip local pool** | Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface. |

# crypto isakmp client configuration browser-proxy

To configure browser-proxy parameters for an Easy VPN remote device and to enter ISAKMP browser proxy configuration mode, use the **crypto isakmp client configuration browser-proxy** command in global configuration mode. To disable the browser-proxy parameters, use the **no** form of this command.

**crypto isakmp client configuration browser-proxy** *browser-proxy-name*
**no crypto isakmp client configuration browser-proxy** *browser-proxy-name*

## Syntax Description

| | |
|---|---|
| *browser-proxy-name* | Name of the browser proxy. |

## Command Default

Browser-proxy parameters are not set.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Usage Guidelines

While specifying the proxy server, the proxy IP address and port number are separated with a colon. The proxy exception list is a semicolon-delimited string of IP addresses.

After enabling this command, you may specify the following subcommand:

- **proxy** --Configures proxy parameters for your Easy VPN remote device (see the **proxy** command for more information about this command and the acceptable parameters).

## Examples

The following example shows various browser-proxy parameter settings for a browser proxy named "bproxy":

```
crypto isakmp client configuration browser-proxy bproxy
 proxy auto-detect
crypto isakmp client configuration browser-proxy bproxy
 proxy none
crypto isakmp client configuration browser-proxy bproxy
 proxy server 10.1.1.1:2000
 proxy exception-list 10.2.2.*,www.*org
 proxy by-pass-local
```

## Related Commands

| Command | Description |
|---|---|
| **proxy** | Configures proxy parameters for an Easy VPN remote device. |

# crypto isakmp client configuration group

To specify to which group a policy profile will be defined and to enter crypto ISAKMP group configuration mode, use the **crypto isakmp client configuration group** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

**crypto isakmp client configuration group** {*group-name* | **default**}
**no crypto isakmp client configuration group**

## Syntax Description

| | |
|---|---|
| *group-name* | Group definition that identifies which policy is enforced for users. |
| default | Policy that is enforced for all users who do not offer a group name that matches a group-name argument. The default keyword can only be configured locally. |

## Command Default

No default behavior or values

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.3(2)T | The **access-restrict**, **firewall are-u-there**, **group-lock**, **include-local-lan**, and **save-password** commands were added. These commands are added during Mode Configuration. In addition, this command was modified so that output for this command will show that the preshared key is either encrypted or unencrypted. |
| 12.3(4)T | The **backup-gateway**, **max-logins**, **max-users , and pfs** commands were added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(2)T | The **browser-proxy** command was added. |
| 12.4(6)T | The **firewall policy** command was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(9)T | The **crypto aaa attribute list**, **dhcp server,**and **dhcp timeout** commands were added. |
| 12.4(11)T | The **dhcp giaddr**command was added. |

## Usage Guidelines

Use the **crypto isakmp client configuration group command to specify group policy information that needs to be defined or changed. You may wish to change the group policy on your router if you decide to connect to the client using a group ID that does not match the** *group-name*argument.

**After enabling this command, which puts you in** Internet Security Association Key Management Protocol (ISAKMP) **group configuration mode, you can specify characteristics for the group policy using the following commands:**

- **access-restrict--Ties a particular Virtual Private Network (VPN) group to a specific interface for access to the Cisco IOS gateway and the services it protects.**
- **acl** --Configures split tunneling.
- **auto-update client** --Configures auto upgrade.
- **backup-gateway** --Configures a server to "push down" a list of backup gateways to the client. These gateways are tried in order in the case of a failure of the previous gateway. The gateways may be specified using IP addresses or host names.
- **banner** --Specifies a mode configuration banner.
- **browser-proxy** --Applies a browser-proxy map to a group.
- **configuration url** --Specifies on a server the URL an Easy VPN remote device must use to get a configuration in a Mode Configuration Exchange.
- **configuration version** --Specifies on a server the version a Cisco Easy VPN remote device must use to get a particular configuration in a Mode Configuration Exchange.
- **crypto aaa attribute list** --Defines a AAA attribute list of per-user attributes on a local Easy VPN server.
- **dhcp giadd** r--Configures an IP address on the Easy VPN server for the Dynamic Host Configuration Protocol (DHCP) to use. The DHCP server uses the giaddr keyword to determine the scope for the client IP address assignment. If the giaddr keyword is not configured, the Easy VPN server must be configured with a loopback interface to communicate with the DHCP server, and the IP address on the loopback interface determines the scope for the client IP address assignment.
- **dhcp server** --Configures multiple DHCP server entries.
- **dhcp timeout** --Controls the wait time before the next DHCP server on the list is tried.
- **dns** --Specifies the primary and secondary Domain Name Service (DNS) servers for the group.
- **domain** --Specifies group domain membership.
- **firewall are-u-there**-- Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
- **firewall policy** --Specifies the CPP firewall policy push name for the crypto ISAKMP client configuration group on a local AAA server.
- **group-lock--Use if preshared key authentication is used with** Internet Key Exchange (**IKE). Allows you to enter your extended authentication (Xauth) username. The group delimiter is compared against the group identifier sent during IKE aggressive mode.**
- **include-local-lan** --Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
- **key** --Specifies the IKE preshared key when defining group policy information for Mode Configuration push.
- **max-logins** --Limits the number of simultaneous logins for users in a specific user group.
- **max-users** --Limits the number of connections to a specific server group.
- **netmask** --Subnet mask to be used by the client for local connectivity.

- **pfs** --Configures a server to notify the client of the central-site policy regarding whether PFS is required for any IPsec SA. Because the client device does not have a user interface option to enable or disable PFS negotiation, the server will notify the client device of the central site policy via this parameter. The Diffie-Hellman (D-H) group that is proposed for PFS will be the same that was negotiated in Phase 1 of the IKE negotiation.
- **pool** --Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **save-password** --Saves your Xauth password locally on your PC.
- **split-dns** --Specifies a list of domain names that must be tunneled or resolved to the private network.
- **wins** --Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

Output for the **crypto isakmp client configuration group** command (using the **key** subcommand) will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp client configuration group key test
```

An output example for a type 6 encrypted preshared key would be as follows:

crypto isakmp client configuration group

```
 key 6 JK_JHZPeJV_XFZTKCQFYAAB
```

**Session Monitoring and Limiting for Easy VPN Clients**

It is possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group and also for limiting the number of simultaneous logins for users in that group.

To limit the number of connections to a specific server group, use the **max-users** subcommand. To limit the number of simultaneous logins for users in the server group, use the **max-logins** subcommand.

The following example shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

The **max-users** and **max-logins** commands can be enabled together or individually to control the usage of resources by any groups or individuals.

If you use a RADIUS server, such as a CiscoSecure access control server (ACS), it is recommended that you enable this session control on the RADIUS server if the functionality is provided. In this way, usage can be controlled across a number of servers by one central repository. When enabling this feature on the router itself, only connections to groups on that specific device are monitored, and load-sharing scenarios are not accurately accounted for.

## Examples

The following example shows how to define group policy information for Mode Configuration push. In this example, the first group name is “cisco” and the second group name is “default.” Thus, the default policy will be enforced for all users who do not offer a group name that matches “cisco.”

```
crypto isakmp client configuration group cisco
```

```
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 domain cisco.com
 pool fred
 acl 199
!
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool fred
 acl 199
```

## Related Commands

| Command | Description |
|---|---|
| **access-restrict** | Ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it protects. |
| **acl** | Configures split tunneling. |
| backup-gateway | Configures a server to “push down” a list of backup gateways to the client. |
| browser-proxy | Applies browser-proxy parameter settings to a group. |
| **crypto isakmp keepalive** | Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls. |
| **dns** | Specifies the primary and secondary DNS servers. |
| **domain (isakmp-group)** | Specifies the DNS domain to which a group belongs. |
| **firewall are-u-there** | Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls. |
| firewall policy | Specifies the CPP firewall policy push name for the crypto ISAKMP client configuration group on a local AAA server. |
| **group-lock** | Allows you to enter your Xauth username, including the group name, when preshared key authentication is used with IKE. |
| **include-local-lan** | Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client. |
| **key (isakmp-group)** | Specifies the IKE preshared key for Group-Policy attribute definition. |
| max-logins | Limits the number of simultaneous logins for users in a specific server group. |
| max-users | Limits the number of connections to a specific server group. |
| **pool (isakmp-group)** | Defines a local pool address. |
| **save-password** | Saves your Xauth password locally on your PC. |

| Command | Description |
|---|---|
| **set aggressive-mode client-endpoint** | Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration. |

# crypto isakmp client firewall

To define the Central Policy Push (CPP) firewall policypush on a server, use the **crypto isakmp client firewall** command in global configuration mode. To remove the CPP that was configured, use the **no** form of this command.

**crypto isakmp client firewall** *policy-name* {**required** | **optional**} *firewall-type*
**nocrypto isakmp client firewall** *policy-name* {**required** | **optional**} *firewall-type*

## Syntax Description

| | |
|---|---|
| *policy-name* | Uniquely identifies a policy. A policy name can be associated with an Easy VPN client group configuration on the server (local group configuration) or on the authentication, authorization, and accounting (AAA) server. |
| **required** | Policy is mandatory. If the CPP policy is defined as mandatory and is included in the Easy VPN server configuration, the tunnel setup is allowed only if the Cisco VPN Client confirms this policy. If the policy is not confirmed, the tunnel is terminated. |
| **optional** | Policy is optional. If the CPP policy is defined as optional and is included in the Easy VPN server configuration, the tunnel setup continues even if the Cisco VPN Client does not confirm the defined policy. |
| *firewall-type* | Type of firewall. See the table below for a list of acceptable firewall types. |

## Command Default

CPP is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The table below lists firewall types that may be used for the *firewall-type* argument.

***Table 25: Acceptable Firewall Types***

| Firewall Type |
|---|
| Cisco-Integrated-firewall (central-policy-push) |
| Cisco-Security-Agent (check-presence) |
| Zonelabs-Zonealarm (both) |
| Zonelabs-ZonealarmPro (both) |

## Examples

The following example defines the CPP policy name as “hw-client-g-cpp.” The “Cisco-Security-Agent” policy type is mandatory. The CPP inbound list is “192” and the outbound list is “sample”:

```
crypto isakmp client firewall hw-client-g-cpp required Cisco-Security-Agent
 policy central-policy-push access-list in 192
 policy central-policy-push access-list out sample
 policy check-presence
```

## Related Commands

| Command | Description |
|---|---|
| **policy** | Specifies the CPP policy. |

# crypto isakmp default policy

To enable default policies for Internet Security Association and Key Management Protocol (ISAKMP) protection suite, use the **crypto isakmp default policy** command in global configuration mode. To disable the default IKE policies, use the **no** form of this command.

**crypto isakmp default policy**
**no crypto isakmp default policy**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default ISAKMP policies are enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

If you have neither manually configured ISAKMP policies with the **crypto isakmp policy** command nor issued the **no crypto isakmp default policy** command, IPsec will use the default ISAKMP policies to negotiate IKE proposals. There are eight default ISAKMP default policies supported (see the table below). The default ISAKMP policies define the following policy set parameters:

- The priority, 65507-65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).
- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The Diffie-Hellman (DH) group specification DH2 or DH5.
  - DH2 specifies the 768-bit Diffie-Hellman group.
  - DH5 specifies the 1536-bit Diffie-Hellman group.

*Table 26: Default ISAKMP Policies*

| Priority | Authentication | Encryption | Hash | Diffie-Hellman |
|---|---|---|---|---|
| 65507 | RSA | AES | SHA | DH5 |
| 65508 | PSK | AES | SHA | DH5 |
| 65509 | RSA | AES | MD5 | DH5 |
| 65510 | PSK | AES | MD5 | DH5 |
| 65511 | RSA | 3DES | SHA | DH2 |
| 65512 | PSK | 3DES | SHA | DH2 |
| 65513 | RSA | 3DES | MD5 | DH2 |
| 65514 | PSK | 3DES | MD5 | DH2 |

## Examples

The following example disables the default ISAKMP policies and shows the resulting output of the **show crypto isakmp default policy** command, which is blank:

```
Router#
configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router#show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.
```

The following example enables the default ISAKMP policies and displays the resulting output of the **show crypto isakmp default policy** command. The default policies are displayed because there are no user configured policies, and the default policies have not been disabled.

```
Router#
configure terminal
Router(config)# crypto isakmp default policy
Router(config)#exit
Router# show crypto isakmp default policy
Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
```

```
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto isakmp default policy** | Displays the default ISAKMP policies currently in use. |

# crypto isakmp enable

To globally enable Internet Key Exchange (IKE) for your peer router, use the **crypto isakmp enable**command in global configuration mode. To disable IKE for the peer, use the **no** form of this command.

**crypto isakmp enable**
**no crypto isakmp enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IKE is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

If you do not want IKE to be used for your IPSec implementation, you can disable IKE for all your IP Security peers. If you disable IKE for one peer, you must disable it for all IPSec peers.

If you disable IKE, you will have to make these concessions at the peers:

- You must manually specify all the IPSec security associations (SAs) in the crypto maps at the peers. (Crypto map configuration is described in the chapter "Configuring IPSec Network Security" in the *Cisco IOS Security Configuration Guide* .)
- The IPSec SAs of the peers will never time out for a given IPSec session.
- During IPSec sessions between the peers, the encryption keys will never change.
- Anti-replay services will not be available between the peers.
- Certification authority (CA) support cannot be used.



**Note** Effective with Cisco IOS Release 12.3(2)T, a device is prevented from responding to Internet Security Association and Key Management Protocol (ISAKMP) by default unless there is a crypto map applied to an interface or if Easy VPN is configured.

## Examples

The following example disables IKE at one peer. (The same command should be issued for all remote peers.)

```
no crypto isakmp enable
```

# crypto isakmp fragmentation

To enable fragmentation of large Internet Key Exchange (IKE) packets into a series of smaller IKE packets to avoid fragmentation at the User Datagram Protocol (UDP) layer, use the **crypto isakmp fragmentation** command in global configuration mode. To disable fragmentation, use the **no** form of this command.

**crypto isakmp fragmentation**
**no crypto isakmp fragmentation**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Fragmentation is not allowed.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T7 | This command was introduced. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Do not configure IKE fragmentation on a Cisco IOS router with Cisco Easy VPN Client versions 5.01 through 5.03. Versions earlier than version 5.01 and version 5.04 or a later release should be all right.

**Note** The **crypto isakmp fragmentation** command is only applicable when the IOS Router is acting as an Easy VPN server and the remote peer is a Cisco IPsec VPN client.

## Examples

The following example shows that fragmentation has been enabled:

```
crypto isakmp fragmentation
crypto isakmp policy 1
  encryption 3des
crypto isakmp profile ezvpn-SW
  match group frag-clients
  vrf frags
```

# crypto isakmp identity

To define the ISAKMP identity used by the router when participating in the Internet Key Exchange (IKE) protocol, use the **crypto isakmp identity** command in global configuration mode. To reset the ISAKMP identity to the default value (address), use the **no** form of this command.

**crypto isakmp identity** {**address** | **dn** | **hostname**}
**no crypto isakmp identity**

## Syntax Description

| | |
|---|---|
| **address** | Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations. |
| dn | Sets the ISAKMP identity to the distinguished name (DN) of the router certificate. |
| **hostname** | Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com). |

## Command Default

The IP address is used for the ISAKMP identity.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3T | This command was introduced. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to specify an ISAKMP identity either by IP address, DN or host name. An ISAKMP identity is set whenever you specify preshared keys or RSA signature authentication.

The **address** keyword is typically used when only one interface (and therefore only one IP address) will be used by the peer for IKE negotiations, and the IP address is known.

The dn keyword should be used if the DN of a router certificate is to be specified and chosen as the ISAKMP identity during IKE processing. The dn keyword is used only for certificate-based authentication.

The **hostname** keyword should be used if more than one interface on the peer might be used for IKE negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).

As a general rule, you should set all peers' identities in the same way, either by IP address or by host name.

## Examples

The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
```

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
```



**Note** In the preceding example if the **crypto isakmp identity** command had not been performed, the ISAKMP identities would have still been set to IP address, the default identity.

The following example uses preshared keys at two peers and sets both their ISAKMP identities to the hostname.

At the local peer the ISAKMP identity is set and the preshared key is specified:

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname RemoteRouter.example.com
ip host RemoteRouter.example.com 192.168.0.1
```

At the remote peer the ISAKMP identity is set and the same preshared key is specified:

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname LocalRouter.example.com
ip host LocalRouter.example.com 10.0.0.1 10.0.0.2
```

In the example, hostnames are used for the peers' identities because the local peer has two interfaces that might be used during an IKE negotiation.

In the example the IP addresses are also mapped to the hostnames; this mapping is not necessary if the routers' hostnames are already mapped in DNS.

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec security-association lifetime** | Specifies the authentication method within an IKE policy. |
| **crypto isakmp key** | Configures a preshared authentication key. |

# crypto isakmp invalid-spi-recovery

To initiate the Internet Key Exchange (IKE) security association (SA) to notify the receiving IP Security (IPSec) peer that there is an "Invalid SPI" error, use the **crypto isakmp invalid-spi-recovery** command in global configuration mode. To disable the notification process, use the **no** form of this command.

**crypto isakmp invalid-spi-recovery**
**no crypto isakmp invalid-spi-recovery**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The IKE notification process is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

This command allows you to configure your router so that when an invalid security parameter index error (shown as "Invalid SPI") occurs, an IKE SA is initiated. The "IKE" module, which serves as a checkpoint in the IPSec session, recognizes the "Invalid SPI" situation. The IKE module then sends an "Invalid Error" message to the packet-receiving peer so that synchronization of the security association databases (SADBs) of the two peers can be attempted. As soon as the SADBs are resynchronized, packets are no longer dropped.

**Note** SPI recovery initiates a new IKE SA only for static peers.

**Caution** Using this command to initiate an IKE SA to notify an IPSec peer of an "Invalid SPI" error can result in a denial-of-service (DoS) attack.

## Examples

The following example shows that the IKE module process has been initiated to notify the receiving peer that there is an "Invalid SPI" error:

```
Router (config)# crypto isakmp invalid-spi-recovery
```

# crypto isakmp keepalive

To allow the gateway to send dead peer detection (DPD) keepalive messages to the peer, use the **crypto isakmp keepalive**command in global configuration mode. To disable keepalives, use the **no** form of this command.

**crypto isakmp keepalive** *seconds* [*retry-seconds*] [**periodic** | **on-demand**]
**no crypto isakmp keepalive** *seconds* [*retry-seconds*] [**periodic** | **on-demand**]

## Syntax Description

| | |
|---|---|
| *seconds* | When the **periodic** keyword is used, this argument is the number of seconds between DPD messages; the range is from 10 to 3600 seconds.<br>When the **on-demand** keyword is used, this argument is the number of seconds during which traffic is not received from the peer before DPD retry messages are sent if there is data (IPSec) traffic to send; the range is from 10 to 3600 seconds.<br>**Note**<br>If you do not specify a time interval, an error message appears. |
| *retry-seconds* | (Optional) Number of seconds between DPD retry messages if the DPD retry message is missed by the peer; the range is from 2 to 60 seconds.<br>Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down.<br>**Note**<br>To configure DPD with IPsec High Availability (HA), the recommendation is to use a value other than the default (which is 2 seconds). A keepalive timer of 10 seconds with 5 retries seems to work well with HA because of the time that it takes for the router to get into active mode. |
| **periodic** | (Optional) DPD messages are sent at regular intervals. |
| **on-demand** | (Optional) The default behavior. DPD retries are sent on demand.<br>**Note**<br>Because this option is the default, the **on-demand** keyword does not appear in configuration output. |

## Command Default

No DPD messages are sent.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |

| Release | Modification |
|---|---|
| 12.3(7)T | The **periodic** and **on-demand** keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the crypto isakmp keepalive command to enable the gateway to send DPD messages to the peer. DPD is a keepalives scheme that allows the router to query the liveliness of its Internet Key Exchange (IKE) peer.

Use the **periodic** keyword to configure your router so that DPD messages are "forced" at regular intervals. This forced approach results in earlier detection of dead peers than with the on-demand approach. If you do not configure the periodic option, the router defaults to the on-demand approach.

**Note** When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

**Note** Cisco IOS VPN Client connections are not supported if you configure the **crypto isakmp keepalive** command with the **periodic** keyword on a Cisco IOS device.

## Examples

The following example shows how to configure DPD messages to be sent every 60 seconds and a DPD retry message every 3 seconds between retries if the peer does not respond one time:

```
crypto isakmp keepalive 60 3
```

The 60 indicates that a keepalive or DPD message is sent every 60 seconds. Once a DPD message is missed by the peer, the router moves to a more aggressive state, sending DPD retry messages every 3 seconds. After 5 aggressive DPD retries, the tunnel is marked as down.

In this example, if the router has sent a DPD message at time *x* and has not received a response within *x* + 60, then the DPD retry is sent again at *x* + 60 and then aggressively at time intervals of *x* + 63, *x* + 66, *x* + 69, and *x* + 72. At *x* + 75, a decision is made by the router to bring down the tunnel and DELETE payload is sent to the peer. The DPD retry message is not sent at *x* + 75 and only DELETE payload is sent. Therefore, the number of aggressive DPD retry messages that can be missed before marking the tunnel as down is 5 (sent at intervals *x* + 60, *x* + 63, *x* +66, *x* + 69, and *x* + 72).

The following example shows that periodic DPD messages are to be sent at intervals of 10 seconds:

```
crypto isakmp keepalive 10 periodic
```

The following example shows that the above periodic behavior is being disabled:

```
crypto isakmp keepalive 10 on-demand
```

The following example shows that DPD has been configured with IPsec HA. The number of seconds between DPD messages is 10, and the number of seconds between DPD retries is 5. DPD messages are to be sent at regular intervals.

```
crypto isakmp keepalive 10 5 periodic
```

## Related Commands

| Command | Description |
|---|---|
| **acl** | Configures split tunneling. |

# crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key command in**global configuration mode. To delete a preshared authentication key, use the **no** form of this command.

**crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** *ipv6-address / ipv6-prefix* | **hostname** *hostname*} [**no-xauth**]
**no crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** *ipv6-address / ipv6-prefix* | **hostname** *hostname*} [**no-xauth**]

## Syntax Description

| | |
|---|---|
| *enc-type-digit* | Specifies whether the password to be used is encrypted or unencrypted.<br>• 0--Specifies that an unencrypted password follows.<br>• 6--Specifies that an encrypted password follows. |
| *keystring* | Specifies the preshared key. Use any combination of alphanumeric or special characters up to 128 bytes. Special characters include the following: !?"#$%&'()*+,-./:;<=>@[\]^_`~. (Type “CTRL-V” before the “?” symbol to avoid invoking help.) This preshared key must be identical at both peers. |
| **address** | Use this keyword if the remote peer Internet Security Association Key Management Protocol (ISAKMP) identity was set with its IP or IPv6 address. The *peer-address*argument specifies the IP or IPv6 address of the remote peer. |
| *peer-address* | Specifies the IP address of the remote peer. |
| *mask* | (Optional) Specifies the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.) |
| **ipv6** | Specifies that an IPv6 address of a remote peer will be used. |
| *ipv6-address* | IPv6 address of the remote peer.<br>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| *ipv6-prefix* | IPv6 prefix of the remote peer. |
| **hostname** *hostname* | Fully qualified domain name (FQDN) of the peer. The **hostname** keyword and *hostname* argument are not supported by IPv6. |
| **no-xauth** | (Optional) Use this keyword if router-to-router IP Security (IPSec) is on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco-IOS IPSec. This keyword prevents the router from prompting the peer for extended authentication (Xauth) information (username and password). |

## Command Default

There is no default preshared authentication key.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3T | This command was introduced. |
| 12.1(1)T | The mask argument was added. |
| 12.2(4)T | The **no-xauth** keyword was added. |
| 12.3(2)T | This command was modified so that output shows that the preshared key is either encrypted or unencrypted. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(4)T | The **ipv6** keyword and the *ipv6-address* and *ipv6-prefix* arguments were added. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

## Usage Guidelines

You must use this command to configure a key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy; you must enable this command at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers--otherwise the policy cannot be used (the policy will not be submitted for matching by the IKE process). The **crypto isakmp key** command is the second task required to configure the preshared keys at the peers. (The first task is accomplished using the **crypto isakmp identity** command.)

Use the **address** keyword if the remote peer ISAKMP identity was set with its IP address.

With the address keyword, you can also use the mask argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the mask argument is used, preshared keys are no longer restricted between two users.



**Note** If you specify mask, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

When using IKE main mode, preshared keys are indexed by IP address only because the identity payload has not yet been received. This means that the hostname keyword in the identity statement is not used to look up a preshared key and will be used only when sending and processing the identity payloads later in the main mode exchange. The identity keyword can be used when preshared keys are used with IKE aggressive mode, and keys may be indexed by identity types other than IP address as the identity payload is received in the first IKE aggressive mode packet.

If **crypto isakmp identity hostname** is configured as identity, the preshared key must be configured with the peer's IP address for the process to work when using IKE in main mode.

Use the **no-xauth** keyword to prevent the router from prompting the peer for Xauth information (username and password). This keyword disables Xauth for static IPSec peers. The **no-xauth** keyword should be enabled when configuring the preshared key for router-to-router IPSec--not VPN-client-to-Cisco-IOS IPSec.

Output for the **crypto isakmp key** command will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp key test123 address 10.1.0.1
```

An output example for a type 6 encrypted preshared key would be as follows:

```
crypto isakmp key 6 RHZE[JACMUI\bcbTdELISAAB address 10.1.0.1
```

## Examples

In the following example, the remote peer "RemoteRouter" specifies an ISAKMP identity by address:

```
crypto isakmp identity address
```

Now, the preshared key must be specified at each peer.

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
crypto isakmp key 0 sharedkeystring address 172.21.230.33  255.255.255.255
```

In the following example for IPv6, the peer specifies the preshared key and designates the remote peer with an IPv6 address:

```
crypto isakmp key 0 my-preshare-key-0 address ipv6 3ffe:1001::2/128
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec security-association lifetime** | Specifies the authentication method within an IKE policy. |
| **crypto isakmp identity** | Defines the identity the router uses when participating in the IKE protocol. |
| **ip host** | Defines a static host name-to-address mapping in the host cache. |

# crypto isakmp nat keepalive

To allow an IPsec node to send Network Address Translation (NAT) keepalive packets, use the **crypto isakmp nat keepalive** command in global configuration mode. To disable NAT keepalive packets, use the **no** form of this command.

**crypto isakmp nat keepalive** *seconds*
**no crypto isakmp nat keepalive**

## Syntax Description

| | |
|---|---|
| *seconds* | Number of seconds between keepalive packets; the range is from 5 to 3600. |

## Command Default

NAT keepalive packets are not sent.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

The **crypto isakmp nat keepalive** command allows users to keep the dynamic NAT mapping alive during a connection between two peers. A NAT keepalive packet is sent by the peer that is behind the NAT device if IPsec does not send or receive a packet within a specified time period. With CSCul35051, if both peers are behind their respective NAT devices, each peer sends NAT keepalive packets according to its configured interval.

If this command is enabled, users should ensure that the idle value is shorter than the NAT mapping expiration time.

**Note** When the timer is modified, it is modified for every Internet Security Association Key Management Protocol (ISAKMP) security association (SA) when the keepalive for that SA is sent based on the existing timer.

**Note** A 5-percent jitter mechanism value is applied to the timer to avoid SA rekey collisions. If there are many peer devices, and the timer is configured too low, then the device can experience high CPU usage.

## Examples

The following example shows how to enable NAT keepalives to be sent every 20 seconds:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 209.165.202.130
crypto isakmp nat keepalive 20
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
no crypto engine accelerator
!
crypto map test2 10 ipsec-isakmp
```

```
set peer 209.165.202.130
set transform-set t2
match address 101
```

# crypto isakmp peer

To enable an IP Security (IPSec) peer for Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto isakmp peer** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**crypto isakmp peer** {**address** {*ipv4-address* | **ipv6** *ipv6-address*} | **hostname** *fqdn-hostname*}
**no crypto isakmp peer** {**address** {*ipv4-address* | **ipv6** *ipv6-address*} | **hostname** *fqdn-hostname*}

## Syntax Description

| | |
|---|---|
| **address** *ip-address* | Address of the peer router. |
| *ipv4-address* | IPv4 address of the peer router. |
| **ipv6** *ipv6-address* | IPv6 address of the peer router. |
| **hostname** | Hostname of the peer router. |
| *fqdn-hostname* | Fully qualified domain name (FQDN) of the peer router. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.2(15)T | The **vrf** keyword and *fvrf-name*argument were added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(4)T | The **ipv6** keyword and *ipv6-address* argument were added. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

## Usage Guidelines

After enabling this command, you can use the **set aggressive-mode client-endpoint** and **set aggressive-mode password** commands to specify RADIUS tunnel attributes in the Internet Security Association and Key Management Protocol (ISAKMP) peer policy for IPSec peers.

Instead of keeping your preshared keys on the hub router, you can scale your preshared keys by storing and retrieving them from an AAA server. The preshared keys are stored in the AAA server as Internet Engineering Task Force (IETF) RADIUS tunnel attributes and are retrieved when a user tries to “speak” to the hub router. The hub router retrieves the preshared key from the AAA server and the spokes (the users) initiate aggressive mode to the hub by using the preshared key that is specified in the ISAKMP peer policy as a RADIUS tunnel attribute.

## Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer ip-address 209.165.200.230 vrf vpn1
```

```
set aggressive-mode client-endpoint user-fqdn user@cisco.com
set aggressive-mode password cisco123
```

## Related Commands

| Command | Description |
|---|---|
| **crypto map isakmp authorization list** | Enables IKE querying of AAA for tunnel attributes in aggressive mode. |
| **set aggressive-mode client-endpoint** | Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration. |
| **set aggressive-mode password** | Specifies the Tunnel-Password attribute within an ISAKMP peer configuration. |

# crypto isakmp policy

To define an Internet Key Exchange (IKE) policy, use the **crypto isakmp policy** command in global configuration mode. To delete an IKE policy, use the **no** form of this command.

**crypto isakmp policy** *priority*
**no crypto isakmp policy** *priority*

## Syntax Description

| | |
|---|---|
| *priority* | Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest. |

## Command Default

Default IKE policies are in use.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.3T | This command was introduced. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | The command default was modified. Support for eight default IKE (ISAKMP) policies was added. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

IKE policies define a set of parameters to be used during the IKE negotiation. Use this command to specify the parameters to be used during an IKE negotiation. (These parameters are used to create the IKE security association [SA].)

This command invokes the Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) command mode. While in the ISAKMP policy configuration command mode, some of the commands for which you can specify parameters are as follows:

- **authentication** ; default = RSA signatures
- **encryption (IKE policy)** ; default = 56-bit DES-CBC

- **group (IKE policy)** ; default = 768-bit Diffie-Hellman
- **hash (IKE policy)** ; default = SHA-1
- **lifetime (IKE policy)** ; def ault = 86,400 seconds (one day)

If you do not specify any given parameter, the default value will be used for that parameter.

To exit the config-isakmp command mode, type **exit**.

You can configure multiple IKE policies on each peer participating in IPsec. When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.

## Examples

The following example shows how to manually configure two policies for the peer:

```
crypto isakmp policy 15
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
```

The above configuration results in the following policies:

```
Router# show crypto isakmp policy
Protection suite priority 15
 encryption algorithm: DES - Data Encryption Standard (56 bit keys)
 hash algorithm: Message Digest 5
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman Group: #2 (1024 bit)
 lifetime: 5000 seconds, no volume limit
Protection suite priority 20
 encryption algorithm: DES - Data Encryption Standard (56 bit keys)
 hash algorithm: Secure Hash Standard
 authentication method: preshared Key
 Diffie-Hellman Group: #1 (768 bit)
 lifetime: 10000 seconds, no volume limit
Default protection suite
 encryption algorithm: DES - Data Encryption Standard (56 bit keys)
 hash algorithm: Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman Group: #1 (768 bit)
 lifetime: 86400 seconds, no volume limit
```

The following sample output from the **show crypto isakmp policy** command displays the default IKE policies when the manually configured IKE policies with priorities 15 and 20 have been removed.

```
Router(config)# no crypto isakmp policy 15
Router(config)# no crypto isakmp policy 20
Router(config)# exit
R1# show crypto isakmp policy
Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
```

```
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

## Related Commands

| Command | Description |
|---|---|
| encryption (IKE policy) | Specifies the encryption algorithm within an IKE policy. |
| group (IKE policy) | Specifies the Diffie-Hellman group identifier within an IKE policy. |
| hash (IKE policy) | Specifies the hash algorithm within an IKE policy. |
| lifetime (IKE policy) | Specifies the lifetime of an IKE SA. |
| show crypto isakmp default policy | Displays the default IKE (ISAKMP) policies currently in use. |
| show crypto isakmp policy | Displays the parameters for each IKE policy. |

# crypto isakmp profile

To define an Internet Security Association and Key Management Protocol (ISAKMP) profile and to audit IP security (IPsec) user sessions, use the **crypto isakmp profile**command in global configuration mode. To delete a crypto ISAKMP profile, use the **no** form of this command.

