

# traffic-export through zone security


- track(firewall), on page 4
- tracking, on page 6
- traffic-export, on page 8
- transfer-encoding type, on page 10
- transport port, on page 12
- transport port (ldap), on page 13
- trm register, on page 14
- trustpoint (tti-petitioner), on page 15
- trustpoint signing, on page 16
- trusted-port (IPv6 NDP Inspection Policy), on page 17
- trusted-port (IPv6 RA Guard Policy), on page 18
- tunnel-limit (GTP), on page 19
- tunnel mode, on page 20
- tunnel mode ipsec dual-overlay , on page 25
- tunnel protection, on page 26
- tunnel protection ipsec policy, on page 30
- type echo protocol ipIcmpEcho, on page 32
- udp half-open, on page 34
- udp idle-time, on page 35
- unmatched-action, on page 37
- url (ips-auto-update), on page 38
- url rewrite, on page 39
- urlfilter, on page 40
- url-list, on page 41
- url-profile, on page 43
- validate source-mac, on page 45
- url-text, on page 46
- usage, on page 47
- user, on page 48
- user-group, on page 50
- user-group (parameter-map), on page 51
- user-group logging, on page 53
- username, on page 54

- username (dot1x credentials), on page 60
- username (ips-autoupdate), on page 61
- username algorithm-type, on page 63
- username secret, on page 65
- user-profile location, on page 68
- variable, on page 70
- view, on page 72
- virtual-template (IKEv2 profile), on page 74
- virtual-template (webvpn context), on page 75
- vlan (local RADIUS server group), on page 76
- vlan group, on page 78
- vpdn aaa attribute, on page 79
- vrf (ca-trustpoint), on page 82
- vrf (ca-trustpool), on page 83
- vrf (isakmp profile), on page 85
- vrfname, on page 87
- vrf-name, on page 88
- vsa vendor-id, on page 89
- web-agent-url, on page 90
- webvpn, on page 92
- webvpn-homepage, on page 93
- webvpn cef, on page 94
- webvpn context, on page 95
- webvpn create template, on page 97
- webvpn enable, on page 99
- webvpn gateway, on page 100
- webvpn import svc profile, on page 102
- webvpn install, on page 103
- webvpn sslvpn-vif nat, on page 105
- whitelist (cws), on page 106
- wins, on page 108
- wlccp authentication-server client, on page 110
- wlccp authentication-server infrastructure, on page 112
- wlccp wds priority interface, on page 113
- xauth userid mode, on page 115
- xsm, on page 117
- xsm dvdm, on page 119
- xsm edm, on page 120
- xsm history vdm, on page 122
- xsm history edm, on page 124
- xsm privilege configuration level, on page 126
- xsm privilege monitor level, on page 128
- xsm vdm, on page 130
- zone-member security, on page 132
- zone-mismatch drop, on page 133
- zone pair security, on page 135

• zone security, on page 137

# track(firewall)

To configure the redundancy group tracking, use the **track**command in redundancy application group configuration mode. To remove the redundancy group tracking, use the **no** form of this command.

**track** *object-number* {**decrement** *value* | **shutdown**}
**no track** *object-number* {**decrement** *value* | **shutdown**}

## Syntax Description

| | |
|---|---|
| *object-number* | ID of the event type