**crypto isakmp profile** *profile-name*[**accounting** *aaa-list*][**per-user**]
**no crypto isakmp profile** *profile-name*[**accounting** *aaa-list*]

## Syntax Description

| | |
|---|---|
| *profile-name* | Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified. |
| **accounting** *aaa-list* | (Optional) Name of a client accounting list. |
| **per-user** | (Optional) To pull the interface attributes from the radius and apply the attributes over Virtual-Access. |

## Command Default

No profile exists if the command is not used.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(2)T | Support for dynamic virtual tunnel interfaces was added. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |
| Cisco IOS XE Release 16.8.1 | The optional keyword per-user was introduced. This keyword allows IKev1 to apply the per-user radius attributes on the Virtual-Access interfaces. |

## Usage Guidelines

### Defining an ISAKMP Profile

An ISAKMP profile can be viewed as a repository of Phase 1 and Phase 1.5 commands for a set of peers. The Phase 1 configuration includes commands to configure such things as keepalive, identity matching, and the authorization list. The Phase 1.5 configuration includes commands to configure such things as extended authentication (Xauth) and mode configuration.

The peers are mapped to an ISAKMP profile when their identities are matched (as given in the identification [ID] payload of the Internet Key Exchange [IKE]) against the identities defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid. Also, there must be at least one **match identity**command defined in the ISAKMP profile for it to be complete.

After enabling this command and entering ISAKMP profile configuration mode, you can configure the following commands:

- **accounting** --Enables authentication, authorization, and accounting (AAA) accounting.
- **ca trust-point** --Specifies certificate authorities.
- **client** --Specifies client configuration settings.
- **default** --Lists subcommands for the **crypto isakmp profile** command.
- **description** --Specifies a description of this profile.
- **initiate mode** --Initiates a mode.
- **isakmp authorization** --ISAKMP authorization parameters.
- **keepalive** --Sets a keepalive interval.
- **keyring** --Specifies a keyring.
- **local-address** --Specifies the interface to use as the local address of this ISAKMP profile.
- **match** --Matches the values of the peer.
- **qos-group** --Applies a quality of service (QoS) policy class map for this profile.
- **self-identity** --Specifies the identity.
- **virtual-template** --Specifies the virtual template for the dynamic interface.
- **vrf** --Specifies the Virtual Private Network routing and forwarding (VRF) instance to which the profile is related.

**Auditing IPSec User Sessions**

Use this command to audit multiple user sessions that are terminating on the IPSec gateway.



**Note** The **crypto isakmp profile** command and the **crypto map (global IPSec)**command are mutually exclusive. If a profile is present (the **crypto isakmp profile** command has been used), with no accounting configured but with the global command present (the **crypto isakmp profile** command without the **accounting** keyword), accounting will occur using the attributes in the global command.

**Dynamic Virtual Tunnel Interfaces**

Support for dynamic virtual tunnel interfaces allows for the virtual profile to be mapped into a specified virtual template.

**VRF-Aware IPsec**

You must include the VRF in the **local-address** command when using the local address with VRF in the ISAKMP profile and keyring.

### ISAKAMP Profile Matching Peer Identities Example

The following example shows how to define an ISAKMP profile and match the peer identities:

```
crypto isakmp profile vpnprofile
 match identity address 10.76.11.53
```

### ISAKAMP Profile with Accounting Example

The following accounting example shows that an ISAKMP profile is configured:

```
aaa new-model
!
!
aaa authentication login cisco-client group radius
aaa authorization network cisco-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
!
crypto isakmp profile cisco
vrf cisco
match identity group cclient
 client authentication list cisco-client
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
crypto dynamic-map dynamic 1
 set transform-set aswan
 set isakmp-profile cisco
 reverse-route
!
!
radius-server host 172.16.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
```

## Related Commands

| Command | Description |
|---|---|
| **crypto map (global IPsec)** | Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list. |
| **debug crypto isakmp** | Displays messages about IKE events. |
| **match identity** | Matches an identity from a peer in an ISAKMP profile. |
| **tunnel protection** | Associates a tunnel interface with an IP Security (IPsec) profile. |
| **virtual template** | Specifies which virtual template to be used to clone virtual access interfaces. |

# crypto key decrypt rsa

To delete the encrypted RSA key and leave only the unencrypted key on the running router, use the **crypto key decrypt rsa** command in global configuration mode.

**crypto key decrypt** [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

## Syntax Description

| | |
|---|---|
| **write** | (Optional) Clear text (unencrypted) key is immediately written to NvRAM.<br>If the **write** keyword is not issued, the configuration must be manually written to NvRAM; otherwise, the key will remain encrypted the next time the router is reloaded. |
| **name** *key-name* | (Optional) Name of the RSA key pair that is to be decrypted. |
| **passphrase** *passphrase* | Passphrase that is used to decrypt the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command. |

## Command Default

The private key running on the router is encrypted.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |

## Usage Guidelines

Use the **crypto key decrypt rsa** command to store the decrypted private key in NvRAM the next time NvRAM is written (which is immediately if the **write** keyword is issed).

## Examples

The following example shows how to decrypt the RSA key "pki1-72a.cisco.com":

```
Router(config)# crypto key decrypt write rsa name pki1-72a.cisco.com passphrase cisco1234
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key encrypt rsa** | Encrypts the RSA private key. |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of your router. |

# crypto key encrypt rsa

To encrypt the RSA private key, use the **crypto key encrypt rsa**command in global configuration mode.

**crypto key encrypt** [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

## Syntax Description

| | |
|---|---|
| **write** | (Optional) Router configuration is immediately written to NVRAM.<br>If the **write** keyword is not issued, the configuration must be manually written to NvRAM; otherwise, the encrypted key will be lost next time the router is reloaded. |
| **name** *key-name* | (Optional) Name of the RSA key pair that is to be encrypted.<br>If a key name is not specified, the default key name, *routername.domainname*, i s used. |
| **passphrase** *passphrase* | Passphrase that is used to encrypt the RSA key. To access the RSA key pair, the passphrase must be specified. |

## Command Default

RSA keys are not encrypted.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |

## Usage Guidelines

The private key is encrypted (protected) via the specified passphrase. After the key is protected, it may continue to be used by the router; that is Internet Key Exchange (IKE) tunnels and encrypted key export attempts should continue to work because the key remains “unlocked.”

To lock the key, which can be used to disable the router, issue the **crypto key lock rsa** privileged EXEC command. (When you lock the encrypted key, all functions which use the locked key are disabled.)

## Examples

The following example shows how to encrypt the RSA key “pki1-72a.cisco.com.” Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa
```

% Key pair was generated at:00:15:32 GMT Jun 25 2003

Key name:pki1-72a.cisco.com

Usage:General Purpose Key

*** The key is protected and UNLOCKED. ***

Key is not exportable.

Key Data:

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C

CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC

23C4D09E

03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001

% Key pair was generated at:00:15:33 GMT Jun 25 2003

Key name:pki1-72a.cisco.com.server

Usage:Encryption Key

Key is exportable.

Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383

854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757

3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4

DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001

```
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key decrypt rsa** | Deletes the encrypted RSA key and leaves only the unencrypted key on the running router. |
| **crypto key lock rsa** | Locks the RSA private key in a router. |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of your router. |

# crypto key export ec

To export an Elliptic Curve (EC) key pair, use the **crypto key export ec** command in global configuration mode.

**crypto key export ec** *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

## Syntax Description

| | |
|---|---|
| *key-label* | Name of the EC key pair to export.<br>The *key-label* argument must match the key pair name that was specified through the **crypto key generate ec keysize** command. |
| **pem** | Exports to a PEM-formatted file. |
| **terminal** | Displays the EC key pair in PEM format on the console terminal. |
| **url** *url* | Specifices the URL of the file system where the device should export the EC key pair. |
| **3des** | Exports the EC key pair using the Triple Data Encryption Standard (3DES) encryption algorithm. |
| **des** | Exports the EC key pair using the DES encryption algorithm. |
| *passphrase* | Specifies the passphrase to be used to encrypt the PEM file for import.<br>**Note**<br>The passphrase can be any phrase that is at least eight characters in length. It can include spaces and punctuation, excluding the question mark (?), which has special meaning to the parser. |

## Command Default

EC key pairs are not exported.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

IPsec and public key infrastructure (PKI) both support the ability to generate, export, and import EC (ECDSA-256 and ECDSA-384) key pairs. The **crypto key export ec** command lets you export EC key pairs to PEM-formatted files. Then, you can import the PEM files back into a Cisco IOS router or other PKI applications.



**Note** Before you export an EC key pair to a PEM file, ensure that the EC key pair is exportable. To generate an exportable EC key pair, use the **crypto key generate ec keysize** command and specify the **exportable** keyword.

## Examples

The following example shows how to generate, export, import, and verify the status of an EC key pair named Device_1_Key:

```
! Generate the key pair
!
Device(config)# crypto key generate ec keysize 256 exportable label Device_1_Key
The name for the keys will be: Device_1_Key

 EC key pair created successfully
!
! Archive the key pair to a remote location, and use a good password.
!
Device(config)# crypto key export ec Device_1_Key pem url nvram: 3des mypassword
% Key name: Device_1_Key
   Usage: Signature Key
Exporting public key...
Destination filename [Device_1_Key-sign.pub]?
Writing file to nvram:Device_1_Key-sign.pub
Exporting private key...
Destination filename [Device_1_Key-sign.prv]?
Writing file to nvram:Device_1_Key-sign.prv
!
! Import the key as a different name.
!
Device(config)# crypto key import ec Device_1_Key url nvram:Device_1_Key mypassword
% Importing public Signature key or certificate PEM file...
Source filename [Device_1_Key-sign.pub]?
Reading file from nvram:Device_1_Key-sign.pub
% Importing private Signature key PEM file...
Source filename [Device_1_Key-sign.prv]?
Reading file from nvram:Device_1_Key-sign.prv
% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Device# show crypto key mypubkey ec
% Key pair was generated at: 17:26:53 PST Jun 7 2012
Key name: Device_1_Key
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data:
  30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 420004A3 E483C98C
  BABE4CAD 9822F5F1 06FDFD4B F70D0103 03C266B6 DA368DB9 AB01C5AB 7333F5B9
  3478E0FE 6CA67598 FB828F47 A92AFE70 93EFE828 2620A611 699E52
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key generate ec keysize** | Generates EC key pairs. |

| Command | Description |
|---|---|
| **crypto key import ec** | Imports EC keys in PEM-formatted files. |
| **crypto key zeroize ec** | Deletes EC keys from a device. |

# crypto key export rsa pem

To export Rivest, Shamir, and Adelman (RSA) keys in privacy-enhanced mail (PEM)-formatted files, use the **crypto key export rsa pem**command in global configuration mode.

**crypto key export rsa** *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

## Syntax Description

| | |
|---|---|
| **rsa** *key-label* | Name of the RSA key pair that will be exported.<br>The *key-label* argument must match the key pair name that was specified through the **crypto key generate rsa** command. |
| **terminal** | RSA key pair will be displayed in PEM format on the console terminal. |
| **url** *url* | URL of the file system where the router should export the RSA key pair. |
| **3des** | Export the RSA key pair using the Triple Data Encryption Standard (3DES) encryption algorithm. |
| des | Export the RSA key pair using the DES encryption algorithm. |
| *passphrase* | Passphrase that is used to encrypt the PEM file for import.<br>**Note**<br>The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |

## Command Default

No default behavior or values

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 15.2(2)SA2 | This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The **crypto key export rsa pem** command allows RSA key pairs to be exported in PEM-formatted files. The PEM files can then be imported back into a Cisco IOS router or other public key infrastructure (PKI) applications.

**Note** Before an RSA key pair is exported in a PEM file, ensure that the RSA key pair is exportable. To generate an exportable RSA key pair, issue the **crypto key generate rsa** command and specify the **exportable** keyword.

## Examples

The following example shows how to generate, export, bring the key back (import), and verify the status of the RSA key pair "mycs":

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable

The name for the keys will be: mycs
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD
% Key name: mycs
Usage: General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD
% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa
% Key pair was generated at: 18:04:56 GMT Jun 6 2003
Key name: mycs
Usage: General Purpose Key
Key is exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at: 18:17:25 GMT Jun 6 2003
```

```
Key name: mycs2
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key generate rsa** | Generates RSA key pairs. |
| crypto key import rsa pem | Imports RSA keys in PEM-formatted files. |

# crypto key generate ec keysize

To generate an Elliptic Curve (EC) key pair, use the **crypto key generate ec keysize** command in global configuration mode.

**crypto key generate ec keysize** {**256** | **384**} [**exportable**] [**label** *key-label*]

## Syntax Description

| | |
|---|---|
| **256** | Specifies a 256-bit key size. |
| **384** | Specifies a 384-bit key size. |
| **exportable** | (Optional) Specifies that the key pair can be exported to another Cisco device, such as a router. |
| **label** *key-label* | (Optional) Specifies the name to be used for the EC key pair when it is being exported.<br>If a key label is not specified, the fully qualified domain name (FQDN) of the router is used. |

## Command Default

The EC key pairs do not exist.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)T | This command was introduced. |
| 15.2(4)M | This command was modified. The **exportable** keyword was added. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

Use this command to generate EC key pairs for your Cisco device (such as a router). IPsec and public key infrastructure (PKI) both support the ability to generate, export, and import EC (ECDSA-256 and ECDSA-384) key pairs.

## Examples

The following example generates a 256-bit EC key pair with a label named Device_1_Key.

```
Device(config)# crypto key generate ec keysize 256 label Device_1_Key
```

The following example generates an exportable 384-bit EC key pair with a label named Device_2_Key.

```
Device(config)# crypto key generate ec keysize 384 exportable label Device_2_Key
```

## Related Commands

| Command | Description |
|---|---|
| **copy** | Copies any file from a source to a destination. |

| Command | Description |
|---|---|
| **crypto key export ec** | Exports EC key pairs. |
| **crypto key export rsa pem** | Exports RSA key pairs in PEM-formatted files. |
| **crypto key generate rsa** | Generates RSA keys. |
| **crypto key import ec** | Imports EC key pairs. |
| **crypto key import rsa pem** | Exports RSA key pairs in PEM-formatted files. |
| **crypto key storage** | Sets the default storage location for RSA key pairs. |
| **crypto key zeroize ec** | Deletes EC keys from a device. |
| **debug crypto engine** | Displays debug messages about crypto engines. |
| **hostname** | Specifies or modifies the hostname for the network server. |
| **ip domain-name** | Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name). |
| **show crypto key mypubkey ec** | Displays the EC public keys of the device. |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of the device. |
| **show crypto pki certificates** | Displays information about your PKI certificate, certification authority, and any registration authority certificates. |

# crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** commandinglobal configuration mode.

**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename* **:**] [**redundancy**] [**on** *devicename* **:**]

## Syntax Description

| | |
|---|---|
| **general-keys** | (Optional) Specifies that a general-purpose key pair will be generated, which is the default. |
| **usage-keys** | (Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated. |
| **signature** | (Optional) Specifies that the RSA public key generated will be a signature special usage key. |
| **encryption** | (Optional) Specifies that the RSA public key generated will be an encryption special usage key. |
| **label** *key-label* | (Optional) Specifies the name that is used for an RSA key pair when they are being exported.<br>If a key label is not specified, the fully qualified domain name (FQDN) of the router is used. |
| **exportable** | (Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router. |
| **modulus** *modulus-size* | (Optional) Specifies the IP size of the key modulus.<br>By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits.<br>**Note**<br>Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits. |
| **storage** *devicename* **:** | (Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:). |
| **redundancy** | (Optional) Specifies that the key should be synchronized to the standby CA. |
| **on** *devicename* **:** | (Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:).<br>Keys created on a USB token must be 2048 bits or less. |

## Command Default

RSA key pairs do not exist.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(8)T | The *key-label* argumentwas added. |
| 12.2(15)T | The **exportable** keyword was added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(4)T | The **storage** keyword and *devicename* **:** argument were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | The **storage** keyword and *devicename* **:** argument were implemented on the Cisco 7200VXR NPE-G2 platform.<br>The **signature**, **encryption** and **on** keywords and *devicename* **:** argument were added. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) was added. |
| XE 2.4 | The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations. |
| 15.0(1)M | This command was modified. The **redundancy** keyword was introduced. |
| 15.1(1)T | This command was modified. The range value for the **modulus** keyword value is extended from 360 to 2048 bits to 360 to 4096 bits. |
| 15.2(2)SA2 | This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs--one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

**Note** Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)

**Note** Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router_FQDN* }.server. For example, if a router name is "router1.cisco.com," the key name is "router1.cisco.com.server."

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

**Note** If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

**Special-Usage Keys**

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

**General-Purpose Keys**

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

**Named Key Pairs**

If you generate a named key pair using the *key-label*argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

**Modulus Length**

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modules takes longer to generate (see the table below for sample times) and takes longer to use.

*Table 27: Sample Times by Modulus Length to Generate RSA Keys*

| Router | 360 bits | 512 bits | 1024 bits | 2048 bits (maximum) |
|---|---|---|---|---|
| Cisco 2500 | 11 seconds | 20 seconds | 4 minutes, 38 seconds | More than 1 hour |
| Cisco 4700 | Less than 1 second | 1 second | 4 seconds | 50 seconds |

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.



**Note** As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage** *devicename* **:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

**Specifying a Device for RSA Key Generation**

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on** *devicename* **:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy**or similar command is issued.)

For information on configuring a USB token, see " Storing PKI Credentials " chapter in the Cisco IOS Security Configuration Guide, Release 12.4T. For information on using on-token RSA credentials, see the " Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment " chapter in the Cisco IOS Security Configuration Guide , Release 12.4T.

**Specifying RSA Key Redundancy Generation on a Device**

You can specify redundancy for existing keys only if they are exportable.

## Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:



**Note** You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
The name for the keys will be: MYKEYS
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]
```

## Related Commands

| Command | Description |
|---|---|
| copy | Copies any file from a source to a destination, use the copy command in privileged EXEC mode. |
| **crypto key storage** | Sets the default storage location for RSA key pairs. |
| **debug crypto engine** | Displays debug messages about crypto engines. |
| **hostname** | Specifies or modifies the hostname for the network server. |
| **ip domain-name** | Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name). |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of your router. |
| show crypto pki certificates | Displays information about your PKI certificate, certification authority, and any registration authority certificates. |

# crypto key import ec

To import an Elliptic Curve (EC) key pair, use the **crypto key import ec** command in global configuration mode.

**crypto key import ec** *key-label* [**exportable**] {**terminal** | **url** *url*} *passphrase*

## Syntax Description

| | |
|---|---|
| *key-label* | Name of the EC key pair to be imported to the device.<br>The *key-label* argument must match the key pair name that was specified through the **crypto key generate ec keysize** command. |
| **exportable** | (Optional) Specifies that the imported EC key pair can be exported to another Cisco device such as a router. |
| **terminal** | Specifies that the certificates and EC key pairs will be manually imported via copy-and-paste to the console terminal. |
| **url** *url* | Specifies the URL of the file system from which the router should import certificates and EC key pairs. |
| *passphrase* | Specifies the passphrase that was used to encrypt the PEM file for import.<br>**Note**<br>The passphrase can be any phrase that is at least eight characters in length. It can include spaces and punctuation, excluding the question mark (?), which has special meaning to the parser. |

## Command Default

EC key pairs are not imported.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

IPsec and public key infrastructure (PKI) both support the ability to generate, export, and import EC (ECDSA-256 and ECDSA-384) key pairs. The **crypto key import ec** command lets you import EC key pairs into PEM-formatted files. The files can be previously exported from another Cisco IOS router or generated by other PKI applications.

You can specify a device from which to import EC key pairs. Devices supported include NVRAM and local disks.

If the device on which the EC key pair is to be imported does not have enough space for this key, then a message appears stating that the importation of the key pair has failed.

To delete EC key pairs from a device, use the **crypto key zeroize ec** command.

## Examples

The following example shows how to generate, export, import, and verify the status of an EC key pair named Device_1_Key:

```
! Generate the key pair
!
Device(config)# crypto key generate ec keysize 256 exportable label Device_1_Key
The name for the keys will be: Device_1_Key

 EC key pair created successfully
!
! Archive the key pair to a remote location, and use a good password.
!
Device(config)# crypto key export ec Device_1_Key pem url nvram: 3des mypassword
% Key name: Device_1_Key
   Usage: Signature Key
Exporting public key...
Destination filename [Device_1_Key-sign.pub]?
Writing file to nvram:Device_1_Key-sign.pub
Exporting private key...
Destination filename [Device_1_Key-sign.prv]?
Writing file to nvram:Device_1_Key-sign.prv
!
! Import the key as a different name.
!
Device(config)# crypto key import ec Device_1_Key url nvram:Device_1_Key mypassword
% Importing public Signature key or certificate PEM file...
Source filename [Device_1_Key-sign.pub]?
Reading file from nvram:Device_1_Key-sign.pub
% Importing private Signature key PEM file...
Source filename [Device_1_Key-sign.prv]?
Reading file from nvram:Device_1_Key-sign.prv
% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Device# show crypto key mypubkey ec
% Key pair was generated at: 17:26:53 PST Jun 7 2012
Key name: Device_1_Key
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data:
  30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 420004A3 E483C98C
  BABE4CAD 9822F5F1 06FDFD4B F70D0103 03C266B6 DA368DB9 AB01C5AB 7333F5B9
  3478E0FE 6CA67598 FB828F47 A92AFE70 93EFE828 2620A611 699E52
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key export ec** | Exports EC keys in PEM-formatted files. |
| **crypto key generate ec keysize** | Generates EC key pairs. |
| **crypto key zeroize ec** | Deletes EC keys from a device. |

# crypto key import rsa pem

To import Rivest, Shamir, and Adelman (RSA) keys in privacy-enhanced mail (PEM)-formatted files, use the **crypto key import rsa pem**command in global configuration mode.

**crypto key import rsa** *key-label* **pem** [**usage-keys** | **signature** | **encryption** | **general-purpose**] {**storage** | **terminal** [*passphrase*] | **url** *url*} [**exportable**] [**on** *devicename* **:**]

## Syntax Description

| | |
|---|---|
| *key-label* | Name of the RSA key pair that is imported to the device.<br>The *key-label* argument must match the key pair name that was specified through the **crypto key generate rsa** command. |
| **usage-keys** | (Optional) Specifies that two RSA special usage key pairs, one encryption pair and one signature pair, are imported. |
| **signature** | (Optional) Specifies that RSA signature keys are imported. |
| **encryption** | (Optional) Specifies that RSA encryption keys are imported. |
| **general-purpose** | (Optional) Specifies a General Purpose Key. |
| **storage** | Stores the key on the specified device. |
| **terminal** | Specifies the certificates and RSA key pairs are manually imported to the console terminal. |
| *passphrase* | Passphrase that is used to encrypt the PEM file for import.<br>**Note**<br>The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |
| **url** *url* | URL of the file system where the router should import certificates and RSA key pairs. |
| **exportable** | (Optional) Specifies that the imported RSA key pair can be exported to another Cisco device such as a router. |
| **on** *devicename* **:** | (Optional) Specifies that the imported RSA key pair is created on the specified device. Devices supported include local disks, NVRAM, and USB tokens. The name of the device is followed by a colon (:).<br>Keys created on a USB token have a maximum size of 1024-bits. |

## Command Default

RSA general-purpose key pair type is expected for import.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.4(11)T | This command was modified. The **signature**, **encryption**, and **on** keywords and *devicename* **:** argument were added. |
| 15.0(1)M | This command was modified. The **terminal** keyword and *passphrase* argument were added. |
| 15.2(2)SA2 | This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The **crypto key import rsa pem** command allows RSA key pairs to be imported into PEM-formatted files. The files can be previously exported from another Cisco IOS router or generated by other public key infrastructure (PKI) applications.

As of Cisco IOS Release 12.4(11)T and later releases, the device can be specified for where RSA keys are generated. Devices supported include NVRAM, local disks and USB tokens. If the router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be imported to a configured and available USB token by using the **on** *devicename* **:** keyword and argument. Keys that reside on a USB token, or on-token keys, are saved to persistent token storage when they are imported. Key deletion removes the on-token keys from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **write memory** or similar command is issued.)

If the device, on which the RSA key is to be imported, does not have enough space for this key, then a message appears saying that the importation of the key has failed.

For information on configuring a USB token, see " Storing PKI Credentials " module. For information on using on-token RSA credentials, see " Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment" module.

## Examples

The following example shows that an encryption key has been imported successfully to a configured and available USB token, shown with crypto engine and crypto PKI transaction debugging messages:

```
Router#
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
crypto key import rsa label encryption on usbtoken0 url nvram:e password

% Importing public Encryption key or certificate PEM file...
filename [e-encr.pub]?
Reading file from nvram:e-encr.pub
% Importing private Encryption key PEM file...
Source filename [e-encr.prv]?
Reading file from nvram:e-encr.prv
% Key pair import succeeded.
```

The following example shows how to generate, export, import, and verify the status of the RSA key pair "mycs":

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable

The name for the keys will be: mycs
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD
% Key name: mycs
Usage: General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD
% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa
% Key pair was generated at: 18:04:56 GMT Jun 6 2003
Key name: mycs
Usage: General Purpose Key
Key is exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at: 18:17:25 GMT Jun 6 2003
```

```
Key name: mycs2
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key export pem** | Exports RSA keys in PEM-formatted files. |
| **crypto key generate rsa** | Generates RSA key pairs. |

# crypto key lock rsa

To lock the RSA private key in a router, use the **crypto key lock rsa**command in privileged EXEC mode.

**crypto key lock rsa** [**name** *key-name*] [**all**] [**passphrase** [*passphrase*]]

## Syntax Description

| | |
|---|---|
| **name** *key-name* | (Optional) Specifies the name of the RSA key pair that is to be locked. The name must match the name that was specified via the **crypto key encrypt rsa** command. |
| **all** | (Optional ) Locks all the encrypted keys. |
| **passphrase** *passphrase* | (Optional ) Specifies the passphrase that is used to lock the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command. |

## Command Default

RSA keys are encrypted, but not locked.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **all** keyword was added. |
| Cisco IOS XE Release 2.1 | This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Usage Guidelines

When the **crypto key lock rsa** command is issued, the unencrypted copy of the key is deleted. Because the private key is not available, all RSA operations will fail.

This command affects only the “run-time” access to the key; that is, it does not affect the key that is stored in NVRAM.

## Examples

The following example shows how to lock the key “pki1-72a.cisco.com.” Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
!
Router# show crypto key mypubkey rsa
% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
```

```
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key encrypt rsa** | Encrypts the RSA private key. |
| **crypto key unlock rsa** | Unlocks the RSA private key in a router. |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of your router. |

# crypto key move rsa

To move an existing Cisco IOS generated Rivest, Shamir, and Adelman (RSA) key pair from one storage location to another storage location, use the **crypto key move rsa** command in global configuration mode.

**crypto key move rsa** *keylabel* [**non-exportable**] [**on** | **storage**] [**redundancy** *routername*] *location*

## Syntax Description

| | |
|---|---|
| *keylabel* | Specifies name of the existing RSA key pair. |
| **non-exportable** | (Optional) Specifies that the RSA key pair cannot be exported once the key pair is moved to the eToken device. |
| **on** | (Optional) Specifies that the RSA key pair will be placed on a configured USB token and stored in the PIN protected flash portion of the USB token. Any subsequent RSA operations will be performed on the USB token. |
| **storage** | (Optional) Specifies that the RSA key pair will be stored on the specified device, for example a smart card. The key pair will be loaded back into Cisco IOS for any subsequent RSA operations. |
| *location* | Identifies the storage location where the RSA key pair will be moved. |
| **redundancy** | (Optional) Specifies that the key should be synchronized to the standby CA. |

## Command Default

The RSA key pair remains stored on the current device.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |
| 15.0(1)M | This command was modified. The **redundancy** keyword was introduced. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

When an existing RSA key pair is generated in Cisco IOS, stored on a USB token, and used for an enrollment, it may be necessary to move those existing RSA key pairs to an alternate location for permanent storage.

Generating the key on the router and moving it to the token requires less than a minute. Generating a key on the token using the **on** keyword could require 5 to 10 minutes and is dependent on hardware key generation routines available on the USB token.

Using the **crypto key move rsa**command allows the storage location of a newly generated key to be changed if the **storage** keyword or **on** keyword was not specified when the key was first generated and the key has not yet been written out to a storage location. You can always move an exportable key.

**Note** If you make the key nonexportable by issuing the **non-exportable**keyword, the key cannot be made exportable again. Also, once you specify the **on** keyword with the target device, either to move an existing key or during key generation, the command cannot be undone.

## Examples

The following example moves an existing RSA key pair to a configured and available USB token, "tokenA," as a nonexportable key pair stored in the PIN protected flash portion of the designated USB token:

```
crypto key move rsa keypairname non-exportable on tokenA
```

## Related Commands

| Command | Description |
|---|---|
| **binary file** | Specifies the binary file location on the registrar and the destination binary file location on the petitioner. |
| **template file** | Specifies the source template file location on the registrar and the destination template file location on the petitioner. |

# crypto key pubkey-chain rsa

To enter public key configuration mode (so you can manually specify other devices' RSA public keys), use the **crypto key pubkey-chain rsa**command in global configuration mode.

**crypto key pubkey-chain rsa**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify other IPSec peers' RSA public keys. You need to specify other peers' keys when you configure RSA encrypted nonces as the authentication method in an Internet Key Exchange policy at your peer router.

## Examples

The following example specifies the RSA public keys of two other IPSec peers. The remote peers use their IP address as their identity.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# addressed-key 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **address** | Specifies the IP address of the remote RSA public key of the remote peer you will manually configure. |
| **addressed-key** | Specifies the RSA public key of the peer you will manually configure. |
| **key-string (IKE)** | Specifies the RSA public key of a remote peer. |
| **named-key** | Specifies which peer RSA public key you will manually configure. |
| **show crypto key pubkey-chain rsa** | Displays peer RSA public keys stored on your router. |

# crypto key storage

To set the default storage location for newly created Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key storage**command in global configuration mode. To store keys on the most recently logged-in USB token (or on NVRAM if there is no token), use the **no** form of this command.

**crypto key storage** *device:*
**nocrypto key storage** *device:*

## Syntax Description

| | |
|---|---|
| *device:* | Name of the device where the RSA key pairs will be stored by default. |

## Command Default

RSA key pairs are stored on NVRAM.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

You may specify a default storage location, other than NVRAM, for newly created USB token RSA keys. The storage location specified by the **crypto key generate rsa** command for RSA keys will override the location specified by the **crypto key storage** command. The name of the designated device is followed by a colon (:).

Regardless of configuration settings, existing keys will be stored on the devices from where they were originally loaded.



**Note** The USB token must be logged into the router for the RSA keys to be read or written.

## Examples

The following example shows how to store new keys in NVRAM by default, regardless of where the token is inserted:

crypto key storage nvram:

The following example shows how to store new keys on usbtoken0: by default:

crypto key storage usbtoken0:

The following example shows how to store new keys on most recently logged-in token, or on NVRAM if there is no token:

no crypto key storage

## Related Commands

| Command | Description |
|---|---|
| crypto key generate rsa | Generates RSA key pairs and specifies RSA key storage location (other than the default location). |
| **crypto pki token user-pin** | Creates a PIN that automatically allows the router to log into the USB token at router startup. |

# crypto key unlock rsa

To unlock the RSA private key in a router, use the **crypto key unlock rsa**command in privileged EXEC mode.

**crypto key unlock rsa** [**name** *key-name*] [**all**] [**passphrase** [*passphrase*]]

## Syntax Description

| | |
|---|---|
| **name** *key-name* | (Optional) Specifies the name of the RSA key pair that is to be unlocked. The name must match the name that was specified via the **crypto key encrypt rsa** command. |
| **all** | (Optional ) Unlocks all the locked key pairs. |
| **passphrase** *passphrase* | (Optional) Specifies the passphrase that is used to unlock the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command. |

## Command Default

The encrypted private key is locked.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **all** keyword was added. |
| Cisco IOS XE Release 2.1 | This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Usage Guidelines

When a router with an encrypted RSA key (via the **crypto key encrypt rsa** command) initially boots up, the key does not exist in plain text and is therefore considered to be locked. Because the private key is not available, all RSA operations will fail. After you unlock the private key, RSA operations will function again.

This command affects only the “run-time” access to the key; that is, it does not affect the key that is stored in NVRAM.

## Examples

The following example shows how to unlock the key “pki1-72a.cisco.com”:

```
Router# crypto key unlock rsa name pki1-72a.cisco.com passphrase cisco1234
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key encrypt rsa** | Encrypts the RSA private key. |

| Command | Description |
|---|---|
| **crypto key lock rsa** | Locks the RSA private key in a router. |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of your router. |

# crypto key zeroize ec

To delete all Elliptic Curve (EC) key pairs from your router, use the **crypto key zeroize ec** command in global configuration mode.

**crypto key zeroize ec** [*key-pair-label*]

## Syntax Description

| | |
|---|---|
| *key-pair-label* | (Optional) Specifies the name of the key pair that the router will delete. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(8)T | The *key-pair-label*argument was added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

This command deletes all EC key pairs that were previously generated by your router unless you include the *key-pair-label* argument, which will delete only the specified EC key pair. If you issue this command, you must also perform two additional tasks for each trustpoint that is associated with the key pair that was deleted:

- Ask the certification authority (CA) administrator to revoke your router's certificates at the CA; you must supply the challenge password you created when you originally obtained the router's certificates using the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration by removing the configured trustpoint (using the **no crypto ca trustpoint** *name*command .)



**Note** This command cannot be undone (after you save your configuration), and after EC keys have been deleted, you cannot use certificates or the CA or participate in certificate exchanges with other IP security (IPsec) peers unless you reconfigure CA interoperability by regenerating EC keys, getting the CA's certificate, and requesting your own certificate again.

This command is not saved to the configuration.

## Examples

The following example deletes the general-purpose EC key pair that was previously generated for the router. After deleting the EC key pair, the administrator contacts the CA administrator and requests that the certificate of the router be revoked. The administrator then deletes the certificate of the router from the configuration.

```
crypto key zeroize ec
crypto ca certificate chain
 no certificate
```

## Related Commands

| Command | Description |
|---|---|
| **certificate** | Adds certificates manually. |
| **crypto ca certificate chain** | Enters the certificate chain configuration mode. |
| **crypto ca trustpoint** | Declares the CA that your router should use. |
| **crypto key zeroize pubkey-chain** | Deletes the remote peer's public key from the cache. |
| **crypto key zeroize rsa** | Deletes all RSA key pairs from the router. |
| **show crypto ca timers** | Specifies which key pair to associate with the certificate. |

# crypto key zeroize pubkey-chain

To delete the remote peer's public key from the cache, use the **crypto key zeroize pubkey-chain** command in global configuration mode.

**crypto key zeroize pubkey-chain** [*index*]

## Syntax Description

| | |
|---|---|
| *index* | (Optional) Specifies an index entry to be deleted. If no index entry is specified, then all the index entries are deleted. The acceptable range of index entries is from 1 to 65535. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

This command is used is used to delete the peer router's public keys in order to help debug signature verification problems in IKEv1 and IKEv2. Keys are cached by default with the lifetime of the certificate revocation list (CRL) associated with the trustpoint.

## Examples

The following example deletes all public key index entries:

```
Router> enable
Router# configure terminal
Router (config)# crypto key zeroize pubkey-chain
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key zeroize ec** | Deletes all EC key pairs from the router. |
| **crypto key zeroize rsa** | Deletes all RSA key pairs from the router. |

# crypto key zeroize rsa

To delete all RSA keys from your router, use the **crypto key zeroize rsa** command in global configuration mode.

**crypto key zeroize rsa** [*key-pair-label*]

## Syntax Description

| | |
|---|---|
| *key-pair-label* | (Optional) Specifies the name of the key pair that router will delete. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(8)T | The *key-pair-label*argument was added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

This command deletes all Rivest, Shamir, and Adelman (RSA) keys that were previously generated by your router unless you include the *key-pair-label* argument, which will delete only the specified RSA key pair. If you issue this command, you must also perform two additional tasks for each trustpoint that is associated with the key pair that was deleted:

- Ask the certification authority (CA) administrator to revoke your router's certificates at the CA; you must supply the challenge password you created when you originally obtained the router's certificates using the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration by removing the configured trustpoint (using the **no crypto ca trustpoint** *name*command .)



**Note** This command cannot be undone (after you save your configuration), and after RSA keys have been deleted, you cannot use certificates or the CA or participate in certificate exchanges with other IP Security (IPSec) peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again.

This command is not saved to the configuration.

## Examples

The following example deletes the general-purpose RSA key pair that was previously generated for the router. After deleting the RSA key pair, the administrator contacts the CA administrator and requests that the certificate of the router be revoked. The administrator then deletes the certificate of the router from the configuration.

```
crypto key zeroize rsa
crypto ca certificate chain
 no certificate
```

## Related Commands

| Command | Description |
|---|---|
| **certificate** | Adds certificates manually. |
| **crypto ca certificate chain** | Enters the certificate chain configuration mode. |
| **crypto ca trustpoint** | Declares the CA that your router should use. |
| **crypto key zeroize ec** | Deletes all EC key pairs from the router. |
| **crypto key zeroize pubkey-chain** | Deletes the remote peer's public key from the cache. |
| **show crypto ca timers** | Specifies which key pair to associate with the certificate. |

# crypto keyring

To define a crypto keyring to be used during Internet Key Exchange (IKE) authentication, use the **crypto keyring**command in global configuration mode. To remove the keyring, use the **no** form of this command.

**crypto keyring** *keyring-name* [**vrf** *fvrf-name*]
**no crypto keyring** *keyring-name* [**vrf** *fvrf-name*]

## Syntax Description

| | |
|---|---|
| *keyring-name* | Name of the crypto keyring. |
| **vrf** *fvrf-name* | (Optional) Front door virtual routing and forwarding (FVRF) name to which the keyring will be referenced. The *fvrf-name*must match the FVRF name that was defined during virtual routing and forwarding (VRF) configuration. The **vrf** keyword and *fvrf-name* argument are not supported by IPv6. |

## Command Default

All the Internet Security Association and Key Management Protocol (ISAKMP) keys that were defined in the global configuration are part of the default global keyring.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.4(4)T | Support for IPv6 was added. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

## Usage Guidelines

A keyring is a repository of preshared and Rivest, Shamir, and Adelman (RSA) public keys. The keyring is used in the ISAKMP profile configuration mode. The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile.

## Examples

The following example shows that a keyring and its usage have been defined:

```
crypto keyring vpnkeys
  pre-shared-key address 10.72.23.11 key vpnsecret
crypto isakmp profile vpnprofile
  keyring vpnkeys
```

## Related Commands

| Command | Description |
|---|---|
| **pre-shared-key** | Defines a preshared key to be used for IKE authentication. |

# crypto logging ezvpn

To enable Easy VPN syslog messages on a server, use the **crypto logging ezvpn** command in global configuration mode. To disable syslog messages on the server, use the **no** form of this command.

**crypto logging ezvpn** [**group** *group-name*]
**no crypto logging ezvpn** [**group** *group-name*]

## Syntax Description

| | |
|---|---|
| **group** *group-name* | (Optional) Group name. If a group name is not provided, syslog messages are enabled for all Easy VPN connections to the server. If a group name is provided, syslog messages are enabled only for that particular group. |

## Command Default

Syslog messages are not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware. |

## Examples

The following configuration shows that syslog messages are to be displayed for group_1.

```
crypto logging ezvpn group group_1
```

The following is an example of a typical Easy VPN syslog message:

```
timestamp: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server)  <event message>  User=<username>
Group=<groupname>  Client_public_addr=<ip_addr> Server_public_addr=<ip addr>
```

The following is an example of an authentication-passed event Easy VPN syslog message:

```
Jul 25 23:33:06.847: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server)  Authentication PASS
ED  User=blue Group=Cisco1760group  Client_public_addr=10.20.20.1
Server_public_addr=10.20.20.2
```

The following is an example of a “Group does not exist” Easy VPN syslog message:

```
*Jun 30 18:02:58.107: %CRYPTO-6-VPN_TUNNEL_STATUS: Group: group_1 does not exist
```

# crypto logging ikev2

To enable Internet Key Exchange Version 2 (IKEv2) syslog messages, use the **crypto logging ikev2** command in global configuration mode. To disable syslog messages, use the **no** form of this command.

**crypto logging ikev2**
**no crypto logging ikev2**

## Syntax Description

This command has no keywords or arguments.

## Command Default

IKEv2 syslog messages are not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)T | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Examples

The following configuration shows how to enable IKEv2 syslog messages:

```
Router(config)# crypto logging ikev2
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 certificate-cache** | Specifies the cache size to store certificates fetched from HTTP URLs. |
| **crypto ikev2 cookie-challenge** | Enables IKEv2 cookie challenge. |
| **crypto ikev2 diagnose error** | Enables IKEv2 error diagnosis. |
| **crypto ikev2 dpd** | Defines DPD globally for all peers. |
| **crypto ikev2 http-url cert** | Enables HTTP CERT support. |
| **crypto ikev2 limit** | Defines call admission control for all peers. |
| **crypto ikev2 nat** | Defines NAT keepalive globally for all peers. |
| **crypto ikev2 window** | Specifies the IKEv2 window size. |

# crypto logging session

To generate crypto logging messages, use the **crypto logging session**command in global configuration mode. To disable logging messages, use the **no** form of this command.

**crypto logging session**
**no crypto logging session**

## Syntax Description

| | |
|---|---|
| **session** | Generates the log of active or up sessions, and inactive or down sessions. |

## Command Default

Crypto logging messages are not generated.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

Crypto logging messages allow users to receive notification for every crypto EZVPN group or session that is made on their device.

## Examples

The following example shows how to enable crypto logging syslog messages for all the sessions:

```
Router(config)# crypto logging session
```

## Related Commands

| Command | Description |
|---|---|
| **crypto logging ezvpn** | Enables Easy VPN syslog messages on a server. |
| **show logging** | Displays the state of system logging and the contents of the standard system logging buffer. |

# crypto map (global IPsec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-manual**]
**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp** [**dynamic** *dynamic-map-name* | **discover** | **profile** *profile-name*]]
**no crypto map** [**ipv6**] *map-name* [*seq-num*]
**crypto map** [**ipv6**] *map-name* **client accounting list** *aaalist*
**no crypto map** [**ipv6**] *map-name* [**client accounting list**]
**crypto map** *map-name seq num* [**gdoi**]
**no crypto map** *map-name* [*seq-num*]

## Syntax Description

| | |
|---|---|
| **ipv6** | (Optional) Specifies an IPv6 crypto map. For IPv4 crypto maps, use the command without this keyword.<br>**Note**<br>IPv6 addresses are not supported on dynamic crypto maps. |
| *map-name* | Identifies the crypto map set. |
| *seq-num* | Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section. |
| **ipsec-manual** | (Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPsec) security associations (SAs) for protecting the traffic specified by this crypto map entry.<br>**Note**<br>The **ipsec-manual** keyword is not supported by the virtual private network Shared Port Adapter (VPN SPA) beginning with Cisco IOS Release 12.2(33)SXH5 or 12.2(33)SXI1. If the **ipsec-manual** keyword is entered for images after those releases, the following error message appears beneath the keyword entry line: "Manually-keyed crypto map configuration is not supported by the current crypto engine." |
| **ipsec-isakmp** | (Optional) Indicates that IKE will be used to establish the IPsec for protecting the traffic specified by this crypto map entry. |
| **dynamic** | (Optional) Specifies that this crypto map entry must reference a preexisting dynamic crypto map.<br>**Note**<br>Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPsec device. If you use this keyword, none of the crypto map configuration commands will be available. |

| | |
|---|---|
| *dynamic-map-name* | (Optional) Name of the dynamic crypto map set that should be used as the policy template. |
| **discover** | (Optional) Enables peer discovery. By default, peer discovery is disabled. |
| **profile** | (Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand. |
| *profile-name* | (Optional) Name of the crypto profile being created. |
| **client accounting list** | Designates a client accounting list. |
| *aaalist* | (Optional) AAA list name. |
| **gdoi** | (Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI). |

## Command Default

No crypto maps exist. Peer discovery is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 11.3T | The following keywords and arguments were added:<br>• **ipsec-manual**<br>• **ipsec-isakmp**<br>• **dynamic**<br>• *dynamic-map-name* |
| 12.0(5)T | The **discover** keyword was added to support Tunnel Endpoint Discovery (TED). |
| 12.2(4)T | The **profile***profile-name* keyword-argument pair was added to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand. |
| 12.2(11)T | This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms. |
| 12.2(15)T | The **client accounting list** *aaalist* keyword-argument pair was added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB without support for the **gdoi** keyword. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH5, 12.2(33)SXI1 | The **ipsec-manual** keyword is not supported by the VPN SPA beginning with Cisco IOS Release 12.2(33)SXH5 or 12.2(33)SXI1. |
| 12.4(6)T | The **gdoi** keyword was added. |
| Cisco IOS XE 2.1 | This command was implemented on Cisco ASR 1000 series routers. |
| 15.1(4) M | This command was modified. The **ipv6** keyword was added. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to create a new crypto map entry or profile. Use the **crypto map ipv6** *map-name seq-num*command without any keyword to modify an existing IPv6 crypto map entry or profile. For IPv4 crypto maps, use the **crypto map** *map-name seq-num*command without any keyword to modify the existing crypto map entry or profile.

After a crypto map entry is created, you cannot change the parameters specified at the global configuration level because these parameters determine the configuration commands that are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map**(interface IPsec) command.

### Crypto Map Functions

Crypto maps provide two functions: filtering and classifying the traffic to be protected and defining the policy to be applied to that traffic. The first affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPsec crypto maps define the following:

- What traffic should be protected
- To which IPsec peers the protected traffic can be forwarded--these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and SAs should be used or managed (or what the keys are, if IKE is not used)

**Note** Crypto maps are not supported on tunnel interface and port-channel interface for Cisco ASR 1000 Series Aggregation Services Routers, Cisco Cloud Services Router 1000V Series, and Cisco 4000 Series Integrated Services Routers.

### Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name*argument. Therefore, for an interface, you could have certain traffic forwarded to one IPsec peer with specified security applied to that traffic and other traffic forwarded to the same or different IPsec peer with different IPsec security applied. To accomplish differential forwarding, you would create two crypto maps, each with the same *map-name* argument but different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.



**Note** If a deny statement (which specifies the conditions under which a packet cannot pass the access control list) in an access control list belongs to a crypto map in a crypto map set, the IPsec logic causes a jump to the next crypto map in the crypto map set, hoping for a better possible match. VPN Service Adapter (VSA) hardware has a restriction of 14 jumps.

### Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, assume that a crypto map set contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named “mymap” is applied to serial interface 0. When traffic passes through serial interface 0, traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (which includes establishing IPsec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPsec security.)

### Dynamic Crypto Maps

Refer to the “Usage Guidelines” section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. If the request does not match any of the static maps, it will be evaluated against the dynamic map set.

If a crypto map entry references a dynamic crypto map set, make it the lowest priority map entry by giving it the highest *seq-num* value of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map**(global IPsec)command using the **dynamic** keyword.



**Note** IPv6 keywords are not supported on dynamic crypto maps.

### TED

Tunnel Endpoint Discovery (TED) is an enhancement to the IPsec feature. Defining a dynamic crypto map allows you to dynamically determine an IPsec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPsec peer for secure IPsec communications.

Dynamic TED helps to simplify the IPsec configuration on individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPsec transforms that are required.

**Note** TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPsec. Thus, TED does not improve the scalability of IPsec (in terms of performance or the number of peers or tunnels).

### Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the L2TP Security feature. The relevant SAs in the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

**Note** The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

## Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
The following example shows the minimum required IPv6 crypto map configuration when IKE
will be used to establish the SAs:
crypto map ipv6 CM_V6 10 ipsec-isakmp
 match address ACL_IPV6_1
  set peer 2001:DB8:0:ABCD::1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
The following example shows the minimum required IPv6 crypto map configuration when the SAs
 are manually established:
crypto map ipv6 CM_V6 ipsec-manual
 match address ACL_V6_2
```

```
 set transform-set someset
 set peer 2001:DB8:0:ABCD::1
 set session-key inbound ah 256 9876543210987654987654321098765 4
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example shows how to configure an IPsec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either or both the remote IPsec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of the two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPsec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPsec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPsec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example shows how to configure TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example shows how to configure a crypto profile to be used as a template for dynamically created crypto maps when IPsec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

The following example shows how to configure a crypto map for a GDOI group member:

```
crypto map diffint 10 gdoi
```

```
set group diffint
```

## Related Commands

| Command | Description |
|---|---|
| **crypto dynamic-map** | Creates a dynamic crypto map entry and enters crypto map configuration command mode. |
| **crypto isakmp profile** | Audits IPsec user sessions. |
| **crypto map (interface IPSec)** | Applies a previously defined crypto map set to an interface. |
| **crypto map local-address** | Specifies and names an identifying interface to be used by the crypto map for IPsec traffic. |
| **match address (IPSec)** | Specifies an extended access list for a crypto map entry. |
| **set peer (IPsec)** | Specifies an IPsec peer in a crypto map entry. |
| **set pfs** | Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs. |
| **set session-key** | Specifies the IPsec session keys within a crypto map entry. |
| **set transform-set** | Specifies which transform sets can be used with the crypto map entry. |
| **show crypto map (IPsec)** | Displays the crypto map configuration. |

# crypto map (interface IPsec)

To apply a previously defined crypto map set to an interface, use the **crypto map** command in interface configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

**crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]]
**no crypto map** [*map-nam e*] [**redundancy** *standby-group-name* [**stateful**]]

## Syntax Description

| | |
|---|---|
| *map-name* | Name that identifies the crypto map set. This is the name assigned when the crypto map was created.<br>When the **no** form of the command is used, this argument is optional. Any value supplied for the argument is ignored. |
| **redundancy** | (Optional) Defines a backup IP security (IPsec) peer. Both routers in the standby group are defined by the redundancy *standby-group-name*argument and share the same virtual IP address. |
| *standby-group-name* | (Optional) Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. |
| **stateful** | (Optional) Enables IPsec stateful failover for the crypto map. |

## Command Default

No crypto maps are assigned to interfaces.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.1(9)E | This command was modified. The redundancy keyword and *standby-group-name* argument were added. |
| 12.2(8)T | This command was modified. The redundancy keyword and *standby-group-name* argument were added. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms. |
| 12.2(9)YE | This command was modified. The redundancy keyword and *standby-group-name* argument were added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.3(11)T | This command was modified. The stateful keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to assign a crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPsec services. Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different sequence number , they are considered to be part of the same set and will all be applied to the interface. The crypto map entry that has the lowest sequence number is considered the highest priority and will be evaluated first. A single crypto map set can contain a combination of **ipsec-isakmp**and **ipsec-manual crypto map** entries.

**Note** A crypto map applied to a loopback interface is not supported.

The standby name must be configured on all devices in the standby group, and the standby address must be configured on at least one member of the group. If the standby name is removed from the router, the IPSec security associations (SAs) will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the **redundancy** option) will have to be reapplied to the interface.

**Note** A virtual IP address must be configured in the standby group to enable either stateless or stateful redundancy.

The **stateful** keyword enables stateful failover of The Internet Key Exchange (IKE) and IPsec sessions. Stateful Switchover (SSO) must also be configured for IPsec stateful failover to operate correctly.

**Note** A crypto map cannot be applied to a tunnel interface. If you try to apply the tunnel interface to a crypto map, an error message is displayed as follows: crypto map is configured on tunnel interface. Currently only Group Domain of Interpretation (GDOI) crypto map is supported on tunnel interface .

## Examples

The following example shows how to connect all remote Virtual Private Network (VPN) gateways to the router via 192.168.0.3::

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102
Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of mymap and, at the same time, ensures that stateless HSRP failover is facilitated between an active and standby device that belongs to the same standby group, named group1.

Reverse route injection (RRI) is also enabled to provide the ability for only the active device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If a failover occurs, routes are deleted on the former active device and created on the new active device.

The following example shows how to configure IPSec stateful failover on the crypto map named to-per-outside:

```
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

## Related Commands

| Command | Description |
|---|---|
| **crypto map (global IPsec)** | Creates or modifies a crypto map entry and enters the crypto map configuration mode. |
| **crypto map local-address** | Specifies and names an identifying interface to be used by the crypto map for IPsec traffic. |
| **redundancy inter-device** | Configures redundancy and enters inter-device configuration mode. |
| **show crypto map (IPsec)** | Displays the crypto map configuration. |
| **standby ip** | Assigns an IP address that is to be shared among the members of the HSRP group and owned by the primary IP address. |
| **standby name** | Assigns a user-defined group name to the HSRP redundancy group. |

# crypto map (Xauth)

To configure Internet Key Exchange (IKE) extended authentication (Xauth) on a router, use the **crypto map** command in global configuration mode. To restore the default value, use the **no** form of this command.

**crypto map** [**ipv6**] *map-name* **client authentication list** *list-name*
**no crypto map** [**ipv6**] *map-name* [**client authentication list**]

## Syntax Description

| | |
|---|---|
| **ipv6** | (Optional) Specifies an IPv6 crypto map. For IPv4 crypto maps, use the command without this keyword. |
| *map-name* | Name you assign to the crypto map set. |
| **client authentication list** | Designates an extended user authentication method. |
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name defined during AAA configuration. |

## Command Default

Xauth is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(4)M | This command was modified. The **ipv6** keyword was added. |

## Usage Guidelines

Before configuring Xauth, you should complete the following tasks:

- Set up an authentication list using AAA commands.
- Configure an IP Security transform.
- Configure a crypto map.
- Configure Internet Security Association Key Management Protocol (ISAKMP) policy.

After enabling Xauth, you should apply the crypto map on which Xauth is configured to the router interface.

## Examples

The following example shows how to configure user authentication (a list of authentication methods called *xauthlist* ) on an existing static crypto map called *xauthmap* :

```
crypto map xauthmap client authentication list xauthlist
```

The following example shows how to configure user authentication (a list of authentication methods called *CM_V6list)* on an existing static IPv6 crypto map called CM_V6:

```
crypto map ipv6 CM_V6 client authentication list CM_V6list
```

The following example shows how to configure user authentication (a list of authentication methods called *xauthlist* ) on a dynamic crypto map called *xauthdynamic* that has been applied to a static crypto map called *xauthmap* :

```
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp dynamic xauthdynamic
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication login** | Sets AAA authentication at login. |
| **crypto ipsec transform-set** | Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode. |
| **crypto isakmp key** | Configures a preshared authentication key. |
| **crypto isakmp policy** | Defines an IKE policy, and enters ISAKMP policy configuration mode. |
| **crypto map (global configuration)** | Creates or modifies a crypto map entry, and enters the crypto map configuration mode. |
| **interface** | Enters the interface configuration mode. |

# crypto map client configuration address

To configure IKE Mode Configuration on your router, use the **crypto map client configuration address** command in global configuration mode. To disable IKE Mode Configuration, use the **no** form of this command.

**crypto map** *tag* **client configuration address** [**initiate** | **respond**]
**no crypto map** *tag* **client configuration address**

## Syntax Description

| | |
|---|---|
| *tag* | The name that identifies the crypto map. |
| **initiate** | (Optional) A keyword that indicates the router will attempt to set IP addresses for each peer. |
| **respond** | (Optional) A keyword that indicates the router will accept requests for IP addresses from any requesting peer. |

## Command Default

IKE Mode Configuration is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(4)XE | This command was introduced. |
| 12.0(7)T | This command was implemented in Cisco IOS release 12.0(7)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

At the time of this publication, this feature is an IETF draft with limited support. Therefore this feature was not designed to enable the configuration mode for every IKE connection by default.

## Examples

The following examples configure IKE Mode Configuration on your router:

```
crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
```

## Related Commands

| Command | Description |
|---|---|
| **crypto map (global)** | Creates or modifies a crypto map entry and enters the crypto map configuration mode |

# crypto map gdoi fail-close

To specify that the crypto map is to work in fail-close mode, use the **crypto map gdoi fail-close** command in global configuration mode. To disable fail-close mode, use the **no** form of this command.

**crypto map [ipv6]***map-name* **gdoi fail-close**
**no crypto map[ipv6]***map-name* **gdoi fail-close**

## Syntax Description

| | |
|---|---|
| **ipv6** | Specifies an IPv6 crypto map. |

## Command Default

The crypto map is not in fail-close mode.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |
| 15.2(3)T | This command was modified. The **ipv6** keyword was added. |

## Examples

The following example shows how to activate fail-close mode for an IPv4 crypto map named map1. This example also defines two extended IP access lists. Unencrypted traffic from access list 102 is allowed before the group member is registered:

```
Router> enable
Router# configure terminal
Router(config)# crypto map map1 gdoi fail-close
Router(config-crypto-map-fail-close)# match address 102
Router(config-crypto-map-fail-close)# activate
Router(config-crypto-map-fail-close)# exit
Router(config)# crypto map map1 10 gdoi
Router(config-crypto-map)# set group ks1_group
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
Router(config)# access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
Router(config)# access-list 102 deny tcp any eq telnet any
Router(config)# end
```

The following example shows how to activate fail-close mode for an IPv6 crypto map named map2. This example also defines two IPv6 access lists. Unencrypted traffic from access list ACL_GETV6_ANY6 is allowed before the group member is registered:

```
Router> enable
Router# configure terminal
Router(config)# crypto map ipv6 map2 gdoi fail-close
Router(config-crypto-map-fail-close)# match address ACL_GETV6_ANY6
Router(config-crypto-map-fail-close)# activate
Router(config-crypto-map-fail-close)# exit
Router(config)# crypto map ipv6 map2 20 gdoi
Router(config-crypto-map)# set group ks2_group
Router(config-crypto-map)# match address ACL_GETV6_ANY5
Router(config-crypto-map)# exit
```

```
Router(config)# ipv6 access-list ACL_GETV6_ANY5
Router(config-ipv6-acl)# deny tcp 2001:DB8:0000::/48 2001:DB8:0001::/48 eq telnet
Router(config-ipv6-acl)# exit
Router(config)# ipv6 access-list ACL_GETV6_ANY6
Router(config-ipv6-acl)# deny tcp any eq telnet any
Router(config-ipv6-acl)# end
```

# crypto map (isakmp)

To enable Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto map**command in global configuration mode. To restore the default value, use the **no** form of this command.

**crypto map** [**ipv6**] *map-name* **isakmp authorization list** *list-name*
**no crypto map** [**ipv6**] *map-name* [**isakmp authorization list**]

## Syntax Description

| | |
|---|---|
| **ipv6** | (Optional) Specifies an IPv6 crypto map. For IPv4 crypto maps, use the command without this keyword. |
| *map-name* | Name you assign to the crypto map set. |
| **isakmp authorization list** | Specifies the Internet Security Association Key Management Protocol (ISAKMP) configuration settings and authorization parameters. |
| *list-name* | Character string used to name the list of authorization methods activated when a user logs in. The list name must match the list name defined during AAA configuration. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(4)M | This command was modified. The **ipv6** keyword was added. |

## Usage Guidelines

Use this command to enable key lookup from an AAA server.

Preshared keys deployed in a large-scale Virtual Private Network (VPN) without a certification authority, with dynamic IP addresses, are accessed during aggression mode of IKE negotiation through an AAA server. Thus, users have their own key, which is stored on an external AAA server. This allows for the central management of the user database, linking it to an existing database and allowing all users to have their own unique and secure pre-shared keys.

Before configuring this command, you should perform the following tasks:

- Set up an authorization list using AAA commands.
- Configure an IPsec transform.
- Configure a crypto map.

- Configure an ISAKMP policy using IPsec and IKE commands.

After enabling this command, you should apply the previously defined crypto map to the interface.

## Examples

The following example shows how to configure the **crypto map** command for IPv4 crypto maps:

```
crypto map ikessaaamap isakmp authorization list ikessaaalist
crypto map ikessaaamap 10 ipsec-isakmp dynamic ikessaaadyn
```

The following example shows how to configure the **crypto map** command for IPv6 crypto maps:

```
crypto map ipv6 CM_V6 isakmp authorization list aaa
crypto map ipv6 CM_V6 10 ipsec-isakmp dynamic aaadyn
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization** | Sets parameters that restrict a user's network access. |
| **crypto ipsec transform-set** | Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode. |
| **crypto isakmp key** | Configures a preshared authentication key. |
| **crypto isakmp policy** | Defines an IKE policy and enters ISAKMP policy configuration mode. |
| **crypto map (global configuration)** | Creates or modifies a crypto map entry and enters the crypto map configuration mode. |
| **interface** | Enters interface configuration mode. |

# crypto map isakmp-profile

To configure an Internet Security Association and Key Management Protocol (ISAKMP) profile on a crypto map, use the **crypto map isakmp-profile** command in global configuration mode. To restore the default values on the crypto map, use the **no** form of this command.

**crypto map** *map-name* **isakmp-profile** *isakmp-profile-name*
**no crypto map** *map-name* **isakmp-profile** *isakmp-profile-name*

## Syntax Description

| | |
|---|---|
| *map-name* | Name assigned to the crypto map set. |
| *isakmp-profile-name* | Character string used to name the ISAKMP profile that is used during an Internet Key Exchange (IKE) Phase 1 and Phase 1.5 exchange. The *isakmp-profile-name* must match the ISAKMP profile name that was defined during the ISAKMP profile configuration. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

This command describes the ISAKMP profile to use to start the IKE exchange. Before configuring this command, you must set up the ISAKMP profile.

## Examples

The following example shows that an ISAKMP profile is configured on a crypto map:

```
crypto map vpnmap isakmp-profile vpnprofile
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec transform-set** | Defines a transform set--an acceptable combination of security protocols and algorithms. |
| **crypto map (global)** | Creates or modifies a crypto map entry. |

# crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPSec traffic, use the **crypto map local-address**command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

**crypto map** *map-name* **local-address** *interface-id*
**no crypto map** *map-name* **local-address**

## Syntax Description

| | |
|---|---|
| *map-name* | Name that identifies the crypto map set. This is the name assigned when the crypto map was created. |
| *interface-id* | The identifying interface that should be used by the router to identify itself to remote peers.<br>If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If you apply the same crypto map to two interfaces and do not use this command, two separate security associations (with different local IP addresses) could be established to the same peer for similar traffic. If you are using the second interface as redundant to the first interface, it could be preferable to have a single security association (with a single local IP address) created for traffic sharing the two interfaces. Having a single security association decreases overhead and makes administration simpler.

This command allows a peer to establish a single security association (and use a single local IP address) that is shared by the two redundant interfaces.

If applying the same crypto map set to more than one interface, the default behavior is as follows:

- Each interface will have its own security association database.
- The IP address of the local interface will be used as the local address for IPSec traffic originating from/destined to that interface.

However, if you use a local-address for that crypto map set, it has multiple effects:

- Only one IPSec security association database will be established and shared for traffic through both interfaces.

- The IP address of the specified interface will be used as the local address for IPSec (and IKE) traffic originating from or destined to that interface.

One suggestion is to use a loopback interface as the referenced local address interface, because the loopback interface never goes down.

## Examples

The following example assigns crypto map set "mymap" to the S0 interface and to the S1 interface. When traffic passes through either S0 or S1, the traffic will be evaluated against the all the crypto maps in the "mymap" set. When traffic through either interface matches an access list in one of the "mymap" crypto maps, a security association will be established. This same security association will then apply to both S0 and S1 traffic that matches the originally matched IPSec access list. The local address that IPSec will use on both interfaces will be the IP address of interface loopback0.

```
interface S0
 crypto map mymap
interface S1
 crypto map mymap
crypto map mymap local-address loopback0
```

## Related Commands

| Command | Description |
|---|---|
| **crypto map (interface IPSec)** | Applies a previously defined crypto map set to an interface. |

# crypto map redundancy replay-interval

To modify the interval at which inbound and outbound replay updates are passed from an active device to a standby device, use the **crypto map redundancy replay-interval** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

**crypto map** *map-name* **redundancy replay-interval inbound** *in-value* **outbound** *out-value*
**no crypto map** *map-name* **redundancy replay-interval inbound** *in-value* **outbound** *out-value*

## Syntax Description

| | |
|---|---|
| *map-name* | Name that identifies the crypto map set. This is the name assigned when the crypto map was created. |
| **inbound** *in-value* | Number of inbound packets that are processed before an anti-replay update is sent from the active router to the standby router. |
| **outbound** *out-value* | Number of outbound packets that are processed before an anti-replay update is sent from the active router to the standby router. |

## Command Default

**inbound** *in-value* : one update every 1,000 packets

**outbound** *out-value* : one update every 100,000 packets

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. |

## Usage Guidelines

**Note** This command can be used only in conjunction with IPSec stateful failover on a crypto map.

Stateful failover enables a router to continue processing and forwarding packets after a planned or unplanned outage occurs; that is, a backup (secondary) router automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason.

The **crypto map redundancy replay-interval** command allows you to modify the interval in which an IP redundancy-enabled crypto map sends anti-replay updates from the active router to the standby router.

## Examples

The following example shows how to enable replay checking for the crypto map “to-peer-outside” and enable IPSec stateful failover:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
```

```
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

# crypto mib ipsec flowmib history failure size

To change the size of the IP Security (IPSec) MIB failure history table, use the **crypto mib ipsec flowmib history failure size**command in global configuration mode.

**crypto mib ipsec flowmib history failure size** *number*

## Syntax Description

| | |
|---|---|
| *number* | Size of the failure history table. |

## Command Default

If this command is not used, the default table size is 200.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(4)E | This command was introduced. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **crypto mib ipsec flowmib history failure size**command to change the size of a failure history table. **If you do not configure the size of a failure history table, the default of 200 will be**implemented**.**

A failure history table stores the reason for tunnel failure and the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, every failure does not correspond to a tunnel. Supported setup failures are recorded in the failure table, but a history table is not associated because a tunnel was never set up.

## Examples

The following example shows the size of a failure history table configured to be 140:

```
crypto mib ipsec flowmib history failure size 140
```

## Related Commands

| Command | Description |
|---|---|
| **crypto mib ipsec flowmib history tunnel size** | Changes the size of the IPSec tunnel history table. |
| **show crypto mib ipsec flowmib history failure size** | Displays the size of the IPSec failure history table. |

# crypto mib ipsec flowmib history tunnel size

To change the size of the IP Security (IPSec) tunnel history table, use the **crypto mib ipsec flowmib history tunnel size** command in global configuration mode.

**crypto mib ipsec flowmib history tunnel size** *number*

## Syntax Description

| | |
|---|---|
| *number* | Size of the tunnel history table. |

## Command Default

The default table size is 200.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(4)E | This command was introduced. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **crypto mib ipsec flowmib history tunnel size**command to change the size of a tunnel history table. If you do not configure the size of a tunnel history table, the default of 200 will be implemented.

A tunnel history table stores the attribute and statistics records, which contain the attributes and the last snapshot of the traffic statistics of a given tunnel. A tunnel history table accompanies a failure table, so you can display the complete history of a given tunnel. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

As an optimization, a tunnel endpoint table can be combined with a tunnel history table. However, if a tunnel endpoint table is combined, all three tables (the failure history table, tunnel history table, and the endpoint table) must remain the same size even though the MIB allows each table to be distinct.

## Examples

The following example shows the size of a tunnel history table configured to be 130:

```
crypto mib ipsec flowmib history tunnel size 130
```

## Related Commands

| Command | Description |
|---|---|
| **crypto mib ipsec flowmib history failure size** | Changes the size of the IPSec failure history table. |
| **show crypto mib ipsec flowmib history tunnel size** | Displays the size of the IPSec tunnel history table. |

# crypto mib topn

To configure TopN sampling parameters, use the **crypto mib topn**command in global configuration mode. To disable TopN sampling, use the **no** form of this command.

**crypto mib topn** [**interval** *seconds*] [**stop** *seconds*]
**no crypto mib topn** [**interval** *seconds*] [**stop** *seconds*]

## Syntax Description

| | |
|---|---|
| **interval** *seconds* | (Optional) Specifies the number of seconds between samples.The allowable range is from 60 to 86400 (60 seconds to 24 hours). The default is 300 (5 minutes).<br>Defined in the MIB as TopnMinSampleInterval. |
| **stop** *seconds* | (Optional) Specifies the time, in seconds, from when this command is executed until sampling ceases.<br>The allowable range is from 0 to 604800. A zero (0) indicates continuous sampling and is the default. For any value other than 0, the stop time value must be greater than or equal to the sampling interval value.<br>Defined in the MIB as TopnStopTime. |

## Command Default

No TopN sampling parameters are configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)E | This command was introduced. |
| 12.2(9)YE | This command was integrated into Cisco IOS Release 12.2(9)YE. |
| 12.2(9)YO1 | This command was integrated into Cisco IOS Release 12.2(9)YO1. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to rank objects according to your chosen criteria. You will not see the stop parameter setting after enabling the **show running configuration** command if the stop parameter is set at a value greater than zero. Otherwise, the current sampling parameters are recorded in the active configuration (if sampling is enabled), and sampling occurs continuously (at the specified intervals) until, and after, the device is rebooted. This command should be disabled if your criteria queries performed by XSM clients (such as VPN Device Manager [VDM]) are not to be processed.

Crypto MIB commands apply to characteristics of the IP Security (IPSec) MIBs. TopN (**topn**) is a special subset of the IPSec MIB Export (IPSMX) interface that provides a set of queries that allows ranked reports of active Internet Key Exchange (IKE) or IPSec tunnels to be obtained depending on certain criteria. While the VPN Device Manager (VDM) application retrieves and presents the data elements defined in the IKE and IPSec MIBs, the application does not use the Simple Network Management Protocol (SNMP) interface.

## Examples

The following example shows the **crypto mib topn**command being enabled with an interval frequency of 240 seconds and a designated stop time of 1200 seconds (20 minutes). At that time, the assigned sampling ceases.

```
crypto mib topn interval 240 stop 1200
```

## Related Commands

| Command | Description |
|---|---|
| **xsm** | Enables XSM client access to the router. |



# crypto pki authenticate through cws whitelisting


- crypto pki authenticate, on page 836
- crypto pki benchmark, on page 838
- crypto pki cert validate, on page 840
- crypto pki certificate chain, on page 841
- crypto pki certificate map, on page 843
- crypto pki certificate query (ca-trustpoint), on page 846
- crypto pki certificate storage, on page 848
- crypto pki crl cache, on page 850
- crypto pki crl request, on page 852
- crypto pki enroll, on page 853
- crypto pki export pem, on page 856
- crypto pki export pkcs12 password, on page 860
- crypto pki http max-buffer-size, on page 863
- crypto pki import, on page 864
- crypto pki import pem, on page 865
- crypto pki import pkcs12 password, on page 868
- crypto pki profile enrollment, on page 871
- crypto pki server, on page 873
- crypto pki server grant, on page 877
- crypto pki server info crl, on page 878
- crypto pki server info requests, on page 879
- crypto pki server password generate, on page 881
- crypto pki server reject, on page 882
- crypto pki server remove, on page 883
- crypto pki server request pkcs10, on page 884
- crypto pki server revoke, on page 888
- crypto pki server start, on page 890
- crypto pki server stop, on page 891
- crypto pki server trim, on page 892
- crypto pki server trim generate expired-list, on page 895
- crypto pki server unrevoke, on page 897
- crypto pki token change-pin, on page 898
- crypto pki token encrypted-user-pin, on page 899

- crypto pki token label, on page 901
- crypto pki token lock, on page 903
- crypto pki token login, on page 905
- crypto pki token logout, on page 906
- crypto pki token max-retries, on page 907
- crypto pki token removal timeout, on page 908
- crypto pki token secondary config, on page 910
- crypto pki token secondary unconfig, on page 912
- crypto pki token unlock, on page 914
- crypto pki token user-pin, on page 916
- crypto pki trustpoint, on page 917
- crypto pki trustpool import, on page 920
- crypto pki trustpool policy, on page 924
- crypto provisioning petitioner, on page 926
- crypto provisioning registrar, on page 928
- crypto skip-client, on page 931
- crypto vpn, on page 933
- crypto wui tti petitioner, on page 935
- crypto wui tti registrar, on page 937
- crypto xauth, on page 940
- csd enable, on page 942
- ctcp port, on page 943
- ctype, on page 944
- cts authorization list network, on page 946
- cts credentials, on page 947
- cts dot1x, on page 949
- cts manual, on page 950
- cts role-based enforcement, on page 951
- cts role-based sgt-cache, on page 952
- cts role-based sgt-caching, on page 954
- cts role-based sgt-map (config), on page 955
- cts role-based sgt-map interface , on page 958
- cts role-based sgt-map sgt, on page 960
- cts sxp connection peer, on page 961
- cts sxp default key-chain, on page 965
- cts sxp default password, on page 966
- cts sxp default source-ip, on page 968
- cts sxp enable, on page 970
- cts sxp filter-enable, on page 972
- cts sxp filter-group, on page 973
- cts sxp filter-list, on page 975
- cts sxp listener hold-time, on page 977
- cts sxp log binding-changes, on page 979
- cts sxp mapping network-map, on page 980
- cts sxp node-id, on page 981
- cts sxp reconciliation period, on page 983

- cts sxp retry period, on page 985
- cts sxp speaker hold-time, on page 986
- custom-page, on page 988
- cws out, on page 990
- cws whitelisting, on page 991

# crypto pki authenticate

To authenticate the certification authority (CA) (by getting the certificate of the CA), use the **crypto pki authenticate** command in global configuration mode.

**crypto pki authenticate** *name*

## Syntax Description

| | |
|---|---|
| *name* | The name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command . |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3T | The **crypto ca authenticate** command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca authenticate** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) was added. |

## Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you enter this command.

If you are using Router Advertisements (RA) mode (using the **enrollment**command) when you issue the **crypto pki authenticate** command, then registration authority signing and encryption certificates will be returned from the CA and the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the Rivest, Shamir, and Adelman (RSA) public key record (called the “RSA public key chain”).



**Note** If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so that it remains available. If this happens, you must reenter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted: error retrieving certificate :incomplete chain If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

## Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)#
crypto pki authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
```

## Related Commands

| Command | Description |
|---|---|
| **debug crypto pki transactions** | Displays debug messages for the trace of interaction (message type) between the CA and the router. |
| enrollment | Specifies the enrollment parameters of your CA. |
| **show crypto pki certificates** | Displays information about your certificate, the certificate of the CA, and any RA certificates. |

# crypto pki benchmark

To start or stop benchmarking data for Public Key Infrastructure (PKI) performance monitoring and optimization, use the **crypto pki benchmark**command in privileged EXEC mode.

**crypto pki benchmark** {**start** *limit* [**wrap**] | **stop**}

## Syntax Description

| | |
|---|---|
| **start** *limit* | Enables PKI benchmarking.<br>The *limit* argument states the number of records from 0 to 9990 that can be stored for the benchmarking session. A limit of 0 indicates an unlimited number of records can be stored. |
| **wrap** | (Optional) Specifies a continuous flow of records. Once the maximum number of records is gathered, they are released and a new set of records is generated. If the **wrap** keyword is not specified, then benchmarking stops once the limit for the maximum number of records has been reached. |
| **stop** | Terminates PKI benchmarking data collection. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

## Usage Guidelines

Use the **crypto pki benchmark start**command to start the collection of PKI benchmarking performance monitoring and optimization data. Use the **crypto pki benchmark stop**command to stop the collection of the PKI benchmarking performance monitoring and optimization data.

Use the **show crypto pki benchmarks  command to view the collection data.**

Use the **clear crypto pki benchmarks command to clear the**PKI benchmarking performance monitoring and optimization data and release all memory associated with this data.

The IOS PKI Performance Monitoring and Optimization feature enables you to collect the following types of PKI performance data:

- Time to validate entire certificate chain.
- Time to verify each certificate.
- Time to check revocation status for each certificate.
- Time to fetch certificate revocation list (CRL) database for each fetch location.
- Time to fetch Simple Certificate Enrollment Protocol (SCEP) method capabilities to retrieve the CRL.
- Time to process each CRL.
- Time to process the Online Certificate Status Protocol (OCSP) response. OCSP is a certificate revocation mechanism.
- Time to fetch Authentication, Authorization, and Accounting (AAA).

- CRL size.
- Validation result.
- Validation Bypass (pubkey cached).
- Method used to fetch a CRL.
- PKI session identifier.
- Crypto engine used (hardware, software, etoken).

## Examples

The following example starts PKI benchmarking data and collects 20 records. Once 20 records are collected, they are released and a new set of 20 records is generated.

```
Router# crypto pki benchmark start 20 wrap
```

## Related Commands

| Command | Description |
|---|---|
| **clear crypto pki benchmarks** | Clears PKI benchmarking performance monitoring and optimization data and releases all memory associated with this data. |
| **show crypto pki benchmarks** | Displays benchmarking data for PKI performance monitoring and optimization that was collected. |

# crypto pki cert validate

To determine if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid, use the **crypto pki cert validate** command in global configuration mode.

**crypto pki cert validate** *trustpoint*

## Syntax Description

| | |
|---|---|
| *trustpoint* | The trustpoint to be validated. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. Also, effective with Cisco IOS Release 12.3(8)T, this command replaced the **crypto ca cert validate** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **crypto pki cert validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

## Examples

The following examples show the possible output from the **crypto pki cert validate** command:

```
Router(config)# crypto pki cert validate ka
Validation Failed: trustpoint not found for ka
Router(config)# crypto pki cert validate ka
Validation Failed: can't get local certificate chain
Router(config)# crypto pki cert validate ka
Certificate chain has 2 certificates.
Certificate chain for ka is valid
Router(config)# crypto pki cert validate ka
Certificate chain has 2 certificates.
Validation Error: no certs on chain
Router(config)# crypto pki cert validate ka
Certificate chain has 2 certificates.
Validation Error: unspecified error
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the certification authority that the router should use. |
| **show crypto pki trustpoints** | Displays the trustpoints that are configured in the router. |

# crypto pki certificate chain

To enter the certificate chain configuration mode, use the **crypto pki certificate chain**command in global configuration mode.

**crypto pki certificate chain** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the certificate authority (CA). The name must match that which was declared for the CA using the **crypto pki trustpoint**command. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | The **crypto ca certificate chain** command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca certificate chain** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.4(2)T | The command output was modified to distinguish the current active certificate and the rollover certificate in the certificate chain. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

You need to be in certificate chain configuration mode to delete certificates.

## Examples

The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.

```
Router# show crypto pki certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
Router# configure terminal
Router(config)# crypto pki certificate chain myca
```

```
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
```

The following example shows a certificate chain with an active CA certificate and a shadow, or rollover, certificate:

```
Router# configure terminal
Router(config)# crypto pki certificate chain myca
certificate 06
certificate ca 01
certificate rollover 0B
 ! This is the peer's shadow PKI certificate.
certificate rollover ca 0A
! This is the CA shadow PKI certificate
```

This example shows how the certificate chain is rewritten when rollover actually happens:

```
Router# configure terminal

Router(config)# crypto pki certificate chain myca
 certificate 0B
 certificate ca 0A
```

## Related Commands

| Command | Description |
|---|---|
| **certificate** | Adds certificates manually. |

# crypto pki certificate map

To define certificate-based access control lists (ACLs), use the **crypto pki certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the no form of this command.

**crypto pki certificate map** *label sequence-number*
**no crypto pki certificate map** *label sequence-number*

## Syntax Description

| | |
|---|---|
| *label* | A user-specified label that is referenced within the **crypto pki trustpoint** command. |
| *sequence-number* | A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result. |

## Command Default

None

## Command Modes

Ca-certificate-map configuration (ca-certificate-map)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | The **crypto ca certificate map** command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca certificate map** command. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(9)T | The **serial-number** field name was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

Issuing this command places the router in ca-certificate-map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

```
field-name match-criteria match-value
```

The *field-name* field in the above example is one of the certificate fields. Field names are similar to the names used in the ITU-T X.509 standard. The *field-name* is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name, subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name** -- Case-insensitive string.
- **expires-on** --Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name** -- Case-insensitive string.
- **name** -- Case-insensitive string.
- serial-number--Case-insensitive string.
- **subject-name** --Case-insensitive string.

- **unstructured-subject-name** -- Case-insensitive string.
- **valid-start** --Date field in the format dd MM. yyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

**Note** For Yang environment, the date and time format for both the **expires-on** date and **valid-start-** field follow the same format. The string UTC should always be appended to the date and time as in yang environment the time is only accepted as Universal Time, Coordinated (UTC).

- **expires-on** -- Case sensitive string. Date field in the format mmm dd yyyy hh:mm:ss UTC.
- **valid-start** -- Case sensitive string. Date field in the format mmm dd yyyy hh:mm:ss UTC.

**Note** The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* field in the example is one of the following logical operators:

- **eq** --equal (valid for name and date fields)
- **ne** --not equal (valid for name and date fields)
- **co** --contains (valid only for name fields)
- **nc** --does not contain (valid only for name fields)
- **lt** --less than (valid only for date fields)
- **ge** --greater than or equal to (valid only for date fields)

The *match-value* field is a case-insensitive string or a date.

## Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Company to an entity within the company.com domain. The label is Company, and the sequence is 10.

```
crypto pki certificate map Company 10
 issuer-name co Company
 unstructured-subject-name co company.com
```

The following example accepts any certificate issued by Company for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto pki certificate map Group 10
 issuer-name co Company
 subject-name co DIAL
```

```
crypto pki certificate map Group 20
 issuer-name co Company
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Company” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Company” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Company” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto pki certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Company
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Company” in the proceeding example will match “o = Company,” “o =Company,” and so on.

The following example shows a CA map file used to certificate serial number session control:

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://CA1_ldap
  revocation-check crl
  match certificate crl-map1
  crypto pki certificate map crl-map1 1
  serial-number ne 489d
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |

# crypto pki certificate query (ca-trustpoint)

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto pki certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the no form of this command.

**crypto pki certificate query**
**no crypto pki certificate query**

## Syntax Description

This command has no arguments or keywords.

## Command Default

CA trustpoints are stored locally in the router's NVRAM.

## Command Modes

Ca-trustpoint configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | The **crypto ca certificate query (ca-trustpoint)** command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca certificate query (ca-trustpoint)** command. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto pki certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto pki trustpoint**command , which puts you in ca-trustpoint configuration mode.



**Note** This command deprecates the **crypto ca certificate query**command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

## Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto pki trustpoint ka
```

```
.
.
.
crypto pki certificate query
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |

# crypto pki certificate storage

To specify the local storage location for public key infrastructure (PKI) credentials, use the **crypto pki certificate storage**command in global configuration mode. To restore the default behavior, that is to store PKI credentials to NVRAM, use the no form of this command.

**crypto pki certificate storage** *location-name*
**no crypto pki certificate storage**

## Syntax Description

| | |
|---|---|
| *location-name* | Name of the local storage device.<br>• Default is NVRAM. |

## Command Default

NVRAM is the default local storage location if this command is not issued.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

All Cisco platforms support NVRAM and flash local storage. Depending on your platform, you may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token.

During run time, you can specify what active local storage device you would like to use to store PKI credentials. You must have the following system requirements before you can specify PKI credentials local storage location:

- A Cisco IOS Release 12.4(2)T PKI-enabled image or a later image
- A platform that supports storing PKI credentials as separate files
- A configuration that contains at least one certificate
- An accessible local file system

When using a local storage device to store PKI data, the following restrictions are applicable:

- Only local file systems may be used. An error message will be displayed if a remote file system is selected, and the command will not take effect.
- A subdirectory may be specified if supported by the local file system. NVRAM does not support subdirectories.
- Settings will take effect only when the running configuration is saved to the startup configuration.

If the keys are generated on the etoken, then the default storage loaction for the certificates is the etoken

for the device certificates. The CA certificates are stored in NVRAM. This allows for the credentials(keysa nd certificates) to be stored together on the removable media by default.

## Examples

The following configuration example shows how to store certificates to the certs subdirectory. The certs subdirectory does not exist and is automatically created.

```
Router# dir nvram:
 114  -rw-        4687                    <no date>  startup-config
 115  ----        5545                    <no date>  private-config
 116  -rw-        4687                    <no date>  underlying-config
   1  ----          34                    <no date>  persistent-data
   3  -rw-         707                    <no date>  ioscaroot#7401CA.cer
   9  -rw-         863                    <no date>  msca-root#826E.cer
  10  -rw-         759                    <no date>  msca-root#1BA8CA.cer
  11  -rw-         863                    <no date>  msca-root#75B8.cer
  24  -rw-        1149                    <no date>  storagename#6500CA.cer
  26  -rw-         863                    <no date>  msca-root#83EE.cer
129016 bytes total (92108 bytes free)
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki certificate storage disk0:/certs
Requested directory does not exist -- created
Certificates will be stored in disk0:/certs/
Router(config)# end
Router# write
*May 27 02:09:00:%SYS-5-CONFIG_I:Configured from console by consolemem
Building configuration...
[OK]
Router# directory disk0:/certs
Directory of disk0:/certs/
  14  -rw-         707  May 27 2005 02:09:02 +00:00  ioscaroot#7401CA.cer
  15  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#826E.cer
  16  -rw-         759  May 27 2005 02:09:02 +00:00  msca-root#1BA8CA.cer
  17  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#75B8.cer
  18  -rw-        1149  May 27 2005 02:09:02 +00:00  storagename#6500CA.cer
  19  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#83EE.cer
47894528 bytes total (20934656 bytes free)
! The certificate files are now on disk0/certs:
```

## Related Commands

| Command | Description |
|---|---|
| **show crypto pki certificates storage** | Displays the current PKI certificate storage location. |

# crypto pki crl cache

To set the maximum amount of volatile memory used to cache certificate revocation lists (CRLs), use the **crypto pki crl cache**command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

**crypto pki crl cache** *cache-size*
**no crypto pki crl cache** *cache-size*

## Syntax Description

| | |
|---|---|
| *cache-size* | The maximum CRL cache size in kilobytes.<br>• The default value is 512 kilobytes.<br>The value specified must be an integer. Specifying a cache size of zero disables CRL caching. |

## Command Default

The default CRL cache size is set to 512 kilobytes.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

The CRL cache is a global cache that holds all CRLs downloaded by the router regardless of the trustpoint configuration. The impact on router memory depends upon the CRL cache size configured by the administrator. Configuring the CRL cache size allows the amount of memory used for the CRL cache to be reduced (for instance, if low memory conditions exist) or to be increased for better performance (for instance, when a large number of CRLs are being processed).

If the **crypto pki crl cache**command is issued, regardless of the CRL cache size value set, the CRL cache size will be included in the configuration. Issuing the **no crypto pki crl cache**commandwill remove the CRL cache size from the configuration.

When a CRL is stored in the CRL cache, it is condensed at least one-fifth of its original size. Therefore, more CRLs can be stored in the CRL cache than would be expected based on the CRL size before being cached.

**Note** To configure CRL caching for a given trustpoint, you may issue either the **crl-cache none** or **crl cache delete-after** command. To disable caching of CRLs for a given trustpoint, use the **crl-cache none** command. To set a maximum age for CRLs in the cache for a given trustpoint, use the **crl cache delete-after** command.

## Examples

The following example sets the maximum CRL cache size to 2048 kilobytes and then shows sample output of the **show crypto pki crls**command:

```
Router# crypto pki crl cache 2048
```

```
Router# show crypto pki crls
     CRL Issuer Name:
           cn=ioscs,l=Anytown,c=US
           LastUpdate: 02:53:41 GMT Mar 6 2007
           NextUpdate: 02:53:41 GMT Mar 13 2007
           Retrieved from CRL Distribution Point:
                ** CDP Not Published - Retrieved via SCEP
     CRL DER is 475 bytes
     CRL is stored in parsed CRL cache
     Parsed CRL cache current size is 1705 bytes
     Parsed CRL cache maximum size is 2048 bytes
```

## Related Commands

| Command | Description |
|---|---|
| **crl cache delete-after** | Deletes a CRL from the cache after the specified number of minutes. |
| **crl cache none** | Disables caching of all CRLs. |
| **crypto pki crl request** | Requests that a new CRL be obtained immediately from the CA. |
| **show crypto pki crls** | Displays the current CRL on the router. |

# crypto pki crl request

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto pki crl request**command in global configuration mode.

**crypto pki crl request** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto pki trustpoint** command. |

## Command Default

Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | The **crypto ca crl request**command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca crl request** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto pki crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.



**Note** This command should be used only after the trustpoint is enrolled.

## Examples

The following example immediately downloads the latest CRL to your router:

```
crypto pki crl request
```

# crypto pki enroll

To obtain the certificates for your router from the certificate authority (CA), use the **crypto pki enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

**crypto pki enroll** *name*
**no crypto pki enroll** *name*

## Syntax Description

| | |
|---|---|
| *name* | The name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint**command. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.3T | The **crypto ca enroll**command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca enroll** command. |
| 12.3(14)T | The command was modified to include self-signed certificate information. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) was added. |

## Usage Guidelines

This command requests certificates from the CA for all of your router's Rivest, Shamir, and Adelmen (RSA) key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general-purpose keys, this command obtains the one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special-usage keys, this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for your keys you are prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate**command.)

The **crypto pki enroll** command is not saved in the router configuration.

**Note** If your router reboots after you issue the **crypto pki enroll** command but before you receive the certificates, you must reissue the command.

**Note** If you are using a Secure Shell (SSH) service, you should set up specific RSA key pairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructure share the same default RSA key pair, a temporary disruption of SSH service could occur. The RSA key pair could become invalid or change because of the CA system, in which case you would not be able to log in using SSH. You could receive the following error message: "key changed, possible security problem.")

### Responding to Prompts

When you issue the **crypto pki enroll** command, you are prompted a number of times.

You are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificates. When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

**Note** This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security (IPsec) or Internet Key Exchange, but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. A router has multiple IP addresses, any of which might be used with IPsec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

## Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, which checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto pki enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: <mypassword>
```

```
Re-enter password: <mypassword>
% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router(config)#
```

If necessary, the router administrator can verify the displayed fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special-usage keys would be the same as in the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

## Related Commands

| Command | Description |
|---|---|
| crypto map local address | Specifies and names an identifying interface to be used by the crypto map for IPsec traffic. |
| **debug crypto pki messages** | Displays debug messages for the details of the interaction (message dump) between the CA and the router. |
| **debug crypto pki transactions** | Displays debug messages for the trace of interaction (message type) between the CA and the router. |
| **show crypto pki certificates** | Displays information about your certificate, the certificate of the CA, and any RA certificates. |

# crypto pki export pem

To export a certificate and Rivest, Shamir, and Adleman (RSA) key pair that is associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file, use the **crypto pki export pem** command in global configuration mode. To remove any of the configured parameters, use the **no** form of this command.

**crypto pki export** *trustpoint* **pem** {**terminal** | **url** *destination-url*} {**3des** | **des**} **password** *password-phrase* [**rollover**]
**no crypto pki export** *trustpoint* **pem** {**terminal** | **url** *destination-url*} {**3des** | **des**} **password** *password-phrase* [**rollover**]

## Syntax Description

| | |
|---|---|
| *trustpoint* | Name of the trustpoint that the associated certificate and RSA key pair exports.<br>The *trustpoint* argument must match the name that was specified through the **crypto pki trustpoint** command. |
| **terminal** | Specifies the certificate and RSA key pair that is displayed in PEM format on the console terminal. |
| **url** *destination-url* | Specifies the URL of the file system where your router should export the certificate and RSA key pairs. |
| **3des** | (Optional) Exports the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm. |
| **des** | (Optional) Exports the trustpoint using the DES encryption algorithm. |
| *password-phrase* | Specifies the encrypted password phrase that is used to encrypt the PEM file for export.<br>**Note**<br>The password phrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |
| **rollover** | (Optional) Exports certificate authority (CA) shadow, or rollover, certificate. |

## Command Default

Certificates and RSA keys are not exported.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | The **crypto ca export pem** command was introduced. |
| 12.3(7)T | This command was introduced. This command replaced the **crypto ca export pem** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.4(2)T | This command was modified. The **rollover** keyword was added. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.2(1)T | This command was modified. Support was added in the CLI for hiding the password in an exported PEM-formatted file with the introduction of the **password** keyword followed by the *password-phrase* argument. |

## Usage Guidelines



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The **crypto pki export pem** command allows you to export certificate and RSA key pairs in PEM-formatted files. The PEM files can then be imported back into the Cisco IOS router (via the **crypto pki import pem** command) or other public key infrastructure (PKI) applications.

The RSA keys in PEM-formatted files can be exported from the following source URL file systems:

***Table 28: Destination URL File Systems from Which RSA Keys in PEM-formatted Files Are Exported***

| File System | Description |
|---|---|
| **archive:** | Exports from the archive file system. |
| **disk0:** | Exports from the disc0 file system. |
| **disk1:** | Exports from the disc1 file system. |
| **ftp:** | Exports from the FTP file system. |
| **http:** | Exports from the HTTP file system. The URL must be in the following formats:<br>• http://*pem_location*:80, where *pem_location* is the Domain Name System (DNS)<br>• http://*ipv4-address*:80. For example: http://10.10.10.1:80<br>• *http://[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be encased in brackets in the URL. |
| **https:** | Exports from the HTTPS file system. The URL must use the same formats as the HTTP: file system formats. |
| **null:** | Exports from the null file system. |
| **nvram:** | Exports from the non-volatile random-access memory (NVRAM) file system. |
| **pram:** | Exports from the parameter random-access memory (PRAM) file system. |
| **rcp:** | Exports from the remote copy protocol (rcp) file system |
| **scp:** | Exports from the secure copy protocol (scp) file system. |

| File System | Description |
|---|---|
| **snmp:** | Exports from the Simple Network Management Protocol (SNMP). |
| **system:** | Exports from the system file system. |
| **tftp:** | Exports from the Trivial File Transfer Protocol (TFTP) file system.<br>**Note**<br>The URL must be in the form: tftp://*pem_location/file_specification* |
| **tmpsys:** | Exports from the Cisco IOS tmpsys file system. |
| **unix:** | Exports from the UNIX file system. |

## Examples

The following example shows how to generate and export the RSA key pair "aaa" and certificates of the router in PEM files that are associated with the trustpoint named "mycs":

```
Router(config)# crypto key generate rsa general-keys label aaa exportable

The name for the keys will be:aaa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be:Router
% The subject name in the certificate will be:bizarro.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Request certificate from CA? [yes/no]:y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint: 8DA777BC 08477073 A5BE2403 812DD157
```

```
00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto pki export aaa pem terminal 3des password cisco123
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
    Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki import pem** | Imports certificates and RSA keys to a trustpoint from PEM-formatted files. |
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| **enrollment url (ca-trustpoint)** | Specifies the enrollment parameters of a CA. |

# crypto pki export pkcs12 password

To export Rivest, Shamir, and Adleman (RSA) keys within a Public-key cryptography standards number 12 (PKCS12) file at a specified location, use the **crypto pki export pkcs12 password** command in global configuration mode. To remove any of the configured parameters, use the **no** form of this command.

**crypto pki export** *trustpointname* **pkcs12** *destination-url* **password** *password-phrase*
**no crypto pki export** *trustpointname* **pkcs12** *destination-url* **password** *password-phrase*

## Syntax Description

| | |
|---|---|
| *trustpointname* | Name of the trustpoint that issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name. |
| *destination-url* | Location of the PKCS12 file to which a user wants to import the RSA key pair. |
| *password-phrase* | Password phrase that is used to encrypt the PKCS12 file for export. |

## Command Default

RSA keys within a PKCS12 file are not exported.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | The **crypto ca export pkcs12** command was introduced. |
| 12.3(7)T | This command was introduced. This command replaced the **crypto ca export pkcs12** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.2(1)T | This command was modified. Support was added in the CLI for hiding the password in an exported PKCS12-formatted file with the introduction of the **password** keyword followed by the *password-phrase* argument. |

## Usage Guidelines

Public-key cryptography standards were devised and published by RSA Security. A PKCS12 file has a format commonly used to store private keys with accompanying public key certificates that is protected with a password-based symmetric key. The **crypto pki export pkcs12 password** command creates a PKCS12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

### Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA key pair is more secure than a password phrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS12 file, the RSA key pair now is only as secure as the password phrase.

To create a good password phrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the password phrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

The RSA keys can be exported from the following destination URL file systems:

***Table 29: Destination URL File Systems from Which RSA Keys Exported***

| File System | Description |
|---|---|
| **archive:** | Exports from the archive file system. |
| **cns:** | Exports from the cns file system. The Cisco CNS Configuration Engine is a web-based system for automatically distributing configuration files to Cisco IOS network devices. |
| **disk0:** | Exports from the disc0 file system. |
| **disk1:** | Exports from the disc1 file system. |
| **ftp:** | Exports from the FTP file system. |
| **http:** | Exports from the HTTP file system. The URL must be in the following formats:<br>• http://*pkcs12_location*:80, where *pkcs12_location* is the Domain Name System (DNS).<br>• http://*ipv4-address*:80. For example: http://10.10.10.1:80.<br>• *http://[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL. |
| **https:** | Exports from the HTTPS file system. The URL must use the same formats as the HTTP: file system formats. |
| **null:** | Exports from the null: file system. |
| **nvram:** | Exports from the non-volatile random-access Memory (NVRAM) file system. |
| **pram:** | Exports from the parameter random-access memory (PRAM) file system. |
| **rcp:** | Exports from the remote copy protocol (rcp) file system. |
| **scp:** | Exports from the secure copy protocol (scp) file system. |
| **snmp:** | Exports from the Simple Network Management Protocol (SNMP). |
| **system:** | Exports from the system file system. |
| **tar:** | Exports from the UNIX tar file system. |
| **tftp:** | Exports from the Trivial File Transfer Protocol (TFTP) file system.<br>**Note**<br>The URL must be in the form: tftp://*pkcs12_location/file_specification*<br>. |
| **tmpsys:** | Exports from the Cisco IOS tmpsys file system. |

| File System | Description |
|---|---|
| **unix:** | Exports from the UNIX file system. |
| **xmodem:** | Exports from the Cisco xmodem file system. |
| **ymodem:** | Exports from the Cisco ymodem file system. |

## Examples

The following example exports an RSA key pair with a trustpoint named “mytp” to an HTTP file:

```
Router(config)# crypto pki export mytp pkcs12 http://[2001:DB8:1:1::1]:80 password myexport
 mycompany
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki import pkcs12 password** | Imports RSA keys. |

# crypto pki http max-buffer-size

To set the maximum http receive buffer for PKI, use the **crypto pki http <max-buffer-size>** command in the global configuration mode.

**crypto pki http max-buffer-size** <*max-buffer-size*>

## Syntax Description

| | |
|---|---|
| *max-buffer-size* | Specifies the maximum limit for the http buffer. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 17.2.1 | This command was introduced in the 17.2.1 release, and was later enabled in the Cisco IOS XE 16.6.8, 16.9.5, and 16.12.3 releases. |

## Usage Guidelines

The **crypto pki http max-buffer-size** command enables you to set the maximum http receive buffer for PKI. By default, the http max-buffer size is 10MB. You can increase this value till 100MB and reduce the value till 1MB by using this command.

It is recommended that you set the max-buffer-size only when you see the following error displayed during PKI transactions: *(debug crypto pki transaction) "CRYPTO_PKI: HTTP Payload is more than the allowed buffer size"*.

### Example

```
Router(config)#crypto pki http max-buffer-size ?
  <1-100>  Specify the size in MB

Router(config)#crypto pki http max-buffer-size 9
```

# crypto pki import

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto pki import**command in global configuration mode.

**crypto pki import** *name* **certificate**

## Syntax Description

| | |
|---|---|
| *name* **certificate** | Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | The **crypto ca import** command was introduced. |
| 12.3(7)T | This command replaced the **crypto ca import** command. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) was added. |

## Usage Guidelines

You must enter the **crypto pki import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

## Examples

The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is “MS.”

```
crypto pki trustpoint MS
 enroll terminal
 crypto pki authenticate MS
!
crypto pki enroll MS
crypto pki import MS certificate
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| **enrollment** | Specifies the enrollment parameters of your CA. |
| **enrollment terminal** | Specifies manual cut-and-paste certificate enrollment. |

# crypto pki import pem

To import certificates and Rivest, Shamir, and Adleman (RSA) keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files, use the **crypto pki import pem** command in global configuration mode. To remove any of the configured parameters, use the **no** form of this command.

**crypto pki import** *trustpoint* **pem** [**check** | **exportable***usage-keys*] {**terminal** | **url** *source-url*} **password** *password-phrase*
**no crypto pki import** *trustpoint* **pem** [**check** | **exportable***usage-keys*] {**terminal** | **url** *source-url*} **password** *password-phrase*

## Syntax Description

| | |
|---|---|
| *trustpoint* | Name of the trustpoint that is associated with the imported certificates and RSA key pairs.<br>The *trustpoint* argument must match the name that was specified through the **crypto pki trustpoint** command. |
| **check** | (Optional) Specifies that an outdated certificate is not allowed. |
| **exportable** | (Optional) Specifies that the imported RSA key pair can be exported again to another Cisco device such as a router. |
| *usage-keys* | (Optional) Specifies that two RSA special usage key pairs are imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair. |
| **terminal** | Specifies that certificates and RSA key pairs are manually imported from the console terminal. |
| **url** *source-url* | Specifies the URL of the file system where your router should import the certificates and RSA key pairs. |
| **password** *password-phrase* | Specifies the encrypted password phrase that is used to encrypt the PEM file for import.<br>**Note**<br>The password phrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |

## Command Default

Certificates and RSA keys are not imported.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | The **crypto ca import pem** command was introduced. |
| 12.3(7)T | This command was introduced. This command replaced the **crypto ca import pem** command. |

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2 XN | This command was modified. The **check** keyword was added. |
| 15.2(1)T | This command was modified. Support was added in the CLI for hiding the password in an imported PEM-formatted file with the introduction of the **password** keyword followed by the *password-phrase* argument. |

## Usage Guidelines

The **crypto pki import pem** command allows certificates and RSA key pairs in PEM-formatted files to be imported. The files can be previously exported from another router or generated from other public key infrastructure (PKI) applications.

The RSA keys in PEM-formatted files can be imported from the following source URL file systems:

***Table 30: Source URL File Systems from Which RSA Keys in PEM-formatted Files are Imported***

| File System | Description |
|---|---|
| **archive:** | Imports from the archive file system |
| **cns:** | Imports from the CNS file system. The Cisco CNS Configuration Engine is a web-based system for automatically distributing configuration files to Cisco IOS network devices. |
| **disk0:** | Imports from the disc0 file system. |
| **disk1:** | Imports from the disc1 file system. |
| **ftp:** | Imports from the FTP file system. |
| **http:** | Imports from the HTTP file system. The URL must be in the following formats:<br>• http://*pem_location:80*:80, where *pem_location:80* is the Domain Name System (DNS)<br>• http://*ipv4-address*:80. For example: http://10.10.10.1:80<br>• *http://[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL. |
| **https:** | Imports from the HTTPS file system. The URL must use the same formats as the HTTP: file system formats. |
| **null:** | Imports from the null: file system. |
| **nvram:** | Imports from the non-volatile random-access memory (NVRAM) file system. |
| **pram:** | Imports from the parameter random-access memory (PRAM) file system. |
| **rcp:** | Imports from the remote copy protocol (rcp) file system. |
| **scp:** | Imports from the secure copy protocol (scp) file system. |

| File System | Description |
|---|---|
| **snmp:** | Imports from the Simple Network Management Protocol (SNMP). |
| **system:** | Imports from the system file system. |
| **tar:** | Imports from the UNIX tar file system. |
| **tftp:** | Imports from the Trivial File Transfer Protocol (TFTP) file system.<br>**Note**<br>The URL must be in the form: tftp://*pem_location/file_specification* |
| **tmpsys:** | Imports from the IOS tmpsys file system. |
| **unix:** | Imports from the UNIX file system. |
| **xmodem:** | Imports from the Cisco xmodem file system. |
| **ymodem:** | Imports from the Cisco ymodem file system. |

## Examples

The following example shows how to import PEM files to trustpoint "ggg" through TFTP:

```
Router(config)# crypto pki import ggg pem url tftp://10.1.1.2/johndoe/msca cisco1234
% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.ca]?
Reading file from tftp://10.1.1.2/johndoe/msca.ca
Loading johndoe/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]
% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.prv]?
Reading file from tftp://10.1.1.2/johndoe/msca.prv
Loading johndoe/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]
% Importing  certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.crt]?
Reading file from tftp://10.1.1.2/johndoe/msca.crt
Loading johndoe/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki export pem** | Exports certificates and RSA keys that are associated with a trustpoint in a PEM-formatted file. |
| **crypto pki trustpoint** | Declares the CA that your router should use. |
| **enrollment url (ca-trustpoint)** | Specifies the enrollment parameters of a CA. |

# crypto pki import pkcs12 password

To import Rivest, Shamir, and Adleman (RSA) keys, use the **crypto pki import pkcs12 password** command in global configuration mode. To remove any of the configured parameters, use the **no** form of this command.

**crypto pki import** *trustpointname* **pkcs12** *source-url* **password** *password-phrase*
**no crypto pki import** *trustpointname* **pkcs12** *source-url* **password** *password-phrase*

## Syntax Description

| | |
|---|---|
| *trustpointname* | Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name. |
| *source-url* | The location of the PKCS12 file to which a user wants to export the RSA key pair. |
| **password** *password-phrase* | Enter the password phrase that must be entered to undo encryption when the RSA keys are imported. |

## Command Default

No default behavior or values

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | The **crypto ca import pkcs12** command was introduced. |
| 12.3(7)T | This command was introduced. This command replaced the **crypto ca import pkcs12** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.2(1)T | This command was modified. Support was added in the CLI for hiding the password in an imported PKCS12-formatted file with the introduction of the **password** keyword followed by the *password-phrase* argument. |

## Usage Guidelines

When you enter the **crypto pki import pkcs12 password** command, a key pair and a trustpoint are generated.

If the key pair and trustpoint that were generated need to be removed, then enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto pki trustpoint** command to remove the trustpoint.



**Note** After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

The RSA keys can be imported from the following source URL file systems:

*Table 31: Source URL File Systems from Which RSA Keys Imported*

| File System | Description |
|---|---|
| **archive:** | Imports from the archive file system. |
| **check** | The **check** keyword is used to validate a certificate on input from a file system. Any file system argument indicated in this table can be used following this keyword. |
| **cns:** | Imports from the CNS file system. The Cisco CNS Configuration Engine is a web-based system for automatically distributing configuration files to Cisco IOS network devices. |
| **disk0:** | Imports from the disc0 file system. |
| **disk1:** | Imports from the disc1 file system. |
| **ftp:** | Imports from the FTP file system. |
| **http:** | Imports from the HTTP file system. The URL must be in the following formats:<br>• http://*pkcs12_location*:80, where *pkcs12_location* is the Domain Name System (DNS)<br>• http://*ipv4-address*:80. For example: http://10.10.10.1:80<br>• *http://[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL. |
| **https:** | Imports from the HTTPS file system. The URL must use the same formats as the HTTP file system formats. |
| **null:** | Imports from the null file system. |
| **nvram:** | Imports from the non-volatile random-access memory (NVRAM) file system. |
| **pram:** | Imports from the parameter random-access memory (PRAM) file system. |
| **rcp:** | Imports from the remote copy protocol (rcp) file system. |
| **scp:** | Imports from the secure copy protocol (scp) file system. |
| **snmp:** | Imports from the Simple Network Management Protocol (SNMP). |
| **system:** | Imports from the system file system. |
| **tar:** | Imports from the UNIX tar file system. |
| **tftp:** | Imports from the Trivial File Transfer Protocol (TFTP) file system.<br>**Note**<br>The URL must be in the form: tftp://pkcs12_location/file_specification. |
| **tmpsys:** | Imports from the IOS tmpsys file system. |
| **unix:** | Imports from the UNIX file system. |
| **xmodem:** | Imports from the Cisco xmodem file system. |

| File System | Description |
|---|---|
| **ymodem:** | Imports from the Cisco ymodem file system. |

## Examples

In the following example, an RSA key pair that has been associated with the trustpoint named "mytp" is to be imported:

```
Router(config)# crypto pki import mytp pkcs12 http://[2001:DB8:1:1::1]:80 password myimport
 mycompany
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki export pkcs12 password** | Exports RSA keys. |
| **crypto key zeroize rsa** | Deletes all RSA keys from your router. |
| **crypto pki trustpoint** | Declares the CA that your router should use. |

# crypto pki profile enrollment

To define an enrollment profile, use the **crypto pki profile enrollment**command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

**crypto pki profile enrollment** *label*
**no crypto pki profile enrollment** *label*

## Syntax Description

| | |
|---|---|
| *label* | Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command. |

## Command Default

An enrollment profile does not exist.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)ZH | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| 12.3(7)T | This command replaced the **crypto ca profile enrollment** command. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto pki profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command** --Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal** --Specifies manual cut-and-paste certificate authentication requests.
- **authentication url** --Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command** --Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal** --Specifies manual cut-and-paste certificate enrollment.
- **enrollment url** --Specifies the URL of the CA server to which to send enrollment requests.
- **parameter** --Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.

**Note** The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

## Examples

The following example shows how to define the enrollment profile named "E" and associated profile parameters:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial
crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the PKI trustpoint that your router should use. |
| **enrollment profile** | Specifies that an enrollment profile can be used for certificate authentication and enrollment. |

# crypto pki server

To enable a Cisco IOS certificate server (CS) and enter certificate server configuration mode, or to immediately generate shadow certification authority (CA) credentials, use the **crypto pki server** command in global configuration mode. To disable the certificate server (which is the default functionality), use the **no** form of this command.

**crypto pki server** *cs-label* [**rollover** [**cancel**]]
**no crypto pki server** *cs-label* [**rollover** [**cancel**]]

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server.<br>**Note**<br>The certificate server name should not exceed 13 characters. |
| **rollover** | (Optional) Immediately generates a shadow CA certificate.<br>**Note**<br>If the **auto-enroll** command has been issued with the **regenerate** keyword, shadow keys will also be generated.<br>**Note**<br>If the shadow certificate and keys are already present this command will fail. |
| **cancel** | (Optional) Deletes the exiting shadow CA certificate when used with the **rollover** keyword.<br>Shadow keys will also be deleted if they exist. |

## Command Default

A certificate server is not enabled; the automatic CA certificate rollover process is not initiated.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.4(2)T | The **rollover** and **cancel** keywords were introduced to support automated CA certificate rollover functionality. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Once the **crypto pki server** command is entered, the certificate server configuration mode commands can be configured to deploy the public key infrastructure (PKI) by defining the default behavior of the CS, which limits user interface complexity. See the Related Commands section for more information on these commands.

**Note** All CS-related commands are optional; therefore any basic CS functionality that is not specified through the CLI for these commands uses their default value.

- **issuer-name** -- Specifies the distinguished name (DN) as the CA issuer name for the certificate server.
- **lifetime (certificate server)** --Specifies the lifetime of the CA or a certificate.
- **lifetime crl** --Defines the lifetime of the certificate revocation list (CRL) that is used by the certificate server.
- **shutdown** --Allows a certificate server to be disabled without removing the configuration.

### Automated CA Certificate Rollover

CAs and their clients, have certificates with expiration dates that have to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring it must generate a new certificate and possibly a new key pair. This process, called rollover, allows for continuous operation of the network while clients and the certificate server are switching from an expiring CA certificate to a new CA certificate.

## Examples

The following example shows how to enable the certificate server "mycertserver":

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database url tftp://mytftp/johndoe/mycertserver
```

The following example shows how to disable the certificate server "mycertserver":

```
Router(config)# no crypto pki server mycertserver
% This will stop the Certificate Server process and delete the server
  configuration
Are you sure you want to do this? [yes/no]: yes
% Do you also want to remove the associated trustpoint and
  signing certificate and key? [yes/no]: no
% Certificate Server Process stopped
```

The following example shows a shadow client certificate request from a terminal:

```
Router# crypto pki server mycs rollover request pkcs10 terminal

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE REQUEST-----
MIIBUTCBuwIBADASMRAwDgYDVQQDEwdOZXdSb290MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDMHeev1ERSs320zbLQQk+3lhV/R2HpYQ/iM6uT1jkJf5iy0UPR
wF/X16yUNmG+ObiGiW9fsASF0nxZw+fO7d2X2yh1PakfvF2wbP27C/sgJNOw9uPf
sBxEc40Xe0d5FMh0YKOSAShfZYKOflnyQR2Drmm2x/33QGol5QyRvjkeWQIDAQAB
oAAwDQYJKoZIhvcNAQEEBQADgYEALM90r4d79X6vxhD0qjuYJXfBCOvv4FNyFsjr
aBS/y6CnNVYySF8UBUohXYIGTWf4I4+sj6i8gYfoFUW1/L82djS18TLrUr6wpCOs
RqfAfps7HW1e4cizOfjAUU+C7lNcobCAhwF1o6q2nIEjpQ/2yfK9O7sb3SCJZBfe
eW3tyCo=
-----END CERTIFICATE REQUEST-----
```

The following example shows the **redundancy**, **show**, and **serial-number** keywords in the **crypto pki server**command.

```
Router(config)#crypto pki server MYCA
Router(cs-server)#grant auto
Router(cs-server)#redundancy
Router(cs-server)#serial-number 0x4c
Router(cs-server)#show
```

```
 redundancy
 serial-number 0x4C
 grant auto
end
```

## Related Commands

| Command | Description |
|---|---|
| **auto-rollover** | Enables the automated CA certificate rollover functionality. |
| **cdp-url** | Specifies a CDP to be used in certificates that are issued by the certificate server. |
| **crl (cs-server)** | Specifies the CRL PKI CS. |
| **database archive** | Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file. |
| **database level** | Controls what type of data is stored in the certificate enrollment database. |
| **database url** | Specifies the location where database entries for the CS is stored or published. |
| **database username** | Specifies the requirement of a username or password to be issued when accessing the primary database location. |
| **default (cs-server)** | Resets the value of the CS configuration command to its default. |
| **grant auto rollover** | Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA. |
| **grant auto trustpoint** | Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests. |
| **grant none** | Specifies all certificate requests to be rejected. |

| Command | Description |
|---|---|
| **grant ra-auto** | Specifies that all enrollment requests from an RA be granted automatically. |
| **hash (cs-server)** | Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA. |
| **issuer-name** | Specifies the DN as the CA issuer name for the CS. |
| **lifetime (cs-server)** | Specifies the lifetime of the CA or a certificate. |
| **mode ra** | Enters the PKI server into RA certificate server mode. |
| **mode sub-cs** | Enters the PKI server into sub-certificate server mode |
| **redundancy (cs-server)** | Specifies that the active CS is synchronized to the standby CS. |
| **serial-number (cs-server)** | Specifies whether the router serial number should be included in the certificate request. |
| **show (cs-server)** | Displays the PKI CS configuration. |
| **shutdown (cs-server)** | Allows a CS to be disabled without removing the configuration. |

# crypto pki server grant

To grant all or certain simple certificate enrollment protocol (SCEP) requests, use the **crypto pki server grant**command in privileged EXEC mode.

**crypto pki server** *cs-label* **grant** {**all***req-id*}

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| all | All certificate enrollment requests are granted. |
| *req-id* | ID associated with a specific enrollment request in the enrollment request database. Use the **crypto pki server info requests** command to display the ID. |

## Command Default

If this command is not issued, the certificate server keeps the requests in a pending state.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

After you enable the **crypto pki server grant** command, your certificate server will immediately grant all specified certificate requests. Certificate requests that are not granted will expire after the time that was specified using the **lifetime enrollment-request** command.

## Examples

The following example shows to grant all manual enrollment requests for the certificate server "mycs":

```
Router# crypto pki server mycs grant all
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| crypto pki server reject | Rejects all or certain SCEP requests. |

# crypto pki server info crl



**Note** Effective with Cisco IOS Release 12.4(20)T, the **crypto pki server info crl** command is replaced by the **show crypto pki server crl**command. See the **show crypto pki server crl** command for more information.

To display information regarding the status of the current certificate revocation list (CRL), use the **crypto pki server info crl** command in privileged EXEC mode.

**crypto pki server** *cs-label* **info crl**

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.4(20)T | This command was replaced by the **show crypto pki server crl**command. |

## Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. To access information, such as the lifetime and location of the CRL, use the **crypto pki server info crl**command.

## Examples

The following example shows how to access CRL information for the certificate server “mycs”:

```
Router# crypto pki server mycs info crl
```

## Related Commands

| Command | Description |
|---|---|
| cdp-url | Specifies a CDP to be used in certificates that are issued by the certificate server. |
| **crypto pki server** | Enables a Cisco IOS certificate server and enter certificate server configuration mode. |
| lifetime crl | Defines the lifetime of the CRL that is used by the certificate server. |

# crypto pki server info requests



**Note** Effective with Cisco IOS Release 12.4(20)T, the **crypto pki server info requests** command is replaced by the **show crypto pki server requests**command. See the **show crypto pki server requests** command for more information.

To display all outstanding certificate enrollment requests, use the **crypto pki server info requests**command in privileged EXEC mode.

**crypto pki server** *cs-label* **info requests**

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.4(2)T | The command output was modified to include shadow CA certificate information. |
| 12.4(20)T | This command was replaced by the **show crypto pki server requests**command. |

## Usage Guidelines

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See the **show pki server** command for a complete list of certificate enrollment request states.)
  - The certificate server refers to the command-line interface (CLI) configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each Simple Certificate Enrollment Protocol (SCEP) query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a “pending” or “denied” state.
  - Forwards to the request to the certification authority (CA) core, where it will generate and sign the appropriate certificate, store the certificate in the enrollment request database, and return the request to the built-in certificate server SCEP server, who will reply to the end user with the certificate on the next SCEP request.

If the connection of the client has closed, the certificate server will wait for client user to request another certificate.

All enrollment requests transitions through the certificate enrollment states that are defined in the table below.

*Table 32: Certificate Enrollment Request State Descriptions*

| Certificate Enrollment State | Description |
|---|---|
| initial | The request has been created by the SCEP server. |
| authorized | The certificate server has authorized the request. |
| malformed | The certificate server has determined that the request is invalid for cryptographic reasons. |
| denied | The certificate server has denied the request for policy reasons. |
| pending | The enrollment request must be manually accepted by the network administrator. |
| granted | The CA core has generated the appropriate certificate for the certificate request. |

## Examples

The following example shows output for the certificate server "certsrv1," which has a pending certificate enrollment request:

```
Router# crypto pki server certsrv1 info requests
   Enrollment Request Database:
   ReqID  State      Fingerprint                       SubjectName
   --------------------------------------------------------------------
   1      pending    0A71820219260E526D250ECC59857C2D serialNumber=2326115A+hostname=831.
```

The following example shows the output for shadow PKI certificate info requests:

```
Router# crypto pki server mycs info requests
Enrollment Request Database:
RA certificate requests:
  ReqID  State      Fingerprint                       SubjectName
--------------------------------------------------------------------
RA rollover certificate requests:
  ReqID  State      Fingerprint                       SubjectName
  --------------------------------------------------------------------
Router certificates requests:
  ReqID  State      Fingerprint                       SubjectName
--------------------------------------------------------------------
1      pending    A426AF07FE3A4BB69062E0E47198E5BF hostname=client
  Router rollover certificates requests:
  ReqID  State      Fingerprint                       SubjectName
  --------------------------------------------------------------------
  2      pending    B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters PKI configuration mode. |

# crypto pki server password generate

To generate a password for simple certificate enrollment protocol (SCEP) requests that can be used only one time, use the **crypto pki server password generate**command in privileged EXEC mode.

**crypto pki server** *cs-label* **password generate** [*minutes*]

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| *minutes* | (Optional) Length of time, in minutes, that the password is valid. Valid times range from 1 to 1440 minutes. The default value is 60 minutes. |

## Command Default

If this command is not enabled, no password is created.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

SCEP, which is the only supported enrollment protocol, supports two client authentication mechanisms--manual and preshared key. Manual enrollment requires the administrator at the certification authority (CA) server to specifically authorize the enrollment requests; enrollment using preshared keys allows the administrator to preauthorize enrollment requests by generating a one-time password.

**Note** Only one password is valid at a time; if a second password is generated, the previous password is no longer valid.

## Examples

The following example shows how to generate a one-time password that is valid for 75 minutes for the certificate server “mycs”:

```
Router# crypto pki server mycs password generate 75
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |

# crypto pki server reject

To reject all or certain Simple Certificate Enrollment Protocol (SCEP) requests, use the **crypto pki server reject** command in privileged EXEC mode.

**crypto pki server** *cs-label* **reject** {**all***req-id*}

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| all | All certificate enrollment requests are rejected. |
| *req-id* | ID associated with a specific enrollment request in enrollment request database. Use the **crypto pki server info requests** command to display the ID. |

## Command Default

If this command is not issued, the certificate server keeps the requests in a pending state.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

After you enable the **crypto pki server reject** command, your certificate server will immediately reject all certificate requests.

SCEP, which is the only supported enrollment protocol, supports two client authentication mechanisms--manual and preshared key. Manual enrollment requires the administrator at the certification authority (CA) server to specifically authorize the enrollment requests. The administrator can become overloaded if there are numerous enrollment requests. Thus, the **crypto pki server reject** command can be reduce user interaction by automatically rejecting all or specific enrollment requests.

## Examples

The following example shows how reject all manual enrollment requests for the certificate server "mycs":

```
Router# crypto pki server mycs reject all
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| **crypto pki server grant** | Grants all or certain SCEP requests. |
| crypto pki server info requests | Displays all outstanding certificate enrollment requests. |

# crypto pki server remove

To remove enrollment requests that are in the certificate server Enrollment Request Database, use the **crypto pki server remove**command in privileged EXEC mode . This command does not have a **no** form.

**crypto pki server** *cs-label* **remove** {**all***req-id*}

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. |
| **all** | Removes all enrollment requests. |
| *req-id* | Removes the specified enrollment request. |

## Command Default

Enrollment requests will remain in the certificate server database.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. |

## Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. Before this command was added, the request would be left in the Enrollment Request Database for 1 hour until the client polled the certficiate server for the result of the request. This command allows you to remove individual or all requests from the database, especially useful if the client leaves and never polls the certificate server.

*In addition, the use of this command also allows the server to be returned to a clean slate with respect to the keys and transaction IDs. Thus, it is a useful command to use during troubleshooting with a Simple Certificate Enrollment Protocol (SCEP) client that may be behaving badly.*

## Examples

The following example shows that all enrollment requests are to be removed from the certificate server:

```
Router# enable
 Router# crypto pki server server1 remove all
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server info request** | Displays all outstanding enrollment requests. |

# crypto pki server request pkcs10

To manually add a certificate request to the request database, use the **crypto pki server request pkcs10**command in privileged EXEC mode.**command** *argument* **keyword**

**crypto pki server** *cs-label* **request pkcs10** {*url* | **terminal**} [**base64** | **pem** | **scep hex**]

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| *url* | URL of the file systems from which the certificate server should retrieve the PKCS10 enrollment request and to which it should post the granted certificate. For a list of available options, see the table below.<br>**Note**<br>The request filename should have a ".req" extension and the granted certificate file name will have a ".crt" extension (see the URL example in the section "Examples" below). |
| **terminal** | Certificate requests will be manually pasted from the console terminal, and the granted certificate will be displayed on the console. |
| base64 | (Optional) Specifies the certificate will be returned without privacy-enhanced mail (PEM) headers, regardless of whether PEM headers were used in the request. |
| pem | (Optional) Specifies the certificate will be returned with PEM headers automatically added to the certificate after the certificate is granted, regardless of whether PEM headers were used in the request. |
| **scep hex** | (Optional) Specifies the certificate will be returned in hexadecimal. Pending requests will also be synchronized with the standby certificate server in hexadecimal. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 15.0(1)M | The command was modified to accept the PKCS10 certificate and the signing certificate in hexadecimal as well as in base64 encoding. |

## Usage Guidelines

Use the **crypto pki server request pkcs10** command to manually add a base64-encoded, PEM-formatted, or hexadecimal-encoded PKCS10 certificate enrollment request. This command is especially useful when the client does not have a network connection with the certificate server so that it can do Simple Certificate Enrollment Protocol (SCEP) enrollment. After the certificate is granted, the certificate will be displayed on the console terminal using base64 encoding if the **terminal** keyword is specified, or it will be sent to the file system that is specified using the *url* argument.

The *url* argument allows you to specify or change the location in which the certificate server retrieves the new certificate request and posts the granted certificate. The table below lists available file system options.

***Table 33: crypto pki server request pkcs10 Options***

| Location | Description |
|---|---|
| cns: | Retrieves certificate from Cisco Networking Services (CNS): file system |
| flash: | Retrieves certificate from flash: file system |
| ftp: | Retrieves certificate from FTP: file system |
| http: | Retrieves certificate from HTTP: file system |
| https: | Retrieves certificate from Secure HTTP (HTTPS): file system |
| null: | Retrieves certificate from null: file system |
| nvram: | Retrieves certificate from NVRAM: file system |
| rcp: | Retrieves certificate from remote copy protocol (rcp): file system |
| scp: | Retrieves certificate from secure copy protocol (scp): file system |
| system: | Retrieves certificate from system: file system |
| tftp: | Retrieves certificate from TFTP: file system |

## Examples

The following example shows how to manually add a base64-encoded certificate request with PEM boundaries to the request database:

```
Router# crypto pki server mycs request pkcs10 terminal pem
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE REQUEST-----
MIIBdTCB3wIBADA2MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEPMA0GA1UEAxMGdGVzdCAxMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDF
EFukc2lCFSHtDJn6HFR2n8rpdhlAYwcs0m68N3iRYHonv847h0/H6utTHVd2qEEo
rNw97jMRZk6BLhVDc05TKGHvUlBlHQWwc/BqpVI8WiHzZdskUH/DUM8kd67Vkjlb
e+FF7WrWT4FIO4vR4rF1V2p3FZ+A29UNc9Pi1s98nQIDAQABoAAwDQYJKoZIhvcN
AQEEBQADgYEAUQCGNzzNJwBOCwmEmG8XEGFSZWDmFlctm8VWvaZYMPOt+vl6iwFk
RmtD1Kg91Vw/qT5FJN8LmGUopOWIrwH4rUWON+TqtRmv2dgsdL5T4dx0sgG5E0s4
T302paxEHiHVRJpe8OD7FJgOvdsKRziCpyD4/Jfb1WnSVQZmvIYAxVQ=
-----END CERTIFICATE REQUEST-----

% Enrollment request pending, reqId=2

Router# crypto pki server mycs grant 2
% Granted certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBAzANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDgyODAxMTcyOVoXDTA1MDgyODAxMTcyOVowNjELMAkGA1UEBhMCVVMx
FjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxDzANBgNVBAMTBnRlc3QgMTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAxRBbpHNpQhUh7QyZ+hxUdp/K6XYZQGMHLNJu
vDd4kWB6J7/OO4dPx+rrUx1XdqhBKKzcPe4zEWZOgS4VQ3NOUyhh71JQZR0FsHPw
aqVSPFoh82XbJFB/w1DPJHeu1ZI5W3vhRe1q1k+BSDuL0eKxdVdqdxWfgNvVDXPT
4tbPfJ0CAwEAAaNCMEAwHwYDVR0jBBgwFoAUggWpVwokbUtGIwGZGavh6C8Bq6Uw
```

```
HQYDVR0OBBYEFFD3jZ/d960qzCGKwKNtFvq85Xt6MA0GCSqGSIb3DQEBBAUAA4GB
AAE4MqerwbM/nO8BCyZAiDzTqwLGnNvzS4H+u3JCsm0LaxY+E3d8NbSY+HruXWaR
7QyjprDGFd9bftRoqGYuiQkupU13sIHEyf3C2KnXJB6imySvAiuaQrGdSuUSIhBO
Xfh/xdWo3XL1e3vtWiYUa4X6jPUMpn74HoNfB4/gHO7g
-----END CERTIFICATE-----
```

The following example shows how to retrieve a certificate request and add it to the request database (using the *url* argument):

**Note** The request file name should have a ".req" extension and the certificate file name a ".crt" extension.

```
Router# crypto pki server mycs request pkcs10 tftp://192.0.2.129/router5
% Retrieving Base64 encoded or PEM formatted PKCS10 enrollment request...
Reading file from tftp://192.0.2.129/router5.req
Loading router5.req from 192.0.2.129 (via Ethernet0): !
[OK - 582 bytes]
% Enrollment request pending, reqId=1
Router# crypto pki server mycs grant 1
% Writing out the granted certificate...
!Writing file to tftp://192.0.2.129/router5.crt!
```

The following example shows how to manually add a hexadecimal-encoded certificate request with PEM boundaries to the request database:

```
Router# crypto pki server mycs request pkcs10
 scep hex 0C4A3A2CA5C2E66DDCD740A4259759E2 5811E7CB133BAC936EF48C6187F4AD22 3
PKCS10 request in hex
Enter the PKCS10 in hexidecimal representation....
Router(config-pubkey)#3082010E 3081B902 0100301D 311B3019 06092A86 4886F70D 01090216 0C697073
Router(config-pubkey)#6563662D 33383435 61305C30 0D06092A 864886F7 0D010101 0500034B 00304802
Router(config-pubkey)#4100B660 EF764AD6 A896E03E 0D1A1A16 5450857C 9B2CC04E B61719E5 2216CBF2
Router(config-pubkey)#1973B464 17E78829 22CDBD87 FBD015F1 2A0A8DD7 5396EAA1 A2A65132 912466D2
Router(config-pubkey)#62C90203 010001A0 37301406 092A8648 86F70D01 09073107 13056369 73636F30
Router(config-pubkey)#1F060A60 86480186 F8450109 08311104 0F300D30 0B060355 1D0F0404 030205A0
Router(config-pubkey)#300D0609 2A864886 F70D0101 04050003 410062A5 81B4C7F2 BDCEE03D 998BAD2B
Router(config-pubkey)#1E763461 EBB812EB 4082E2BB 273AA5DD 74FF7E12 E16035E9 4525A041 AF65E48F
Router(config-pubkey)#F0E6E13C 2646F943 5C23A634 BC50BC1F 343A
Router(config-pubkey)#30820123 3081CE02 0101300D 06092A86 4886F70D 01010405 00301D31 1B301906
Router(config-pubkey)#092A8648 86F70D01 0902160C 69707365 63662D33 38343561 301E170D 30393031
Router(config-pubkey)#31323032 33323039 5A170D31 39303131 30303233 3230395A 301D311B 30190609
Router(config-pubkey)#2A864886 F70D0109 02160C69 70736563 662D3338 34356130 5C300D06 092A8648
Router(config-pubkey)#6F70D01 01010500 034B0030 48024100 B660EF76 4AD6A896 E03E0D1A 1A165450
Router(config-pubkey)#857C9B2C C04EB617 19E52216 CBF21973 B46417E7 882922CD BD87FBD0 15F12A0A
Router(config-pubkey)#8DD75396 EAA1A2A6 51329124 66D262C9 02030100 01300D06 092A8648 86F70D01
Router(config-pubkey)#01040500 03410041 B2EBC44A 7F5FD26A DBAAB574 655D0C5D 84CCC7B5 48643525
Router(config-pubkey)#E85E4E06 5465A27F 6066BC8C 52AF9FF4 CE6A9C66 44441BF0 053325DC 736FD696
Router(config-pubkey)#97F8335 DDA951
Router(config-pubkey)#quit
Enter the certificate in hexidecimal representation....
Router(config-pubkey)#quit
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| crypto pki server grant | Grants all or certain SCEP requests. |

| Command | Description |
|---|---|
| **show crypto pki server** | Displays the current state and configuration of a certificate server. |

# crypto pki server revoke

To revoke a certificate on the basis of its serial number, use the **crypto pki server revoke**command in privileged EXEC mode.

**crypto pki server** *cs-label* **revoke** *certificate-serial-number*

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| *certificate-serial-number* | Serial number of the certificate that is to be revoked. The serial number can be a hexadecimal number with the prefix "0x" (for example, 0x4c) or a decimal number (for example, 76). |

## Command Default

Certificates are revoked on the basis of their name.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 15.0(1)M | The command was modified to remove the serial-number check against the last-issued serial number. |

## Usage Guidelines

When a new certificate revocation list (CRL) is issued, the certificate server obtains the previous CRL, makes the appropriate changes, and resigns the new CRL. A new CRL is issued after a certificate is revoked from the CLI. If this process negatively affects router performance, the crypto pki server revoke command can be used to revoke a list or range of certificates.

**Note** In Cisco IOS Release 15.0(1)M, the serial number to be revoked is not compared with the last-issued serial number.

**Note** A new CRL cannot be issued unless the current CRL is revoked or changed.

## Examples

The following examples show how to revoke a certificate with the serial number 76 (for example, 0x4c in hexidecimal) from the certificate server "mycs":

```
Router# crypto pki server mycs revoke 76
Router# crypto pki server mycs revoke 0x4c
```

## Related Commands

| Command | Description |
|---|---|
| **cdp-url** | Specifies that CDP should be used in the certificates that are issued by the certificate server. |
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |

# crypto pki server start

To enable a Cisco IOS certificate server, use the **crypto pki server start** command in privileged EXEC mode. To disable a certificate server, use the **crypto pki server stop** command.

**crypto pki server** *servername* **start**

## Syntax Description

| | |
|---|---|
| *servername* | Name of the certificate server.<br>**Note**<br>The certificate server name must not exceed 13 characters. |

## Command Default

The certificate server is disabled.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

Using the **crypto pki server start** command is the same as using the **no shut** command in DSP configuration mode.

## Examples

The following example shows how to enable a certificate server on a router:

```
Router# crypto pki server MYCA start
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
% Certificate Server enabled.
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server stop** | Disables a Cisco IOS certificate server. |
| **show crypto pki server** | Displays the current state and configuration of a certificate server. |

# crypto pki server stop

To disable a Cisco IOS certificate server, use the **crypto pki server stop** command in privileged EXEC mode.

**crypto pki server** *servername* **stop**

## Syntax Description

| | |
|---|---|
| *servername* | Name of the certificate server. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

Using the **crypto pki server stop** command is the same as using the **shutdown** command in DSP configuration mode.

## Examples

The following example shows how to disable a certificate server:

```
Router# crypto pki server MYCA stop
Certificate server 'shut' event has been queued for processing.
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server start** | Enables a Cisco IOS certificate server. |
| **show crypto pki server** | Displays the current state and configuration of a certificate server. |

# crypto pki server trim

To trim certificates from the certificate revocation list (CRL), use the **crypto pki server trim**command in privileged EXEC mode.

**crypto pki server** [*cs-label*] **trim** {**expired** [*start-number* [*end-number*] [**verbose**]] | **generate expired-list** [*start-number end-number*] [**url** *url*] | **url** *url* [**verbose**]}

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified using the **crypto pki server** command. |
| **expired** | Specifies that the expired certificates are to be trimmed from the CRL. |
| *start-number* | The beginning of the certificate serial number range to check and trim from the CRL if the certificate has expired. |
| *end-number* | (Optional) The ending number of the certificate serial number range to check and trim from the CRL if the certificate has expired. |
| **verbose** | Displays information about the action taken on the certificates checked in the CRL. |
| **generate** | Generates information about CRL trimming. |
| **expired-list** | Generates information about trimmed expired certificates. |
| **url** *url* | Specifies the location of the expired certificate list, which contains a list of certificate serial numbers to be trimmed from the CRL. |

## Command Default

All certificates in the specified certificate server database will be searched to locate and to trim expired certificates.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **generate** keyword was added. |

## Usage Guidelines

This command trims expired certificates from the CRL. Only certificates that are expired and have accurate and complete information in the certificate database can be trimmed from the database.

Depending on the size and location of the certificate database, searching the database for expired certificates may be a time-consuming process. Depending on your environment, you may choose one of three methods to search and to trim your CRL:

- Search the entire certificate database.

This is usually the most time-consuming and resource-consuming method.

- Specify a range of certificate serial numbers to search.

If a large number of certificates are in your certificate database or if your certificate database is stored at a remote location (for example, TFTP or Secure Copy [SCP]) you may limit the range of certificates to search by specifying both the starting and ending certificate serial numbers. If no starting and ending certificate serial numbers are specified, the entire certificate database will be searched and all expired certificates will be trimmed.

- Use an input list to specify the expired certificates to be trimmed from the CRL.

This is the most scalable method because it divides the process into two steps: searching the certificate database for expired certificates and trimming the CRL. An input file listing expired certificate serial numbers may be generated using a Perl script or similar program, manually, or by issuing the **crypto pki server trim generate expired-list** command. The input list must follow the format as shown:

```
# CRL Trimming file generated on 01/31/2008
version=1
35
37
```

Lines that begin with a pound sign (#) are inserted comments. The second line contains a version string indicating the file type. Each remaining line (in this example lines 35 and 37) contains a certificate serial number indicating one certificate to be removed from the CRL.

## Examples

The following example shows how to check and trim the CRL of all expired certificates in the certificate database for the certificate server “mycs”:

```
Router#
crypto pki server mycs trim expired
```

The following example shows how to check and trim the CRL of expired certificates within the certificate serial number range 0x1-0x3 in the certificate database for the certificate server “mycs”. The result is the same as generating and using an input file of expired certificate serial numbers, as shown in the next example.

```
Router# crypto pki server mycs trim expired 0x1 end 0x3
```

The following example shows how to generate a list of expired certificate serial numbers, store the list on an HTTP server, then use the resulting list to trim the CRL of all expired certificates for the certificate server “mycs”:

```
Router# crypto pki server mycs trim generate expired-list 0x1 0x3 url
http://databaselocation/expired-certs.1st
Router# crypto pki server mycs trim url http://databaselocation/expired-certs.1st
The following example shows how to check and trim the CRL for only one certificate serial
number in the certificate database for the certificate server "mycs." If the certificate
with the serial number 45 has expired, it will be trimmed from the CRL.
Router# crypto pki server mycs trim expired 0x2
The following example shows how to trim the CRL of all expired certificates for the
certificate server "mycs" and display the resulting action taken for each certificate serial
 number:
Router#
crypto pki server mycs trim expired verbose
Certificate 2: Expired. Removed from CRL.
Certificate F4240: Expired. Removed from CRL.
```

```
Certificate 4593: Not Removed.
Certificate 1234: Not Removed.
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| **crypto pki server trim generate expired-list** | Generates a list of expired certificates in the CRL. |

# crypto pki server trim generate expired-list

To generate a list of expired certificates in the current certificate revocation list (CRL), use the **crypto pki server trim generate expired-list**command in privileged EXEC mode.

**crypto pki server** *cs-label* **trim generate expired-list** [**start** *number* **end** *number*] [**url** *url*]

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| **start** *number* | (Optional) The first certificate serial number from which to begin searching the CRL for expired certificates. To locate expired certificates within a range both the starting certificate serial number and the ending certificate serial number must be specified. |
| **end** *number* | (Optional) The last certificate serial number that will be checked when searching the CRL for a range of expired certificates. |
| **url** *url* | (Optional) Specifies the location where the resulting list of expired certificates will be stored. |

## Command Default

All certificates in the specified certificate server database will be searched to locate expired certificates.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

This command generates a list of expired certificates that are in the CRL for the specified certificate server. The resulting list of expired certificates may be used as input to the **crypto pki server trim** command to remove the listed certificates from the CRL resulting in trimming, or revoking, the expired certificates.

Only certificates that have accurate and complete information in the certificate database can be automatically added to the list of expired certificates and later trimmed from the database. Only CRL entries for expired certificates can be trimmed.

If there are a large number of certificates in your certificate database or if your certificate database is stored at a remote location, for example TFTP or SCP, you may limit the range of certificates to search by specifying both the starting and ending certificate serial numbers. If no starting and ending certificate serial numbers are specified, the entire certificate database will be searched and all expired certificates will be added to the expired certificates list.

A URL may be specified to save the list of expired certificates to a specified location. If no URL is specified, the list of expired certificates will be printed on your terminal. The list may then be cut and pasted to a file.

## Examples

```
The following example shows both how to generate a list of expired certificates within the
 certificate serial number range 34-38 in the certificate database for the certificate
server "mycs" and how to save the resulting list to an HTTP location:
```

```
Router#
crypto pki server mycs trim generate expired-list start 34 end 38 url
http://databaselocation/expired-certs.1st
```

The following example shows the resulting list of expired certificates in the file expired-certs.1st:

```
# CRL Trimming file generated on 01/31/2008
version=1
35
37
```

Lines that begin with a pound sign (#) are inserted comments. The second line contains a version string indicating the file type. Each remaining line, in this example lines 35 and 37, contains a certificate serial number indicating one certificate to be removed from the CRL.

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| **crypto pki server trim** | Trims certificates from the certificate revocation list. |

# crypto pki server unrevoke

To recover a revoked certificate, that is to remove a certificate from the certificate revocation list (CRL), use the **crypto pki server unrevoke**command in privileged EXEC mode.

**crypto pki server** *cs-label* **unrevoke** *certificate-serial-number*

## Syntax Description

| | |
|---|---|
| *cs-label* | Name of the certificate server. The name must match the name specified via the **crypto pki server** command. |
| *certificate-serial-number* | Serial number of the certificate that is to be recovered. The serial number can be a hexadecimal number with the prefix "0x" (for example, 0x4c) or a decimal number (for example, 76). |

## Command Default

None.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

If a certificate is erroneously revoked, either the client has to reenroll in the PKI or the administrator may recover the revoked certificate by issuing the **crypto pki server unrevoke** command. This command removes a certificate, specified by its serial number, from the CRL. The CRL is then resigned and can be republished.

## Examples

The following examples show how to unrevoke a certificate with the serial number 76, or 0x4c in hexidecimal, from the certificate server "mycs":

```
Router# crypto pki server mycs unrevoke 76
Router# crypto pki server mycs unrevoke 0x4c
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| **cyrpto pki server revoke** | Revokes a certificate based on its serial number. |

# crypto pki token change-pin

To change the user PIN on the USB eToken, use the **crypto pki token change-pin** command in privileged EXEC mode.

**crypto pki token** *token-name* [**admin**] **change-pin** [*pin*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB token specified via the **crypto pki token login**command. |
| **admin** | (Optional) The router will change the administrative PIN on the USB token. If this keyword is not issued, the router will change the user pin. |
| *pin* | (Optional) User PIN required to access the etoken. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

If you want to change the administrative PIN on the token, you must be logged into the eToken as an admin via the **crypto pki token admin login**command.

After the user PIN has been changed, you must reset the login failure count to zero (via the **crypto pki token max-retries** command). The maximum number of allowable login failures is set (by default) to 15.

## Examples

The following example shows that the user PIN was changed to 1234:

```
crypto pki token usbtoken0 admin login 5678
crypto pki token usbtoken0 change-pin 1234
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token login** | Logs into the USB eToken. |
| **crypto pki token max-retries** | Sets the maximum number of allowed failed login attempts. |

# crypto pki token encrypted-user-pin

To encrypt a USB token PIN that is stored in private NVRAM, use the **crypto pki token encrypted-user-pin** command in global configuration mode. To decrypt the token's PIN, use the **no** form of this command.

**crypto pki token** {*token-name* | **default**} **encrypted-user-pin** [**write**] [**passphrase** *passphrase*]
**no crypto pki token** {*token-name* | **default**} **encrypted-user-pin** [**write**] [**passphrase** *passphrase*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of the token that will have its PIN encrypted. |
| **default** | Configures default values for tokens. |
| **write** | **(Optional) Writes to memory immediately after the passphrase is entered. This keyword saves the running configuration to NVRAM.** |
| **passphrase** *passphrase* | (Optional) Enables noninteractive command-line interface (CLI). If you do not issue this keyword, you will automatically be prompted for the passphrase.<br>**Tip**<br>Noninteractive CLI is provided for instances where users will not be responding to prompts, for example in scripts, configuration tools, or other automated processes.<br>If you are issuing this command from the console, it is recommended that you use the interactive CLI to help protect against observation from unauthorized persons. |

## Command Default

The PIN stored in private NVRAM is not encrypted.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco IOS Release 12.4(11)T and implemented on 7200VXR NPE-G2 platform. |
| 15.0(1)M | This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After the token's PIN is encrypted with the **crypto pki token encrypted-user-pin**command, no action is taken when you insert the token into the router. The user must log in to the router and enter the passphrase to decrypt the PIN before the router can use the PIN to log in to the token.

After the PIN has been successfully decrypted, the router will execute the configuration commands from the token at privilege level 15.

**Tip** It is recommended that you create a passphrase different from the token's PIN. Also, the user should log in to the token as a "normal user" (a privilege level 1 user), so the user cannot access commands that can alter the configuration of the router.

## Examples

The following example shows the configuration of a user PIN and the encryption of that user PIN:

```
! Configure the user PIN.
Router(config)#
crypto pki token usbtoken0: user-pin
Enter password:
!
! Now, the user PIN can be encrypted.
!
Router(config)#
crypto pki token usbtoken0: encrypted-user-pin
 Enter passphrase:
Router(config)#
exit
Router#
Router#
show running config
.
.
.
     crypto pki token usbtoken0 user-pin *encrypted*
.
.
.
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token user-pin** | Creates a PIN that automatically allows the router to log in to the USB token at router startup. |
| **privilege** | Configures a new privilege level for users and associates commands with that privilege level. |

# crypto pki token label

To set or change the name of a USB token label, use the **crypto pki token label** command in global configuration mode.

**crypto pki token** *device* **: label** *token-label*

## Syntax Description

| | |
|---|---|
| *device:* | Location or name of the USB device. |
| *token-label* | Specifies the label, or name, of the USB token.<br>• *token-label* may be up to 31 alphanumeric characters in length, including dashes and underscores. |

## Command Default

No label is set. The USB token is known by its factory name.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After you have logged in your USB token to the router, you may want to change the factory default label. Changing the default factory name to a unique name is useful when configuring multiple USB tokens for automatic login, secondary configuration files, or other token specific settings.

**Note** Either the device name or label may be used to specify the USB token. If using the device name, it is followed by a colon, ":".

## Examples

The following example shows how to change the USB token label from the "oldlabel" to "newlabel" after the token has been logged in. The router will not use the "newlabel" until the next time the token is inserted or the router is reloaded:

```
Router#
Router# configure terminal
Router(config)# crypto pki token oldlabel label newlabel
Token label changed.
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token user-pin** | Creates a PIN that automatically allows the router to log into the USB token at router startup. |

# crypto pki token lock

To lock the token, use the **crypto pki token lock**command in privileged EXEC mode.

**crypto pki token** *token-name* **lock** [**user-pin**] [**passphrase** *passphrase*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of the token that is to be locked. |
| **user-pin** | (Optional) Specifies the USB token PIN if set. |
| **passphrase** *passphrase* | (Optional) Enables the noninteractive command-line interface (CLI). If you do not issue this keyword, you will automatically be prompted for the passphrase.<br>**Tip**<br>The noninteractive CLI is provided for instances where users will not be responding to prompts, for example in scripts, configuration tools, or other automated processes.<br><br>If you are issuing this command from the console, it is recommended that you use the interactive CLI to help protect against observation from unauthorized persons. |

## Command Default

The token is not locked.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After you have locked a token with the **crypto pki token lock** command, all Rivest, Shamir, and Adelman (RSA) keys that have been loaded from the token will be deleted and, if configured, the secondary “unconfig” file will run with full privileges.

## Examples

The following example shows how to reload a router, unlock the PIN, and then lock the PIN again:

Router> **enable**

Password:

Router# **crypto pki token usbtoken0: unlock**

Token eToken is usbtoken0

Enter passphrase:

Token login to usbtoken0(eToken) successful

Router#

Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken

```
Login Successful
```

Router# **crypto pki token usbtoken0: lock**

**Related Commands**

| Command | Description |
|---|---|
| **crypto pki token name secondary unconfig file** | Specifies a secondary “unconfig” file. |
| **crypto pki token unlock** | Unlocks the token and decrypts the PIN that is stored in private NVRAM. |

# crypto pki token login

To log into the USB eToken, use the **crypto pki token login** command in privileged EXEC mode.

**crypto pki token** *token-name* [**admin**] **login** [*pin*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB eToken. |
| **admin** | (Optional) The router will attempt to log into the token as an administrator. If this keyword is not issued, the router will attempt to log into the token as a user.<br>**Note**<br>If you want to change the PIN via the **crypto pki token change-pin** command, you must issue this keyword. |
| *pin* | (Optional) User PIN required to access the token. If a user PIN is not specified, the default PIN, 1234567890, is used. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

This command allows you to manually log into a USB eToken. To automatically log into an eToken, issue the **crypto pki token user-pin** command, which allows you to create a PIN for automatic login.

## Examples

The following example shows how to log into the USB eToken manually:

```
crypto pki token usbtoken0:login 1234567890
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token logout** | Logs the router out of the USB eToken. |

# crypto pki token logout

To log the router out of the USB eToken, use the **crypto pki token logout** command in privileged EXEC mode.

**crypto pki token** *token-name* **logout**

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB eToken specified via the **crypto pki token login**command. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

If you want to save any data to the USB eToken, you must log back into the eToken.

## Examples

The following example shows how to successfully log out of a USB eToken:

```
crypto pki token usbtoken0:logout
Token eToken is usbtoken0
Token logout from usbtoken0(eToken) successful
*Jan 28 05:46:59.544:%CRYPTO-6-TOKENLOGOUT:Cryptographic Token eToken Logout Successful
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token login** | Logs into the USB eToken. |

# crypto pki token max-retries

To set the maximum number of allowed failed login attempts, use the **crypto pki token max-retries**command in global configuration mode. To return to the default functionality (which is 15 failed login attempts), use the **no** form of this command.

**crypto pki token** {*token-name* | **default**} **max-retries** [*number*]
**no crypto pki token** {*token-name* | **default**} **max-retries** [*number*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB token that the router will log into. |
| **default** | Default value is to be used. |
| *number* | (Optional) Number of consecutive failed login attempts the router will allow before locking out the user. Available range: 0 to 15. Default value is 15. |

## Command Default

15 failed login attempts are allowed

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After the user PIN is changed via the **crypto pki token c hange-pin command**, the login failure count is automatically reset to 15; however, it is recommended that the login failure count be set to zero.

## Examples

The following example shows how to change the allowed maximum number of failed login attempts to 20:

```
crypto pki token usbtoken0 max-retries 20
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token c hange-pin** | Changes the user PIN number on the USB eToken. |
| **crypto pki token login** | Logs into the USB eToken. |

# crypto pki token removal timeout

To set the time interval that the router waits before removing the Rivest, Shamir, and Adelman (RSA) keys that are stored in the eToken, use the **crypto pki token removal timeout**command in global configuration mode. To return to the default functionality (which is no timeout), use the **no** form of this command.

**crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*]
**no crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB eToken that is being removed from the router. |
| **default** | Default value, which is automatic RSA key removal, is to be used. |
| *seconds* | (Optional) Time interval, in seconds, that the router waits before removing the RSA keys and tearing down IP Security (IPSec) tunnels associated with the specified eToken. Available range: 0 to 480.<br>**Note**<br>If a time interval is not specified, all RSA keys and associated tunnels are immediately torn down after the eToken is removed from the router. |

## Command Default

The default timeout is zero, which causes the RSA keys to be removed automatically after the eToken is removed from the router . The default appears in the running configuration as:

```
crypto pki token default removal timeout 0
```

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After the eToken is removed from the router, you can clear from your router any RSA keys that were obtained from the eToken; all IPSec tunnels that used those RSA keys for authentication are also torn down. Both the keys and tunnels are immediately cleared unless otherwise specified via the **crypto pki token removal timeout** command.

Although the RSA keys remain on the eToken, they can only be accessed with the correct PIN. Too many unsuccessful attempts to log into the eToken will disable the PIN and any further login attempts will be refused.

**Note** The **no** version of this command does not remove RSA keys from the router. To immediately remove RSA keys from the router, set the timeout value to zero.

## Examples

The following example shows how to set the time that the router will wait before removing the RSA keys that are stored in the eToken after the eToken has been removed from the router:

```
crypto pki token usbtoken0 removal timeout 60
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token logout** | Logs the router out of the USB token. |
| crypto pki token max-retries | Sets the maximum number of allowed failed login attempts. |

# crypto pki token secondary config

To merge a specified file with the running configuration after the eToken is logged in to the router, use the **crypto pki token secondary config** command in global configuration mode. To remove the specified file, use **no** form of the command.

**crypto pki token** {*token-name* | **default**} **secondary config** [*file*]
**no crypto pki token** {*token-name* | **default**} **secondary config** [*file*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB eToken that will have its running configuration merged with the secondary configuration file. |
| **default** | Sets the default values for tokens. |
| *file* | (Optional) Name of the file that will be merged with the running configuration.<br>**Note**<br>The filename is relative to the eToken, so the name should not include a device name such as "usbtoken0:." |

## Command Default

A secondary configuration file does not exist.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| 15.0(1)M | This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

Use the **crypto pki token secondary config** command if you want to merge, not overwrite, a file with the running configuration on the router. The secondary configuration is processed after the eToken is logged in to the router.

## Examples

The following example shows how to merge the secondary configuration file "CONFIG1.CFG" with the current running configuration:

```
Router# configure terminal
Router(config)# crypto pki token default secondary config CONFIG1.CFG
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token login** | Logs in to the USB eToken. |
| **crypto pki token user-pin** | Creates a PIN that automatically allows the router to log into the USB eToken at router startup. |

# crypto pki token secondary unconfig

To specify a secondary "unconfig" file and its location for a USB token, use the **crypto pki token secondary unconfig** command in global configuration mode. To remove secondary configuration elements from the running configuration, use the **no** form of this command.

**crypto pki token** {*token-name* | **default**} **secondary unconfig** [*file*]
**no crypto pki token** {*token-name* | **default**} **secondary unconfig** [*file*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of the token that is to be unlocked. |
| **default** | Configures default values for tokens. |
| *file* | (Optional) Name and location of the secondary configuration file. |

## Command Default

Secondary "unconfig" file will not be processed.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| 15.0(1)M | This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

Configuration files that exist on a USB token are called secondary configuration files. If you create and configure a secondary configuration file, it is executed after the token is logged in. The existence of a secondary configuration file is determined by the presence of a secondary configuration file option in the Cisco IOS configuration stored in NVRAM.

When the token is removed, logged out, or the removal timer (if set) expires, a separate "unconfig" file is processed to remove all secondary configuration elements from the running configuration. Secondary configuration and secondary "unconfig" files are executed at privilege level 15 and are not dependent on the level of the user logged in.

## Examples

The following example shows a how a secondary "unconfig" file might be used to remove secondary configuration elements from the running config. For example, a secondary configuration file might be used to set up a public key infrastructure (PKI) trustpoint. A corresponding "unconfig" file, named mysecondaryunconfigfile.cfg, might contain the following command:

no crypto pki trustpoint token-tp

If the token were removed and the following commands executed, the trustpoint and associated certificates would be removed from the router's running configuration:

```
Router#
configure terminal
Router(config)# no crypto pki token mytoken secondary unconfig mysecondaryunconfigfile.cfg
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token secondary config** | Merges a specified secondary configuration file with the running configuration after the USB token is logged in to the router. |
| **crypto pki token user-pin** | Creates a PIN that automatically allows the router to log in to the USB token at router startup. |

# crypto pki token unlock

To unlock the token and decrypt the PIN that is stored in private NVRAM, use the **crypto pki token unlock** command in privileged EXEC mode.

**crypto pki token** *token-name* **unlock** [**user-pin**] [**passphrase** *passphrase*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of the token that is to be unlocked. |
| **user-pin** | (Optional) Specifies the USB token PIN if set. |
| **passphrase** *passphrase* | (Optional) Enables the noninteractive command-line interface (CLI). If you do not issue this keyword, you will automatically be prompted for the passphrase.<br>**Tip**<br>The noninteractive CLI is provided for instances where users will not be responding to prompts, for example in scripts, configuration tools, or other automated processes.<br>**Note**<br>If you are issuing this command from the console, it is recommended that you use the interactive CLI to help protect against observation from unauthorized persons. |

## Command Default

USB token is not unlocked, or decrypted.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After you unlock a token via the **crypto pki token unlock** command, the Cisco IOS software will treat the token as if it is automatically logged into the router. Any Rivest, Shamir, and Adelman (RSA) keys on the token are loaded onto the router and the secondary configuration file on the token is executed (if a secondary configuration file has been configured by the user). Secondary configuration files are executed with full user privileges.

## Examples

The following example shows the configuration and encryption of a user PIN and then that the router is reloading and the user PIN is being unlocked.

```
! Configuring the user PIN

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# crypto pki token usbtoken0: user-pin
```

```
Enter password:
! Encrypt the user PIN
Router (config)# crypto pki token usbtoken0: encrypted-user-pin
Enter passphrase:
Router(config)# exit
Router#
Sep 20 21:51:38.076: %SYS-5-CONFIG_I: Configured from console by console
Router# show running-config
crypto pki token usbtoken0 user-pin *encrypted*
! Reloading the router.
Router> enable
Password:
! Decrypting the user pin.
Router# crypto pki token usbtoken0: unlock
Token eToken is usbtoken0
Enter passphrase:
Token login to usbtoken0(eToken) successful
Router#
Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken
Login Successful
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki token user-pin** | Creates a PIN that automatically allows the router to log into the USB token at router startup. |

# crypto pki token user-pin

To create a PIN that automatically allows the router to log in to the USB eToken at router startup, use the **crypto pki token user-pin** command in global configuration mode. To remove the stored PIN from the configuration, use t he **no** form of this command.

**crypto pki token** {*token-name* | **default**} **user-pin** [*pin*] [*token-pin*]
**no crypto pki token** {*token-name* | **default**} **user-pin** [*pin*] [*token-pin*]

## Syntax Description

| | |
|---|---|
| *token-name* | Name of USB eToken that the router will log in to. |
| **default** | Sets the default values for tokens. |
| **user-pin** | Specifies the PIN to access token. |
| *pin* | (Optional) User PIN required to log in to the eToken. The PINs are stored in private NVRAM. If a user PIN is not specified, the default PIN, 1234567890, will be used. |
| *token-pin* | (Optional) Token PIN name. |

## Command Default

If this command is not issued, the router cannot access the eToken.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(11)T | This command was integrated into the Cisco 7200VXR NPE-G2 platform. |
| 15.0(1)M | This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added. |
| Cisco IOS XE Release 3.6 | This command was integrated into Cisco IOS XE Release 3.6. |

## Usage Guidelines

After the eToken is plugged into the router, the router will use the specified PIN (or the default PIN if no PIN is specified) to automatically log in as the user.

## Examples

The following example shows how to access the eToken via the user PIN “12345”:

```
crypto pki token usbtoken0 user-pin 12345
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki login** | Logs in to the USB eToken. |
| **crypto pki token logout** | Logs the router out of the USB eToken. |

# crypto pki trustpoint

To declare the trustpoint that your router should use, use the **crypto pki trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

**crypto pki trustpoint** *name* **redundancy**
**no crypto pki trustpoint** *name*

## Syntax Description

| | |
|---|---|
| *name* | Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.) |
| **redundancy** | (Optional) Specifies that the key, and any certificates associated with it, should be synchronized to the standby certificate authority (CA). |

## Command Default

Your router does not recognize any trustpoints until you declare a trustpoint using this command.

Your router uses unique identifiers during communication with Online Certificate Status Protocol ( OCSP) servers, as configured in your network.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | The **crypto ca trustpoint** command was added. |
| 12.2(15)T | The **match certificate** subcommand was introduced. |
| 12.3(7)T | This command replaced the **crypto ca trustpoint** command. You can still enter the **crypto ca trusted-root** or **crypto ca trustpoint** command, but the command will be written in the configuration as “crypto pki trustpoint.” |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.3(14)T | The **enrollment selfsigned**subcommand was introduced. |
| 12.4(4)T | The **ocsp disable-nonce** subcommand was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.0(1)M | This command was modified. The **redundancy**keyword was introduced. |

## Usage Guidelines

### Declaring Truspoints

Use the **crypto pki trustpoint** command to declare a trustpoint, which can be a self-signed root certificate authority (CA) or a subordinate CA. Issuing the **crypto pki trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint using the following subcommands:

- **crl** --Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)** --Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment** --Specifies enrollment parameters (optional).
- **enrollment http-proxy** --Accesses the CA by HTTP through the proxy server.
- **enrollment selfsigned** --Specifies self-signed enrollment (optional).
- **match certificate** --Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map**command.
- **ocsp disable-nonce** --Specifies that your router will not send unique identifiers, or nonces, during OCSP communications
- **primary** --Assigns a specified trustpoint as the primary trustpoint of the router.
- **root** --Defines the TFTP to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

### Specifying Use of Unique Identifiers

When using OCSP as your revocation method, unique identifiers, or nonces, are sent by default during peer communications with the OCSP server. The use of unique identifiers during OCSP server communications enables more secure and reliable communications. However, not all OCSP servers support the use of unique dentures, see your OCSP manual for more information. To disable the use of unique identifiers during OCSP communications, use the **ocsp disable-nonce** subcommand.

## Examples

The following example shows how to declare the CA named ka and specify enrollment and CRL parameters:

```
crypto pki trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based ACL with the label Group defined in a **crypto pki certificate map** command and included in the **match certificate** subcommand of the **crypto pki trustpoint** command:

```
crypto pki certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto pki trustpoint pki1
 match certificate Group
```

The following example shows a self-signed certificate being designated for a trustpoint named local using the enrollment selfsigned subcommand of the crypto pki trustpoint command:

```
crypto pki trustpoint local
 enrollment selfsigned
```

The following example shows the unique identifier being disabled for OCSP communications for a previously created trustpoint named ts:

```
crypto pki trustpoint ts
 ocsp disable-nonce
```

The following example shows the **redundancy** keyword specified in the **crypto pki trustpoint** command:

```
Router(config)#crypto pki trustpoint mytp
Router(ca-trustpoint)#redundancy
Router(ca-trustpoint)#show
 redundancy
 revocation-check crl
end
```

## Related Commands

| Command | Description |
|---|---|
| **crl** | Queries the CRL to ensure that the certificate of the peer has not been revoked. |
| **default (ca-trustpoint)** | Resets the value of a ca-trustpoint configuration subcommand to its default. |
| **enrollment** | Specifies the enrollment parameters of your CA. |
| **enrollment http-proxy** | Accesses the CA by HTTP through the proxy server. |
| **primary** | Assigns a specified trustpoint as the primary trustpoint of the router. |
| **root** | Obtains the CA certificate via TFTP. |

# crypto pki trustpool import

To manually import (download) the certification authority (CA) certificate bundle into the public key infrastructure (PKI) trustpool to update or replace the existing CA bundle, use the **crypto pki trustpool import** command in global configuration mode. To remove any of the configured parameters, use the **no** form of this command.

**crypto pki trustpool import** {**clean** [**terminal** | **url** *url*] | **terminal** | **url** *url*}
**no crypto pki trustpool import** {**clean** [**terminal** | **url** *url*] | **terminal** | **url** *url*}

## Syntax Description

| | |
|---|---|
| **clean** | Specifies the removal of the downloaded PKI trustpool certificates before the new certificates are downloaded. Use the optional **terminal** keyword to remove the existing CA certificate bundle terminal setting or the **url** keyword and *url* argument to remove the URL file system setting. |
| **terminal** | Specifies the importation of a CA certificate bundle through the terminal (cut-and-paste) in Privacy Enhanced Mail (PEM) format. |
| **url** *url* | Specifies the importation of a CA certificate bundle through the URL. |

## Command Default

The PKI trustpool feature is enabled. The router uses the built-in CA certificate bundle in the PKI trustpool, which is updated automatically from Cisco.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

PKI trustpool certificates are automatically updated from Cisco. When the PKI trustpool certificates are not current, use the **crypto pki trustpool import** command to update them from another location.

The *url* argument specifies or changes the URL file system of the CA. The table below lists the available URL file systems.

***Table 34: URL File Systems***

| File System | Description |
|---|---|
| **archive:** | Imports from the archive file system. |

| File System | Description |
|---|---|
| **cns:** | Imports from the Cluster Namespace (CNS) file system. |
| **disk0:** | Imports from the disc0 file system. |
| **disk1:** | Imports from the disc1 file system. |
| **ftp:** | Imports from the FTP file system. |
| **http:** | Imports from the HTTP file system. The URL must be in the following formats:<br>• http://*CAname:80*, where *CAname* is the Domain Name System (DNS)<br>• http://*ipv4-address*:80. For example: http://10.10.10.1:80.<br>• http://*[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL. |
| **https:** | Imports from the HTTPS file system. The URL must use the same formats as the HTTP: file system formats. |
| **null:** | Imports from the null file system. |
| **nvram:** | Imports from NVRAM file system. |
| **pram:** | Imports from Parameter Random-access Memory (PRAM) file system. |
| **rcp:** | Imports from the remote copy protocol (rcp) file system. |
| **scp:** | Imports from the secure copy protocol (scp) file system. |
| **snmp:** | Imports from the Simple Network Management Protocol (SNMP). |
| **system:** | Imports from the system file system. |
| **tar:** | Imports from the UNIX tar file system. |
| **tftp:** | Imports from the TFTP file system.<br>**Note**<br>The URL must be in the form: tftp://*CAname/filespecification*. |
| **tmpsys:** | Imports from the Cisco IOS tmpsys file system. |
| **unix:** | Imports from the UNIX file system. |
| **xmodem:** | Imports from the xmodem simple file transfer protocol system. |
| **ymodem:** | Imports from the ymodem simple file transfer protocol system. |

## Examples

The following example shows how to remove all downloaded PKI trustpool CA certificates and subsequently update the CA certificates in the PKI trustpool by downloading a new CA certification bundle:

```
Router(config)# crypto pki trustpool import clean
Router(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

The following example shows how to update the CA certificates in the PKI trustpool by downloading a new CA certification bundle without removing all downloaded PKI trustpool CA certificates:

```
Router(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

## Related Commands

| Command | Description |
|---|---|
| **cabundle url** | Configures the URL from which the PKI trustpool CA bundle is downloaded. |
| **chain-validation** | Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool. |
| **crl** | Specifes the certificate revocation list (CRL) query and cache options for the PKI trustpool. |
| **crypto pki trustpool policy** | Configures PKI trustpool policy parameters. |
| **default** | Resets the value of a ca-trustpool configuration command to its default. |
| **match** | Enables the use of certificate maps for the PKI trustpool. |
| **ocsp** | Specifies OCSP settings for the PKI trustpool. |
| **revocation-check** | Disables revocation checking when the PKI trustpool policy is being used. |
| **show** | Displays the PKI trustpool policy of the router in ca-trustpool configuration mode. |
| **show crypto pki trustpool** | Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy. |
| **source interface** | Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool. |

| Command | Description |
|---|---|
| **storage** | Specifies a file system location where PKI trustpool certificates are stored on the router. |
| **vrf** | Specifies the VRF instance to be used for CRL retrieval. |

# crypto pki trustpool policy

To configure a public key infrastructure (PKI) trustpool policy parameters, use the **crypto pki trustpool policy** command in global configuration mode.

**crypto pki trustpool policy**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default PKI trustpool policy is used.

## Command Modes

Global configuration mode (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

The **crypto pki trustpool policy** command enters ca-trustpool configuration mode where commands can be accessed to configure certificate authority (CA) PKI trustpool policy parameters.

## Examples

```
Router(config)# crypto pki trustpool policy
```

## Related Commands

| Command | Description |
|---|---|
| **cabundle url** | Configures the URL from which the PKI trustpool CA bundle is downloaded. |
| **chain-validation** | Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool. |
| **crl** | Specifes the CRL query and cache options for the PKI trustpool. |
| **crypto pki trustpool import** | Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle. |
| **default** | Resets the value of a ca-trustpool configuration command to its default. |
| **match** | Enables the use of certificate maps for the PKI trustpool. |

| Command | Description |
|---|---|
| **ocsp** | Specifies OCSP settings for the PKI trustpool. |
| **revocation-check** | Disables revocation checking when the PKI trustpool policy is being used. |
| **show** | Displays the PKI trustpool policy of the router in ca-trustpool configuration mode. |
| **show crypto pki trustpool** | Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy. |
| **source interface** | Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool. |
| **storage** | Specifies a file system location where PKI trustpool certificates are stored on the router. |
| **vrf** | Specifies the VRF instance to be used for CRL retrieval. |

# crypto provisioning petitioner

To configure a device to become an easy secure device provisioning (SDP) petitioner and enter tti-petitioner configuration mode, use the **crypto provisioning petitioner**command in global configuration mode. To disable petitioner support, use the **no** form of this command.

**crypto provisioning petitioner**
**no crypto provisioning petitioner**

## Syntax Description

This command has no arguments or keywords.

## Command Default

A device (with a crypto image) is configured to be an SDP petitioner.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | The **crypto wui tti petitioner**command was introduced. |
| 12.3(14)T | This command replaced the **crypto wui tti petitioner** command. |

## Usage Guidelines

SDP uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer--A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner--A new device that is joined to the secure domain.
- Registrar--A server that authorizes the petitioner. The registrar can be a certificate server.



**Note** Because the petitioner is enabled by default on the device, you only have to issue the **crypto provisioning petitioner** command if you have previously disabled the petitioner or if you want to use an existing trustpoint instead of the automatically generated trustpoint.

## Examples

After the SDP exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration at the petitioner.



**Note** The petitioner will not have any TTI-specific configuration in the beginning except that the IP HTTP server will be turned on and the Domain Name System (DNS) server needs to be properly configured.)

```
crypto pki trustpoint tti
```

```
! Enrollment url contains the registrar CS details
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

## Related Commands

| Command | Description |
|---|---|
| **crypto provisioning registrar** | Configures a device to become an SDP registrar and enters tti-registrar configuration mode. |
| **trustpoint (tti-petitioner)** | Specifies the trustpoint that is to be associated with the TTI exchange between the SDP petitioner and the SDP registrar. |

# crypto provisioning registrar

To configure a device to become an easy secure device provisioning (SDP) registrar and enter tti-registrar configuration mode, use the **crypto provisioning registrar**command in global configuration mode. To disable registrar support, use the **no** form of this command.

**crypto provisioning registrar**
**no crypto provisioning registrar**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The registrar is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | The **crypto wui tti registrar**command was introduced. |
| 12.3(14)T | This command replaced the **crypto wui tti registrar** command. |

## Usage Guidelines

SDP uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer--A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner--A new device that is joined to the secure domain.
- Registrar--A server that authorizes the petitioner.

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

## Examples

The following sample output from the **show running-config**command verifies that the certificate server "cs1" was configured and associated with the TTI exchange between the registrar and petitioner:

```
crypto pki server cs1
 issuer-name CN = ioscs,L = Santa Cruz,C =US
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
!
crypto pki trustpoint cs1
 revocation-check crl
 rsakeypair cs1
```

```
!
!
crypto pki certificate chain pki-36a
 certificate 03
  308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
  86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
  706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
  370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
  191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
  C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
  AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
  4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
  C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
  3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
crypto pki certificate chain cs1
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A02;
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
!
```

```
crypto provisioning registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| crypto provisioning **petitioner** | Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode. |

# crypto skip-client

To configure the Secure Key Integration Protocol (SKIP) client that specifies parameters to securely connect to and import PPKs from an external key source, use the **crypto skip-client** command in global configuration mode. To delete a SKIP client configuration, use the **no** form of this command in the global configuration mode.

**crypto skip-client** *skip-client-name*
**no crypto skip-client** *skip-client-name*

## Syntax Description

| | |
|---|---|
| *skip-client-name* | The name of the SKIP client. |

## Command Default

There is no default SKIP client configuration.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 17.11.1a | This command was introduced. |

## Usage Guidelines

The SKIP client configuration specifies the parameters that are required to securely communicate with and request PPKs from an external SKIP-compliant key source, for quantum-safe encryption.

After you enter the **crypto skip-client** command, the prompt changes to the following:

```
Router(config-crypto-skip-client)#
```

The following **crypto skip-client** submode commands are available:

- **exit** - Exits from crypto ssl policy submode.
- **no** - Negates a command or set its defaults.
- **psk** - Specifies the preshared key for the SKIP TLS session.

  **psk id** *identity* **key** { **0** | **6** | **hex** } *key-value*

  | | |
  |---|---|
  | *identity* | PSK identity. |
  | **0** | An unencrypted password will follow. |
  | **6** | An encrypted password will follow. |
  | **hex** | A hexadecimal string will follow. |
  | *key-value* | Encrypted or unencrypted PSK. |

- **server** - Specifies the SKIP server.

  **server** *identity* **key** { **fqdn** *domain-name* **port** *port-number* | **ipv4** *ipv4-address* **port** *port-number* | **ipv6** *ipv6-address* **port** *port-number* }

| | |
|---|---|
| *domain-name* | Fully Qualified Domain Name (FQDN). |
| *port-number* | Port number. |
| *ipv4-address* | IPv4 address. |
| *ipv6-address* | IPv6 address. |

## Examples

The following example shows how to configure an SKIP client with an IPv4 server address and an unencrypted PSK in plain text:

```
Router(config-crypto-skip-client)#crypto skip-client skip-client-cfg
Router(config-crypto-skip-client)#server ipv4 10.10.0.3 port 9991
Router(config-crypto-skip-client)#psk id psk-id key 0 cisco123
Router(config-crypto-skip-client)#end
```

The following example shows how to configure an SKIP client with an IPv6 server address and an encrypted PSK:

```
Router(config-crypto-skip-client)#crypto skip-client skip-client-cfg
Router(config-crypto-skip-client)#server ipv6 2001::1:1 port 443
Router(config-crypto-skip-client)#psk id psk-id key 6 [XO[J\fAbOhiLUC]^ZRIEQNTefDAAB
Router(config-crypto-skip-client)#end
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 keyring** | Specifies a manual or dynamic PPK in a keyring. |
| **crypto ikev2 profile** | Configures a PPK keyring in an IKEv2 profile. |

# crypto vpn

To install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client package file on a Secure Socket Layer VPN (SSL VPN) gateway for distribution to end users, use the **crypto vpn** command in global configuration mode. To remove a package file from the SSL VPN gateway, use the **no** form of this command.

**crypto vpn** {**anyconnect** *file name* **sequence** *sequence-number* | **profile** *profile-name device* **:** *file name* | **csd** *file name*}
**no crypto vpn** {**anyconnect** *file name* **sequence** *sequence-number* | **profile** *profile-name device* **:** *file name* | **csd** *file name*}

## Syntax Description

| | |
|---|---|
| **anyconnect** *file name* | Installs the specified file from the Cisco AnyConnect VPN Client package. |
| **sequence** *sequence-number* | Allows for multiple packages to be installed on one gateway. If the **sequence** keyword and the *sequence-number* argument are not configured, a sequence number of 1 is applied to the package. |
| **profile** *profile-name device:file name* | Installs the profile of the Cisco AnyConnect VPN Client and the device into which the profile is imported. |
| **csd** | Installs the CSD package. |

## Command Default

Neither a CSD nor a Cisco AnyConnect VPN Client package file is installed on an SSL VPN gateway.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |

## Usage Guidelines

The CSD and Cisco AnyConnect VPN Client installation packages must first be copied to a local file system, such as disk, flash, or USB flash. The CSD and Cisco AnyConnect VPN Client software packages are pushed to end users as access is needed. The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or a later version must be installed before a CSD or Cisco AnyConnect VPN Client package can be installed.

**Note** SSL VPN Client (SVC) is the predecessor of Cisco AnyConnect VPN Client software.

If you have not entered the **sequence** keyword and the *sequence-number* argument and you want to install another package, you can remove the previous package (using the **no** form of the command) or you can provide another sequence number.

If you try to install a package with a sequence number that is being used, you will get an error message.

## Examples

The following example shows how to install the Cisco AnyConnect VPN Client package on an SSL VPN gateway:

```
Device(config)# crypto vpn anyconnect filea sequence 5
```

## Related Commands

| Command | Description |
|---|---|
| **csd enable** | Enables CSD support for SSL VPN sessions. |

# crypto wui tti petitioner

**Note** This command was replaced by the **crypto provisioning petitioner** command effective with Cisco IOS Release 12.3(14)T.

To configure a device to become an easy secure device deployment (EzSDD) petitioner and enter tti-petitioner configuration mode, use the **crypto wui tti petitioner**command in global configuration mode. To disable petitioner support, use the **no** form of this command.

**crypto wui tti petitioner**
**no crypto wui tti petitioner**

## Syntax Description

This command has no arguments or keywords.

## Command Default

A device (with a crypto image) is configured to be an EzSDD petitioner.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

EzSDD uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer--A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner--A new device that is joined to the secure domain.
- Registrar--A server that authorizes the petitioner. The registrar can be a certificate server.

**Note** Because the petitioner is enabled by default on the device, you only have to issue the **crypto wui tti petitioner** command if you have previously disabled the petitioner or if you want to use an existing trustpoint instead of the automatically generated trustpoint.

## Examples

After the EzSDD exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration at the petitioner. (Note that petitioner will not have any TTI-specific configuration in the beginning except that the http server will be turned on and the Domain Name System (DNS) server needs to be properly configured.)

```
crypto pki trustpoint tti
! Enrollment url contains the registrar CS details
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

## Related Commands

| Command | Description |
|---|---|
| **crypto wui tti registrar** | Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode. |
| **trustpoint (tti-petitioner)** | Specifies the trustpoint that is to be associated with the TTI exchange between the EzSDD petitioner and the EzSDD registrar. |

# crypto wui tti registrar



**Note** This command was replaced by the **crypto provisioning registrar** command effective with Cisco IOS Release 12.3(14)T.

To configure a device to become an easy secure device deployment (EzSDD) registrar and enter tti-registrar configuration mode, use the **crypto wui tti registrar**command in global configuration mode. To disable registrar support, use the **no** form of this command.

**crypto wui tti registrar**
**no crypto wui tti registrar**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The registrar is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

EzSDD uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer--A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner--A new device that is joined to the secure domain.
- Registrar--A server that authorizes the petitioner.

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

## Examples

The following sample output from the **show running-config**command verifies that the certificate server "cs1" was configured and associated with the TTI exchange between the registrar and petitioner:

```
crypto pki server cs1
 issuer-name CN = ioscs,L = Santa Cruz,C =US
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
```

```
!
crypto pki trustpoint cs1
 revocation-check crl
 rsakeypair cs1
!
!
crypto pki certificate chain pki-36a
 certificate 03
  308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
  86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
  706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
  370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
  191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
  C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
  AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
  4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
  C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
  3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
crypto pki certificate chain cs1
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A02;
```

```
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
!
crypto wui tti registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki server** | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| **crypto wui tti petitioner** | Configures a device to become an EzSDD petitioner and enters tti-petitioner configuration mode. |

# crypto xauth

To configure crypto Extended Authentication (xauth) parameters globally on a per-interface basis, use the **crypto xauth**command in global configuration mode. To disable the xauth parameters, use the **no** form of this command.

**crypto xauth** *interface-name interface-number*
**no crypto xauth** *interface-name interface-number*

## Syntax Description

| | |
|---|---|
| *interface-name* | Name of the interface. |
| *interface-number* | Number of the related interface. Each interface has a related range of numbers. For example, the asynchronous interface has a range of interface numbers from 1 to 5 and the BVI interface has a range of interface numbers from 1 to 255. |

## Command Default

Crypto xauth parameters are not configured on any interface.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS 15.0(1)M. |

## Usage Guidelines

This command is mainly used on responders.

This command is used to disable the negotiation of xauth capabilities during proposals for a session that is terminating on a specific interface.

The **no crypto xauth** command enables the negotiation of xauth capabilities.

## Examples

The following example shows how to enable crypto xauth parameters globally on a per-interface basis:

```
Router> enable
Router# configure terminal
Router(config)# crypto xauth fastethernet 0/1
```

The following example shows how the **no crypto xauth** command uses the nonvolatile generation (NVGEN) process to perform a configuration state retrieval operation when you specify the **show run**command:

```
Router> enable
Router# configure terminal
Router(config)# no crypto xauth fastethernet 0/1

Router# show run
archive
 log config
  hidekeys
!
```

```
redundancy
!
!
!
no crypto xauth Ethernet0/0
```

## Related Commands

| Command | Description |
|---|---|
| **crypto key decrypt rsa** | Deletes the encrypted RSA key and leaves only the unencrypted key on the running router. |

# csd enable

To enable Cisco Secure Desktop (CSD) support for SSL VPN sessions, use the **csd enable** command in webvpn context configuration mode. To remove CSD support from the SSL VPN context configuration, use the **no** form of this command.

**csd enable**
**no csd enable**

## Syntax Description

This command has no keywords or arguments.

## Command Default

CSD support is not enabled.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The CSD software installation package must be present in a local file system, such as flash memory, and it must be cached for distribution to end users (remote PC or networking device). The **webvpn install**command is used to install the software installation package to the distribution cache.

## Examples

The following example enables CSD support for SSL VPN sessions:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg

SSLVPN Package Cisco-Secure-Desktop : installed successfully
Router(config)# webvpn context context1

Router(config-webvpn-context)# csd enable
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **webvpn install** | Installs a CSD or SSL VPN client package file to a SSL VPN gateway for distribution to end users. |

# ctcp port

To set the port number for Cisco Tunneling Control Protocol (cTCP) encapsulation for Easy VPN, use the **ctcp port** command in crypto ipsec client ezvpn configuration mode. To disable the port that was configured, use the **no** form of this command.

**ctcp port** *port-number*
**no ctcp port**

## Syntax Description

| | |
|---|---|
| *port-number* | Port number. Value = 1 through 65535. |

## Command Default

If a port is not specified, the default port is the port on which the cTCP server listens.

## Command Modes

Crypto ipsec client ezvpn configuration (config-crypto-ezvpn)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

This command is used only on the Easy VPN remote device.

## Examples

The following example shows that the cTCP port number has been set to 10:

```
Router (config)# crypto ipsec client ezvpn client1
Router (config-crypto-ezvpn)# ctcp port 10
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ctcp** | Configures cTCP encapsulation for Easy VPN. |

# ctype

To preauthenticate calls on the basis of the call type, use the **ctype** command in AAA preauthentication configuration mode. To remove the **ctype** command from your configuration, use the **no** form of this command.

**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v . 110** | **v . 120**]
**no ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v . 110** | **v . 120**]

## Syntax Description

| | |
|---|---|
| **if-avail** | (Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes. |
| **required** | (Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails. |
| **accept-stop** | (Optional) Prevents subsequent preauthentication elements such as clid or dnis from being tried once preauthentication has succeeded for a call element. |
| **password** *password* | (Optional) Defines the password for the preauthentication element. |
| **digital** | (Optional) Specifies “digital” as the call type for preauthentication. |
| **speech** | (Optional) Specifies “speech” as the call type for preauthentication. |
| **v.110** | (Optional) Specifies “v.110” as the call type for preauthentication. |
| **v.120** | (Optional) Specifies “v.120” as the call type for preauthentication. |

## Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

## Command Modes

AAA preauthentication configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Set up the RADIUS preauthentication profile with the call type string as the username and with the password that is defined in the **ctype** command as the password. The table below shows the call types that you may use in the preauthentication profile.

***Table 35: Preauthentication Call Types***

| Call Type String | ISDN Bearer Capabilities |
|---|---|
| **digital** | Unrestricted digital, restricted digital. |
| **speech** | Speech, 3.1 kHz audio, 7 kHz audio. |
| **v.110** | Anything with V.110 user information layer. |
| **v.120** | Anything with V.120 user information layer. |

## Examples

The following example specifies that incoming calls be preauthenticated on the basis of the call type:

```
aaa preauth
 group radius
 ctype required
```

## Related Commands

| Command | Description |
|---|---|
| **clid** | Preauthenticates calls on the basis of the CLID number. |
| **dnis (RADIUS)** | Preauthenticates calls on the basis of the DNIS number. |
| **dnis bypass (AAA preauthentication configuration)** | Specifies a group of DNIS numbers that will be bypassed for preauthentication. |
| **group (RADIUS)** | Specifies the AAA RADIUS server group to use for preauthentication. |

# cts authorization list network

To specify a list of AAA servers for the Cisco TrustSec (CTS) seed device to use, use the **cts authorization list network** command in global configuration mode. To stop using the list during authentication, use the **no** form of this command.

**cts authorization list network** *server_list*
**no cts authorization list network** *list-name*

## Syntax Description

| | |
|---|---|
| *list-name* | Specifies a Cisco TrustSec AAA server group. |

## Command Default

No CTS AAA server list is specified.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

A CTS AAA server list is specified in order to establish CTS credentials so that CTS works on your router that is acting as a seed device.

This command is only for the seed device. Non-seed devices obtain the CTS AAA server list from their CTS authenticator peer as a component of their TrustSec environment data. This server list is created by the **aaa authorization network** *list-name* **group radius** command.

## Examples

The following example shows how to specify a list of AAA servers for a CTS seed device:

```
Router# cts credentials id Router password Cisco123

Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network cts-mlist group radius
Router(config)# cts authorization list cts-mlist
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **show cts server-list** | Displays RADIUS server configurations for CTS seed devices. |

# cts credentials

To specify the Cisco TrustSec (CTS) ID and password of the network device, use the **cts credentials** command in privileged EXEC mode. To delete the CTS credentials, use the **clear cts credentials** command.

**cts credentials id** *cts-id* **password** *cts-pwd*

## Syntax Description

| | |
|---|---|
| *cts-id* | The CTS device ID for this device used when authenticating with other CTS devices with EAP-FAST. This argument has a maximum length of 32 characters and is case sensitive. |
| **password** *cts-pwd* | Specifies the password for this device to use when authenticating with other CTS devices with EAP-FAST. |

## Command Default

No CTS credentials are specified.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced on the Catalyst 6500 series switches. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

CTS requires each device in the network to identity itself uniquely. For use in TrustSec Network Device Admission Control (NDAC) authentication, the **cts credentials** command specifies the Cisco TrustSec device ID and password for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The CTS credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the CTS credential information is saved in the keystore, not in the startup-config. The device can be assigned a CTS identity by the Cisco Secure Access Control Server (ACS), or auto-generate a new password when prompted to do so by the ACS. Those credentials are stored in the keystore, eliminating the need to save the running-config. To display the CTS device ID, use the **show cts credentials** command. The stored password is never displayed.

To change the device ID or the password, reenter the command. To clear the keystore, use the **clear cts credentials** command.

**Note** When the CTS device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because the PACs are associated with the old device ID and are not valid for a new identity.

## Examples

The following example configures himalaya and cisco as the CTS device ID and password:

```
Router# cts credentials id himalaya password cisco

CTS device ID and password have been inserted in the local keystore. Please make sure that
 the same ID and password are configured in the server database.
```

The following example changes the CTS device ID and password to atlas and cisco123:

```
Router# cts credentials id atlas password cisco123

A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y
TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following example displays the CTS device ID and password state:

```
Router# show cts credentials

CTS password is defined in keystore, device-id = atlas
```

## Related Commands

| Command | Description |
|---|---|
| **clear cts credentials** | Clears the CTS device ID and password. |
| **show cts credentials** | Displays the state of the current CTS device ID and password. |
| **show cts keystore** | Displays contents of the hardware and software keystores. |

# cts dot1x

Use the **cts dot1x** command in interface configuration mode to enable Network Device Admission Control (NDAC) and configure NDAC authentication parameters. Use the **no** form of the command to disable NDAC authentication on the interface.

**cts dot1x**
**no cts dot1x**

## Syntax Description

This command has no arguments or keywords.

## Command Default

CTS dot1x configuration on the interface is disabled by default.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

Once the **cts dot1x** command is specified, CTS dot1x interface configuration mode (config-if-cts-dot1x) is entered where Cisco TrustSec NDAC parameters can be configured. Cisco TrustSec NDAC is enabled when the interface is enabled. Cisco TrustSec NDAC must be enabled with 802.1X on each uplink interface that connects to another Cisco TrustSec device.

## Examples

```
Device# configure terminal
Device(config)# interface gigabitethernet 3/1
Device(config-if)# cts dot1x
Device(config-if-cts-dot1x)# sap mode-list gcm null no-encap
Device(config-if-cts-dot1x)# timer reauthentication 43200
Device(config-if-cts-dot1x)# exit
Device(config-if)# no shutdown
Device(config-if)# end
Device#
```

## Related Commands

| Command | Description |
|---|---|
| **propagate sgt (config-if-cts-dot1x)** | Enables Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface. |
| **sap mode-list (config-if-cts-dot1x)** | Configures CTS Security Association Protocol (SAP) authentication. |
| **show cts interface** | Displays CTS interface status and configurations. |
| **show dot1x interface** | Displays IEEE 802.1x configurations and statistics. |
| **timer reauthentication (config-if-cts-dot1x)** | Configures the reauthentication timer for a CTS device. |

# cts manual

To manually enable an interface for Cisco TrustSec Security (CTS), use the **cts manual** command in interface configuration mode.

**cts manual**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 4.1(2) | This command was introduced on the Cisco Nexus 7000 series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

When the **cts manual** command is entered, CTS is enabled on the interface and CTS manual interface configuration mode is entered where CTS parameters can be configured.

All CTS configuration commands with VRF parameters require that the named VRF exists. If the VRF is removed, then the associated CTS configuration is also removed.

## Examples

The following example shows how to enter CTS manual interface configuration mode on an interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# cts manual
Router(config-if-cts-manual))#
```

The following example shows how to remove the CTS manual configuration from an interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# no cts manual
```

## Related Commands

| Command | Description |
|---|---|
| **propagate sgt** | Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces. |
| **show cts interface** | Displays information about CTS interfaces. |

# cts role-based enforcement

To enable role-based access control globally and on specific Layer 3 interfaces using Cisco TrustSec, use the **cts role-based enoforcement** command in global configuration mode and interface configuration mode respectively. To disable the enforcement of role-based access control at an interface level, use the **no** form of this command.

**cts role-based enforcement**
**no cts role-based enforcement**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Enforcement of role-based access control at an interface level is disabled globally.

## Command Modes

Global configuration (config)

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)SY | This command was introduced. |

## Usage Guidelines

The **cts role-based enforcement** command in global configuration mode enables role-based access control globally. Once role-based access control is enabled globally, it is automatically enabled on every Layer 3 interface on the device. To disable role-based access control on specific Layer 3 interfaces, use the **no** form of the command in interface configuration mode. The **cts role-based enforcement** command in interface configuration mode enables enforcement of role-based access control on specific Layer 3 interfaces.

The attribute-based access control list organizes and manages the Cisco TrustSec access control on a network device. The security group access control list (SGACL) is a Layer 3-4 access control list to filter access based on the value of the security group tag (SGT). The filtering usually occurs at an egress port of the Cisco TrustSec domain. The terms role-based access control list (RBACL) and SGACL can be used interchangeably, and they refer to a topology-independent ACL used in an attribute-based access control (ABAC) policy model.

The following example shows how to enable role-based access control on a Gigabit Ethernet interface:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

# cts role-based sgt-cache

To enable Security Group Tag (SGT) caching on an interface, use the **cts role-based sgt-cache** command in interface configuration mode. To disable SGT caching on an interface, use the **no** form of this command.

**cts role-based sgt-cache** {**egress** | **ingress**}

**no cts role-based sgt-cache** {**egress** | **ingress**}

## Syntax Description

| | |
|---|---|
| **egress** | Enables SGT caching at the egress point of an interface. |
| **ingress** | Enables SGT caching at the ingress point of an interface. |

## Command Default

SGT caching is enabled on the interface.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS 15.5(2)T | This command was introduced. |
| Cisco IOS XE Release 3.15S | This command was integrated into Cisco IOS XE Release 3.15S. |

## Usage Guidelines

The global SGT caching configuration and the interface-specific ingress configuration are mutually exclusive. If an interface has ingress SGT caching enabled using the **cts role-based sgt-cache ingress** command in interface configuration mode, and a global configuration is attempted using the **cts role-based sgt-caching** command, the following message is displayed:

```
There is at least one interface that has ingress sgt caching configured. Please remove all
 interface ingress sgt caching configuration(s) before attempting global enable.
```

When an interface is configured to be on a Virtual Routing and Forwarding (VRF) network, the IP-SGT bindings identified on that interface are added under the specific VRF.

### Example

The following example shows how to configure SGT caching on an interface:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# end
```

The following example shows how to disable SGT caching on an interface when SGT caching is enabled globally:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet 0/1/0
Device(config-if)# no cts role-based sgt-cache ingress
Device(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **cts role-based sgt-caching** | Enables SGT caching in ingress direction for all interfaces. |
| **interface** | Specifies the interface for network traffic. |
| **show cts role-based sgt-map all** | Displays the IP-SGT binding table. |

# cts role-based sgt-caching

To enable Security Group Tag (SGT) caching in ingress direction for all interfaces, use the **cts role-based sgt-caching** command in global configuration mode. To disable SGT caching, use the **no** form of this command.

**cts role-based sgt-caching**

**no cts role-based sgt-caching**

## Syntax Description

This command has no arguments or keywords.

## Command Default

SGT caching is enabled globally.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS 15.5(2)T | This command was introduced. |
| Cisco IOS XE Release 3.15S | This command was integrated into Cisco IOS XE Release 3.15S. |

## Usage Guidelines

Cisco TrustSec uses SGT caching to ensure that the network traffic tagged with SGT can pass through services that cannot propagate SGTs.

SGT caching can be enabled globally or on an interface. The global SGT caching configuration and the interface-specific ingress configuration are mutually exclusive. If global configuration is enabled using the **cts role-based sgt-caching** command, and an interface configuration is attempted using the **cts role-based sgt-cache ingress** command in interface configuration mode, the following message is displayed:

```
Note that ingress sgt caching is already active on this interface due to global sgt-caching
 enable.
```

### Example

The following example shows how to configure SGT caching globally:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **cts role-based sgt-cache** | Enables SGT caching on an interface. |
| **show cts role-based sgt-map all** | Displays the IP-SGT binding table. |

# cts role-based sgt-map (config)

To assign an Security Group Tag (SGT) value to hosts of an IPv4 or IPv6 network, a VLAN instance, or a VRF instance, use the **cts role-based sgt-map** command in global configuration mode. To remove the SGT value, use the **no** form of this command.

**cts role-based sgt-map** {[**vrf** *vrf-name*] {*ipv4-address ipv4-address/prefix ipv6-address ipv6-address/prefix* | **host** {*ipv4-address ipv6-address*}} | **vlan-list** {*vlan-id* | **all**}} **sgt** *sgt-value*

**no cts role-based sgt-map** {[**vrf** *vrf-name*] {*ipv4-address ipv4-address/prefix ipv6-address ipv6-address/prefix* | **host** {*ipv4-address ipv6-address*}} | **vlan-list** {*vlan-id* | **all**}} **sgt** *sgt-value*

## Syntax Description

| | |
|---|---|
| **vrf** *vrf-name* | Specifies a VRF instance. |
| *ipv4-address* | The IPv4 address for a single host. |
| *ipv4-address/prefix* | The IPv4 address for all hosts within the specified subnet. |
| *ipv6-address* | The IPv6 address for a single host. |
| *ipv6-address/prefix* | The IPv6 address for all hosts within the specified subnet. |
| **host** {*ipv4-address* \| *ipv6-address*} | Specifies the IPv4 or IPv6 address for the host IP-SGT binding. |
| **vlan-list** *vlan-id* | Specifies a VLAN ID. The VLAN ID values range from 1 to 4094. Individual VLAN IDs are separated by commas, a range of IDs is specified with a hyphen. |
| **all** | Specifies all VLAN instances. |
| **sgt** *sgt-value* | Specifies the SGT. The SGT values range from 2 to 65519. |

## Command Default

SGT value is not assigned.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(2)SE | This command was introduced. |
| 15.2(2)E | This command was modified. The *ipv6-address* and *ipv6-address/prefix* arguments were added. |

## Usage Guidelines

If you do not have a Cisco Identity Services Engine (ISE), Cisco Secure ACS, dynamic ARP inspection, DHCP snooping, or Host Tracking available to your device to automatically map SGTs to source IP addresses, you can manually map an SGT to the following with the **cts role-based sgt-map** command:

- A single host IPv4 or IPv6 address
- All hosts of an IPv4 or IPv6 network or subnetwork
- VRFs
- Single or multiple VLANs

The **cts role-based sgt-map host** command binds the specified SGT with incoming packets when the IP source address is matched by the specified host address. This IP-SGT binding has the lowest priority and is ignored in the presence of any other dynamically discovered bindings from other sources (such as, SXP or locally authenticated hosts).

The **cts role-based sgt-map** *ipv4-address ipv4-address/prefix* and **cts role-based sgt-map** *ipv6-address ipv6-address/prefix* commands bind the specified SGT with packets that fall within the specified network address.

SXP exports an exhaustive expansion of all possible individual IP-SGT bindings within the specified network or subnetwork. IPv6 bindings and subnet bindings are exported only to SXP listener peers of SXP version 2 or later.

The **vrf** keyword specifies a Virtual Routing and Forwarding table previously defined with the **vrf definition** global configuration command. The configuration of VRF contexts is outside the scope of this document. The IP-SGT binding specified with the **cts role-based sgt-map vrf** global configuration command command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version which is implied by the type of IP address entered.

The **cts role-based** sgt-map vlan-list command binds an SGT with a specified VLAN or a set of VLANs. The keyword **all** is equivalent to the full range of VLANs supported by the device and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs.

### Example

The following example shows how to assign an SGT value of 5 to an IPv6 address:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map sgt-map 2001:DB8:: sgt 5
Device(config)# end
```

The following example shows how to assign an SGT value of 5 to an IP address that falls within an IPv4 network of 10.0.0.0/8:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map sgt-map 10.0.0.0/8 sgt 5
Device(config)# end
```

The following example shows how to assign an SGT value of 5 to a VRF instance:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf vrfname 10.2.2.3 sgt 5
Device(config)# end
```

The following example shows how to assign an SGT value of 5 to a VLAN:

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vlan-list 2 sgt 5
Device(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show cts role-based sgt-map** | Displays the IP-SGT binding table. |

# cts role-based sgt-map interface

To manually map a source IP address to a Security Group Tag (SGT) on either a host or a VRF, use the **cts role-based sgt-map interface** command in global configuration mode. Use the **no** form of the command to remove the mapping.

**cts role-based sgt-map** *interface-type slot/port* {**security-group** | **sgt**} *sgt-number*
**no cts role-based sgt-map interface** *interface-type slot/port* {**security-group** | **sgt**} *sgt-number*

## Syntax Description

| | |
|---|---|
| *interface-type* | Specifies the type of interface. For example, ethernet. The specified SGT is mapped to traffic from this logical or physical Layer 3 interface. |
| *slot/port* | Specifies the interface slot and port number. |
| **sgt** *sgt-number* | Specifies the SGT number from 0-65535. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(0)SY | This command was introduced on the Catalyst 6500 series switches. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)Y. |
| 15.3(2)T | This command was integrated into Cisco IOS Release 15.3(2)T. |

## Usage Guidelines

The **cts role-based sgt-map interface** command binds a specified Layer 3 logical interface to a security group name or to an SGT. A security group information table that maps SGTs to security group names is downloaded from the authentication server with the TrustSec environment data. The **cts role-based sgt-map interface security-group** command is rejected if a security group name table is not available.

Whenever a security group table is downloaded for the first time or refreshed, all L3IF mappings are reprocessed. IP-SGT bindings are added, updated, or deleted for all network prefixes that have output paths through the specified interface.

**Note** The **interface** keyword is not supported on the Cisco ASR 1000 series routers.

When configuring this command on a Cisco ASR 1000 series router, use the following syntax: **cts role-based sgt-map** {*ipv4-address* | *ipv6-address* | *host-ip-address* | *vrf*} {**security-group** | **sgt**} *sgt-number*.

## Examples

The following example shows how to manually map a source IP address to an SGT on a Catalyst 6500 series switch:

```
Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77
```

The following example shows how to manually map a source IP address to an SGT on a Cisco ASR 1000 series router:

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

**Related Commands**

| Command | Description |
|---|---|
| **cts sxp** | Configures SXP on a network device. |
| **cts sgt** | Configures local device security group tag. |
| **show cts role-based sgt-map** | Displays role-based access control information. |

# cts role-based sgt-map sgt

To bind all traffic on a Layer 3 ingress interface to a security group tag (SGT), use the **cts role-based sgt-map sgt** command in interface configuration mode. To remove the mapping, use the **no** form of this command.

**cts role-based sgt-map sgt** *sgt-number*
**no cts role-based sgt-map sgt** *sgt-number*

## Syntax Description

| | |
|---|---|
| *sgt-number* | SGT number from 2 to 65519. |

## Command Default

The traffic on a Layer 3 interface is not mapped to an SGT.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.4(2)T | This command was introduced on Cisco Integrated Services Router Generation 2 (Cisco ISR G2). |
| Cisco IOS XE Release 3.12S | This command was implemented on the Cisco ASR 1000 Series Routers. |

## Usage Guidelines

The **cts role-based sgt-map sgt** command binds a logical Layer 3 ingress interface to an SGT. Once the mapping is implemented, Cisco TrustSec uses the SGT to segregate traffic from various Layer 3 ingress interfaces.

The SGT is assigned to all traffic on the Layer 3 ingress interface and can be used for inline tagging and policy enforcement.

## Examples

The following example shows how to map a Layer 3 ingress interface to an SGT:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# cts role-based sgt-map sgt 77
Device(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show cts role-based sgt-map** | Displays the IP-SGT binding table. |

# cts sxp connection peer

Use the **cts sxp connection peer** command in global configuration mode to specify

- the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) peer IP address
- if a password is used for the peer connection or a TCP key-chain should be used to provide TCP-AO authentication
- the global hold-time period for a listener or speaker device
- if the connection is bidirectional.

To remove these configurations for a peer connection, use the **no** form of this command.

**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **key-chain** | **none**} **mode** {**local** | **peer**} { {**listener** | **speaker**} [**hold-time** *minimum-time maximum-time*] [**vrf** *vrf-name*] | **both** [**vrf** *vrf-name*]}

**no cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **key-chain** | **none**} **mode** {**local** | **peer**} { {**listener** | **speaker**} [**hold-time** *minimum-time maximum-time*] [**vrf** *vrf-name*] | **both** [**vrf** *vrf-name*]}

## Syntax Description

| | |
|---|---|
| *ipv4-address* | SXP peer IPv4 address. |
| **source** | Specifies the source IPv4 address. |
| **password** | Specifies that an SXP password is used for the peer connection. |
| **default** | Specifies that the default SXP password is used. |
| **key-chain** | Specifies that the TCP-AO key-chain should be used to authenticate TCP segments. |
| **none** | Specifies no password is used. |
| **mode** | Specifies either the local or peer SXP connection mode. |
| **local** | Specifies that the SXP connection mode refers to the local device. |
| **peer** | Specifies that the SXP connection mode refers to the peer device. |
| **listener** | (Optional) Specifies that the device is the listener in the connection. |
| **speaker** | (Optional) Specifies that the device is the speaker in the connection. |

| | |
|---|---|
| **hold-time** *minimum-time maximum-time* | (Optional) Specifies the hold-time period, in seconds, for the device. The range for minimum and maximum time is from 0 to 65535.<br>A *maximum-time* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a *minimum-time* value is required.<br>**Note**<br>If both minimum and maximum times are required, the *maximum-time* value must be greater than or equal to the *minimum-time* value. |
| **vrf** *vrf-name* | (Optional) Specifies the virtual routing and forwarding (VRF) instance name to the peer. |
| **both** | (Optional) Specifies that the device is both the speaker and the listener in the bidirectional SXP connection. |

## Command Default

The CTS-SXP peer IP address is not configured and no CTS-SXP peer password is used for the peer connection.

The default setting for a CTS-SXP connection password is **none**.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |
| 15.3(2)T | This command was modified. The **hold-time** keyword and *minimum-time* and *maximum-time* arguments were added. |
| Cisco IOS XE Release 3.11S | This command was modified. The **both** keyword was added. |
| 15.4(1)T | This command was modified. The **both** keyword was added. |
| 16.12.1 | This command was modified. The **key-chain** keyword was added. |

## Usage Guidelines

When a CTS-SXP connection to a peer is configured with the **cts sxp connection peer** command, only the connection mode can be changed. The **vrf** keyword is optional. If a VRF name is not provided or a VRF name is provided with the **default** keyword, then the connection is set up in the default routing or forwarding domain.

A **hold-time** *maximum-period* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time** *minimum-period* value is required.

**Note** The *maximum-period* value must be greater than or equal to the *minimum-period* value.

Use the **both** keyword to configure a bidirectional SXP connection. With the support for bidirectional SXP configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

Use the **key-chain** keyword to specify that TCP-AO should be used to authenticate the TCP segments exchanged by the SXP peers. You must define the default key-chain to use for TCP-AO using **cts sxp default key-chain**.

## Examples

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener with the password option for TCP MD5 authentication: :

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

You can also configure both peer and source IP addresses for an SXP connection. The source IP address specified in the **cts sxp connection** command overwrites the default value.

The following example shows how to configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener without a password or key chain option:

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none mode
local speaker
```

```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none mode
local listener
```

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device_A to connect to Device_B:

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

The following example shows how to enable CTS-SXP and configure a CTS-SXP peer connection with TCP-AO authentication on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default key-chain sxp_1
Device_A#(config)# cts sxp connection peer 2.2.2.2 password key-chain mode local speaker
hold-time 0
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp default password** | Configures the Cisco TrustSec SXP default password. |
| **cts sxp default key-chain** | Configures the default key-chain to use for TCP-AO authentication. |
| **cts sxp default source-ip** | Configures the Cisco TrustSec SXP source IPv4 address. |
| **cts sxp enable** | Enables Cisco TrustSec SXP on a device. |
| **cts sxp log** | Enables logging for IP-to-SGT binding changes. |
| **cts sxp reconciliation** | Changes the Cisco TrustSec SXP reconciliation period. |
| **cts sxp retry** | Changes the Cisco TrustSec SXP retry period timer. |
| **cts sxp speaker hold-time** | Configures the global hold-time period of a speaker device in a Cisco TrustSec SGT SXPv4 network. |
| **cts sxp listener hold-time** | Configures the global hold-time period of a listener device in a Cisco TrustSec SGT SXPv4 network. |
| **show cts sxp** | Displays the status of all Cisco TrustSec SXP configurations. |

# cts sxp default key-chain

To specify the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) default key-chain for TCP-AO, use the **cts sxp default key-chain** command in global configuration mode. To remove the CTS-SXP default key-chain, use the **no** form of this command.

**cts sxp default key-chain** *key-chain-name*
**no cts sxp default key-chain** *key-chain-name*

## Syntax Description

| | |
|---|---|
| *key-chain-name* | Name of the TCP key-chain that must be used by default to provide TCP-AO authentication for CTS SXP sessions. |

## Command Default

A default key chain is not configured for CTS SXP.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 16.12.1 | Command introduced |

## Usage Guidelines

Use this command to specify the key-chain that must be used by default to provide TCP-AO authentication for CTS SXP sessions.

Define the key-chain using the **key chain** *key-chain-name* **tcp** command.

### Example

In the following example, a TCP-AO key chain named sxp_1 is configured as the default key chain for CTS SXP sessions using TCP-AO.

```
Device> enable
Device# configure terminal
Device(config)# cts sxp default key-chain sxp_1
```

## Related Commands

| Command | Description |
|---|---|
| **key chain** *key-chain-name* **tcp** | Use this command to define a key-chain for TCP-AO. |

# cts sxp default password

To specify the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) default password, use the **cts sxp default password** command in global configuration mode. To remove the CTS-SXP default password, use the **no** form of this command.

**cts sxp default password** {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}
**no cts sxp default password** {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}

## Syntax Description

| | |
|---|---|
| **0** *unencrypted-pwd* | Specifies that an unencrypted CTS-SXP default password follows. The maximum password length is 32 characters. |
| **6** *encrypted-key* | Specifies that a 6 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters. |
| **7** *encrypted-key* | Specifies that a 7 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters. |
| *cleartext-pwd* | Specifies a cleartext CTS-SXP default password. The maximum password length is 32 characters. |

## Command Default

Type **0** (cleartext)

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

The **cts sxp default password** command sets the CTS-SXP default password to be optionally used for all CTS-SXP connections configured on the device. The CTS-SXP password can be cleartext, or encrypted with the **0**, **7**, **6** encryption type keywords. If the encryption type is 0, then an unencrypted cleartext password follows.

## Examples

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Router_A, a speaker, for connection to Router_B, a listener:

```
Router_A# configure terminal
Router_A#(config)# cts sxp enable
```

```
Router_A#(config)# cts sxp default password Cisco123
Router_A#(config)# cts sxp default source-ip 10.10.1.1
Router_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Router_B, a listener, for connection to Router_A, a speaker:

```
Router_B# configure terminal
Router_B(config)# cts sxp enable
Router_B(config)# cts sxp default password Cisco123
Router_B(config)# cts sxp default source-ip 10.20.2.2
Router_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp connection peer** | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| **cts sxp default source-ip** | Configures the CTS-SXP source IPv4 address. |
| **cts sxp enable** | Enables CTS-SXP on a device. |
| **cts sxp log** | Enables logging for IP-to-SGT binding changes. |
| **cts sxp reconciliation** | Changes the CTS-SXP reconciliation period. |
| **cts sxp retry** | Changes the CTS-SXP retry period timer. |
| **show cts sxp** | Displays the status of all SXP configurations. |

# cts sxp default source-ip

To configure the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) source IPv4 address, use the **cts sxp default source-ip** command in global configuration mode. To remove the CTS-SXP default source IP address, use the **no** form of this command.

**cts sxp default source-ip** *ipv4-address*
**no cts sxp default source-ip** *ipv4-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | Default source CTS-SXP IPv4 address. |

## Command Default

The CTS-SXP source IP address is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

The **cts sxp default source-ip** command sets the default source IP address that CTS-SXP uses for all new TCP connections where a source IP address is not specified. Preexisting TCP connections are not affected when this command is entered. CTS-SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

## Examples

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Router_A, a speaker, for connection to Router_B, a listener:

```
Router_A# configure terminal
Router_A#(config)# cts sxp enable
Router_A#(config)# cts sxp default password Cisco123
Router_A#(config)# cts sxp default source-ip 10.10.1.1
Router_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Router_B, a listener, for connection to Router_A, a speaker:

```
Router_B# configure terminal
Router_B(config)# cts sxp enable
Router_B(config)# cts sxp default password Cisco123
Router_B(config)# cts sxp default source-ip 10.20.2.2
Router_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp connectionpeer** | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| **cts sxp default password** | Configures the CTS-SXP default password. |
| **cts sxp enable** | Enables CTS-SXP on a device. |
| **cts sxp log** | Enables logging for IP-to-SGT binding changes. |
| **cts sxp reconciliation** | Changes the CTS-SXP reconciliation period. |
| **cts sxp retry** | Changes the CTS-SXP retry period timer. |
| **show cts sxp** | Displays the status of all SXP configurations. |

# cts sxp enable

To enable the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) on a device, use the **cts sxp enable** command in global configuration mode. To disable the CTS-SXP on a device, use the **no** form of this command.

**cts sxp enable**
**no cts sxp enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

The **cts sxp enable** command enables CTS-SXP over a TCP (SXP) connection. CTS-SXP propagates IP-to-SGT binding information across network devices that do not have the capability to tag packets, which allows security services on switches, routers or firewalls to learn identity information from devices that access the network.

## Examples

The following example shows how to enable CTS-SXP and configure the SXP peer connection on Router_A, a speaker, for connection to Router_B, a listener:

```
Router_A# configure terminal
Router_A#(config)# cts sxp enable
Router_A#(config)# cts sxp default password Cisco123
Router_A#(config)# cts sxp default source-ip 10.10.1.1
Router_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Router_B, a listener, for connection to Router_A, a speaker:

```
Router_B# configure terminal
Router_B(config)# cts sxp enable
Router_B(config)# cts sxp default password Cisco123
Router_B(config)# cts sxp default source-ip 10.20.2.2
Router_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp sxp connectionpeer** | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| **cts sxp default password** | Configures the CTS-SXP default password. |
| **cts sxp default source-ip** | Configures the CTS-SXP source IPv4 address. |
| **cts sxp log** | Enables logging for IP-to-SGT binding changes. |
| **cts sxp reconciliation** | Changes the CTS-SXP reconciliation period. |
| **show cts sxp** | Displays the status of all CTS-SXP configurations. |
| **cts sxp retry** | Changes the CTS-SXP retry period timer. |

# cts sxp filter-enable

To enable filtering after creating filter lists and filter groups, use the **cts sxp filter-enable** command in global configuration mode. To disable filtering, use the **no** form of the command.

**cts sxp filter-enable**
**no cts sxp filter-enable**

## Syntax Description

| |
|---|
| This command has no keywords or arguments. |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 16.6.1 | This command was introduced. |

## Usage Guidelines

This command can be used at any time to enable or disable filtering. Configured filter lists and filter groups can be used to implement filtering only after filtering is enabled. The filter action will only filter bindings that are exchanged after filtering is enabled; there won't be any effect on the bindings that were exchanged before filtering was enabled.

## Examples

```
Device(config)# cts sxp filter-enable
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp filter-list** | Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both. |
| **cts sxp filter-group** | Creates a filter group for grouping a set of peers and applying a filter list to them. |
| **show cts sxp filter-group** | Displays information about the configured filter groups.. |
| **show cts sxp filter-list** | Displays information about the configured filter lists. |
| **debug cts sxp filter events** | Logs events related to the creation, deletion and update of filter-lists and filter-groups |

# cts sxp filter-group

To create a filter group for grouping a set of peers and applying a filter list to them, use the **cts sxp filter-group** command in global configuration mode. To delete a filter group, use the **no** form of this command.

**cts sxp filter-group** {**listener** | **speaker**} [**global**] {*filter-group-name*}
**no cts sxp filter-group** {**listener** | **speaker**} [**global**] {*filter-group-name*}

## Syntax Description

| | |
|---|---|
| **listener** | Creates a filter group for a set of listeners. |
| **speaker** | Creates a filter group for a set of speakers. |
| **global** | Groups all speakers or listeners on the device. |
| *filter-group-name* | Name of the filter group. |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 16.6.1 | This command was introduced. |

## Usage Guidelines

Issuing this command, places the device in the filter group configuration mode. From this mode, you can specify the devices to be grouped and apply a filter list to the filter group.

The command format to add devices or peers to the group is a follows:

**peer ipv4** *peer-IP*

In a single command, you can add one peer. To add more peers, repeat the command as many times as required.

The command format to apply a filter list to the group is as follows:

**filter** *filter-list-name*

You cannot specify a peer list for the global listener and global speaker filter-group options because in this case the filter is applied to all SXP connections

When both the global filter group and peer-based filter groups are applied, the global filter takes priority. If only a global listener or global speaker filter group is configured, then the global filtering takes precendence only in that specific direction. For the other direction, the peer-based filter group is implemented.

## Examples

The following example shows how to create a listener group called **group_1**, and assign peers and a filter list to this group:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

The following example shows how to create a global listener group called **group_2**

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp filter-list** | Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both. |
| **cts sxp filter-enable** | Enables filtering. |
| **show cts sxp filter-group** | Displays information about the configured filter groups. |
| **show cts sxp filter-list** | Displays information about the configured filter lists. |
| **debug cts sxp filter events** | Logs events related to the creation, deletion and update of filter-lists and filter-groups |

# cts sxp filter-list

To create a SXP filter list to hold a set of filter rules for filtering IP-SGT bindings, use the **cts sxp filter-list** command in global configuration mode. To delete a filter list, use the **no** form of the command.

**cts sxp filter-list** *filter-list-name*
**no cts sxp filter-list** *filter-list-name*

## Syntax Description

| | |
|---|---|
| *filter-list-name* | Name of the filter-list. |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 16.6.1 | This command was introduced. |

## Usage Guidelines

Issuing this command, places the device in the filter list configuration mode. From this mode, you can specify rules for the filter lists.

A filter rule can be based on SGT or IP Prefixes or a combination of both SGT and IP Prefixes.

The command format to add rules to the group is a follows:

*sequence-number* **action(permit/deny) filter-type(ipv4/ipv6/sgt)** *value/values*

For example, to permit SGT-IP bindings whose SGT value is 20, the rule is as follows:

```
30 permit sgt 20
```

Note that the sequence number is optional. If you do not specify a sequence number, it is generated by the system. Sequence numbers are automatically incremented by a value of 10 from the last used/configured sequence number. A new rule can be inserted by specifying a sequence number in between two existing rules.

The range of valid SGT values is between 2 and 65519. To provide multiple SGT values in a rule, seperate the values using a space. A maximum of 8 SGT values are allowed in a rule.

In a SGT and IP prefix combination rule, if there is a match for the binding in both the parts of the rule, then the action specified in the second part of the rule takes precedence. For example, in the following rule, if the SGT value of the IP prefix 10.0.0.1 is 20, the corresponding binding will be denied even if the first part of the rule permits the binding.

```
Router(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

Similarly, in the rule below the binding with the sgt value 20 will be permitted even if the sgt of the IP prefix 10.0.0.1 is 20, and the first action does not permit the binding.

```
Router(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

## Examples

The following example shows how to create a filter list and add some rules to the list:

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp filter-enable** | Enable SXP IP-prefix and SGT-based filtering. |
| **cts sxp filter-group** | Creates a filter group for grouping a set of peers and applying a filter list to them. |
| **show cts sxp filter-group** | Displays information about the configured filter groups. |
| **show cts sxp filter-list** | Displays information about the configured filter lists. |
| **debug cts sxp filter events** | Logs events related to the creation, deletion and update of filter-lists and filter-groups. |

# cts sxp listener hold-time

To configure the global hold-time period of a listener network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp listener hold-time** command in global configuration mode. To remove the hold time from the listener device, use the **no** form of this command.

**cts sxp listener hold-time** *minimum-period maximum-period*
**no cts sxp listener hold-time**

## Syntax Description

| | |
|---|---|
| *minimum-period* | Minimum allowed hold time in seconds. The range is from 1 to 65534. |
| *maximum-period* | Specifies the maximum allowed hold-time in seconds. The range is from 1 to 65534 seconds.<br>**Note**<br>The *maximum-period* specified must be greater than or equal to the *minimum-period*. |

## Command Default

The default hold time range for a listener device is 90 seconds to 180 seconds.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.3(2)T | This command was introduced. |
| Cisco IOS Release 3.9S | This command was modified. Support was added for the Cisco ASR 1000 Series Routers. |

## Usage Guidelines

SXP uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism, the hold-time period, in order to provide more predictable and timely detection of connection loss.

Hold time can be configured globally on a network device. This global configuration will apply the configuration to all SXP connections configured on the device.

You may configure a hold-time period locally on a listener device or a default of 90 seconds to 180 seconds is used. A value of “0xFFFF..0xFFFF” indicates that the keepalive mechanism is not used.

The hold-time negotiation between the speaker device and the listener device succeeds when the speaker’s minimum acceptable hold-time falls below or within the desirable hold-time range of the listener. (Use the **cts sxp speaker hold-time** command to configure the hold-time of the speaker device.) If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.

The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.

The selected hold-time period of a successful negotiation is the maximum of the speaker’s minimum acceptable hold-time and the lower bound of the listener’s hold-time range.

The speaker calculates the keepalive time to one-third of the selected hold time by default, unless a different keepalive time is locally configured.

The following example shows how to configure the hold time period of a listener device for a minimum of 300 seconds and a maximum of 500 seconds:

```
Device> enable
Device# configure terminal
Device(config)# cts sxp listener hold-time 300 500
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp enable** | Enables Cisco TrustSec SXP on a device. |
| **cts sxp speaker hold-time** | Configures the hold time of a speaker device in an SXPv4 network. |
| **show cts sxp** | Displays the status of all Cisco TrustSec SXP configurations. |

# cts sxp log binding-changes

To enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes, use the **cts sxp log binding-changes** command in global configuration mode. To disable logging, use the **no** form of this command.

**cts sxp log binding-changes**
**no cts sxp log binding-changes**

## Command Default

Logging disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

The **cts sxp log binding-changes** command enables logging for IP-to-SGT binding changes. SXP syslogs (sev 5 syslogs) are generated whenever IP address-to-SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection.

## Related Commands

| Command | Description |
|---|---|
| **cts sxp connectionpeer** | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection |
| **cts sxp default password** | Configures the CTS-SXP default password. |
| **cts sxp default source-ip** | Configures the CTS-SXP source IPv4 address. |
| **cts sxp enable** | Enables CTS-SXP on a device. |
| **cts sxp reconciliation** | Changes the CTS-SXP reconciliation period. |
| **cts sxp retry** | Changes the CTS-SXP retry period timer. |
| **show cts sxp** | Displays status of all SXP configurations. |

# cts sxp mapping network-map

To configure the subnet to Security Group Tag (SGT) mapping host count constraint to limit the number of subnet bindings SXPv3 can export, use the **cts sxp mapping network-map** command in global configuration mode. To return to the default, use the **no** form of this command.

**cts sxp mapping network-map** *bindings*

## Syntax Description

| | |
|---|---|
| *bindings* | Specifies the maximum number of subnet IP hosts from 0 to 65,535 that can be bound to SGTs and exported to the SXP listener. |

## Command Default

The default is 0 (no expansions performed).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

In IPv4 networks, SXPv3, and more recent versions, can receive and parse subnet network address/prefix strings from SXPv3 peers. Earlier SXP versions convert the subnet prefix into its set of host bindings before exporting them to an SXP listener peer.

For example, the IPv4 subnet 198.1.1.0/29 is expanded as follows (only 3 bits for host addresses):

- Host addresses 198.1.1.1 to 198.1.1.7 are tagged and propagated to SXP peer.
- Network and broadcast addresses 198.1.1.0 and 198.1.1.8 are not tagged and not propagated.

Subnet bindings are static, which means that active hosts are not learned. They can be used locally for SGT imposition and SGACL enforcement. Packets tagged by subnet to SGT mapping can be propagated on Layer 2 or Layer 3 TrustSec links.

**Note** For IPv6 networks, SXPv3 cannot export subnet bindings to SXPv2 or SXPv1 peers.

## Examples

```
Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234
```

## Related Commands

| Command | Description |
|---|---|
| **cts role-based** | Manually maps a source IP address to a SGT on either a host or a VRF. |

# cts sxp node-id

To configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4), use the **cts sxp node-id** command in global configuration mode. To remove the node ID, use the **no** form of this command.

**cts sxp node-id** {*node-id* | **interface** *interface-type* | *ipv4-address*}
**no cts sxp node-id**

## Syntax Description

| | |
|---|---|
| *node-id* | Specifies the node ID of the device. Enter the node ID in hexadecimal format. |
| **interface** *interface-type* | Specifies the type of interface. |
| *ipv4-address* | Specifies the SXP peer IPv4 address. |

## Command Default

A node ID is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.3(2)T | This command was introduced. |
| Cisco IOS Release 3.9S | This command was modified. Support was added for the Cisco ASR 1000 Series Routers. |

## Usage Guidelines

The **cts sxp node-id** command configures the node ID of a network device.

An SXP node ID is used to identify the individual devices within the network. The node ID is a four-octet integer that can be configured by the user. If it is not configured by the user, SXP picks a node ID itself using the highest IPv4 address in the default VRF domain, in the same manner that EIGRP generates its node ID.

The node ID has to be unique in the network that SXP connections traverse to enable SXP loop prevention.

The SXP loop detection mechanism drops the binding propagation packets based on finding its own node ID in the peer sequence attribute. Changing a node ID in a loop detection running SXP network could break SXP loop detection functionality and therefore needs to be handled carefully.

Wait until the SXP bindings that are propagated with the particular node ID in the path attribute are deleted, before you change the node ID.



**Note** A syslog is generated when you change the node ID.

```
Device(config)# cts sxp node-id 172.16.1.3
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp enable** | Enables CTS-SXP on a device. |
| **show cts sxp** | Displays the status of all CTS-SXP configurations. |

# cts sxp reconciliation period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period, use the **cts sxp reconciliation period** command in global configuration mode. To return the CTS-SXP reconciliation period to its default value, use the **no** form of this command.

**cts sxp reconciliation period** *seconds*
**no cts sxp reconciliation period** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | CTS-SXP reconciliation timer in seconds. The range is from 0 to 64000. The default is 120. |

## Command Default

120 seconds (2 minutes)

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

After a peer terminates a CTS-SXP connection, an internal Delete Hold-down timer starts. If the peer reconnects before the Delete Hold-down timer expires, then the CTS-SXP Reconciliation timer starts. While the CTS-SXP Reconciliation period timer is active, the CTS-SXP software retains the SGT mapping entries learned from the previous connection and removes invalid entries. Setting the SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

## Related Commands

| Command | Description |
|---|---|
| **cts sxp connection peer** | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| **cts sxp default password** | Configures the CTS-SXP default password. |
| **cts sxp default source-ip** | Configures the CTS-SXP source IPv4 address. |
| **cts sxp enable** | Enables CTS-SXP on a device. |
| **cts sxp log** | Turns on logging for IP to SGT binding changes. |
| **cts sxp retry** | Changes the CTS-SXP retry period timer. |

| Command | Description |
|---|---|
| **show cts sxp** | Displays status of all CTS-SXP configurations. |

# cts sxp retry period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) retry period timer, use the **cts sxp retry period** command in global configuration mode. To return the CTS-SXP retry period timer to its default value, use the **no** form of this command.

**cts sxpretry period** *seconds*
**no cts sxpretry period** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | CTS-SXP retry timer in seconds. The range is from 0 to 64000. The default is 120. |

## Command Default

120 seconds (2 minutes)

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI3 | This command was introduced on the Catalyst 6500 series switches. |
| 12.2(50)SG7 | This command was integrated on the Catalyst 4000 series switches. |
| 12.2(53)SE2 | This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches. |
| Cisco IOS XE Release 3.4S | This command was integrated into Cisco IOS XE Release 3.4S. |
| 15.1(3)S | This command was integrated into Cisco IOS Release 15.1(3)S. |

## Usage Guidelines

The retry timer is triggered if there is at least one CTS-SXP connection that is not up. A new CTS-SXP connection is attempted when this timer expires. A zero value results in no retry being attempted.

## Related Commands

| Command | Description |
|---|---|
| **cts sxp connectionpeer** | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| **cts sxp default password** | Configures the CTS-SXP default password. |
| **cts sxp default source-ip** | Configures the CTS-SXP source IPv4 address. |
| **cts sxp enable** | Enables CTS-SXP on a device. |
| **cts sxp log** | Enables logging for IP-to-SGT binding changes. |
| **cts sxp reconciliation** | Changes the CTS-SXP reconciliation period. |
| **show cts sxp** | Displays the status of all CTS-SXP configurations. |

# cts sxp speaker hold-time

To configure the global hold-time period of a speaker network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp speaker hold-time** command in global configuration mode. To remove the hold time from the speaker device, use the **no** form of this command.

**cts sxp speaker hold-time** *minimum-period*
**no cts sxp speaker hold-time**

## Syntax Description

| | |
|---|---|
| *minimum-period* | Minimum allowed hold time in seconds. The range is from 1 to 65534. |

## Command Default

The default hold time for a speaker device is 120 seconds.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.3(2)T | This command was introduced. |
| Cisco IOS Release 3.9S | This command was modified. Support was added for the Cisco ASR 1000 Series Routers. |

## Usage Guidelines

The Security Group Tag Exchange Protocol (SXP) uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism, the hold-time period, in order to provide more predictable and timely detection of connection loss.

Hold time can be configured globally on a network device. This global configuration will apply the configuration to all SXP connections configured on the device.

You may configure a hold-time period locally on a speaker device or a default of 120 seconds is used. This is the shortest period of time a speaker is willing to send keepalive messages for keeping the connection active. Any shorter hold-time period would require a faster keepalive rate than the rate the speaker is ready to support. A value of 0xFFFF indicates that the keepalive mechanism is not used.

The hold-time negotiation between the speaker device and the listener device succeeds when the speaker's minimum acceptable hold time falls below or within the desirable hold-time range of the listener. (Use the **cts sxp listener hold-time** command to configure the hold time of the listener device.) If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.

The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.

The selected hold-time period of a successful negotiation is the maximum of the speaker's minimum acceptable hold time and the lower bound of the listener's hold-time range.

The speaker calculates the keepalive time to one-third of the selected hold time by default, unless a different keepalive time is locally configured.

The following example shows how to configure the minimum hold time period of a speaker device for 300 seconds:

```
Device(config)# cts sxp speaker hold-time 300
```

## Related Commands

| Command | Description |
|---|---|
| **cts sxp enable** | Enables Cisco TrustSec SXP on a device. |
| **cts sxp listener hold-time** | Configures the hold time of a listener device in an SXPv4 network. |
| **show cts sxp** | Displays the status of all Cisco TrustSec SXP configurations. |

# custom-page

To display custom web pages during web authentication login, use the **custom-page** command in parameter map webauth configuration mode. To disable custom web pages, use the **no** form of this command.

**custom-page** {**failure** | **login** [**expired**] | **success**} **device** *location***:***filename*
**no custom-page** {**failure** | **login** [**expired**] | **success**} **device** *location***:***filename*

## Syntax Description

| | |
|---|---|
| **failure** | Displays the custom web page if the login fails. |
| **login** | Displays the custom web page during login. |
| **expired** | (Optional) Displays the custom web page if the login expires. |
| **success** | Displays the custom web page when the login is successful. |
| *location* **:***filename* | Location and name of the locally stored HTML file to use in place of the default HTML file for the specified condition. |

## Command Default

The internal default web pages are displayed.

## Command Modes

Parameter map webauth configuration (config-params-parameter-map)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2SE | This command was introduced. |

## Usage Guidelines

Use the **custom-page** command to display custom web pages during web authentication login. To enable custom web pages:

- You must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages are used.
- The four custom HTML files and any images in the custom pages must be stored in the disk or flash of the switch. The maximum size of each HTML file is 256 KB.
- Filenames must start with web_auth.
- To serve custom pages and images from an external server, you must configure a redirect portal IP address by using the **redirect** (parameter-map webauth) command instead of using local custom pages.
- Any external link from a custom page requires an intercept ACL configuration.
- Any name resolution required for external links or images requires an intercept ACL configuration.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.
- Because the custom login page is a public web form, consider the following guidelines for this page:
  - The login form must accept user input for the username and password and must POST the data as uname and pwd.

- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

## Examples

The following example shows how to configure a named parameter map for web authentication with custom pages enabled:

```
parameter-map type webauth PMAP_WEBAUTH
 type webauth
 custom-page login device flash:webauth_login.html
 custom-page success device flash:webauth_success.html
 custom-page failure device flash:webauth_fail.html
 custom-page login expired device flash:webauth_expire.html
```

## Related Commands

| Command | Description |
|---|---|
| **banner** (parameter-map webauth) | Displays a banner on the web-authentication login web page. |
| **consent email** | Requests a user's e-mail address on the consent login web page. |
| **redirect** (parameter-map webauth) | Redirects clients to a particular URL during web-based authentication. |

# cws out

To enable Cloud Web Security content scanning on an egress interface, use the **cws out** command in interface configuration mode. To disable Cloud Web Security content scanning, use the **no** form of this command.

**cws out**
**no cws out**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Cloud Web Security content scan is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.4(2)T | This command was introduced. This command replaces the **content-scan out** command. |

## Usage Guidelines

The content scanning process redirects client web traffic to Cloud Web Security. Content scanning is enabled on an Internet-facing WAN interface to protect the web traffic going out.

In case you enable content scanning on a interface that has Wide Area Application Services (WAAS) configured, you must not apply both the WAAS and content scanning feature on the same TCP session.

## Examples

The following example shows how to enable Cloud Web Security content scanning on a Gigabit Ethernet interface:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# cws out
```

## Related Commands

| Command | Description |
|---|---|
| **cws whitelisting** | Enables allowed listing of incoming traffic and enters Cloud Web Security allowed list configuration mode. |
| **interface** | Configures an interface and enters interface configuration mode. |

# cws whitelisting

To enable allowed listing of incoming traffic and to enter Cloud Web Security allowed listing configuration mode, use the **cws whitelisting** command in global configuration mode. To disable the allowed listing of traffic, use the **no** form of this command.

**cws whitelisting**
**no cws whitelisting**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Allowed listing of traffic is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.4(2)T | This command was introduced. This command replaces the **content-scan whitelisting** command. |

## Usage Guidelines

An approved list contains entities that are provided a particular privilege, service, mobility, access, or recognition. Allowed lists grant access.

The web traffic that you have configured for allowed listing will bypass the content scanning by Cloud Web Security.

## Examples

The following example shows how to enable Cloud Web Security content scan allowed listing and enter Cloud Web Security allowed list configuration mode:

```
Device(config)# cws whitelisting
Device(config-cws-wl)#
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type cws global** | Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode. |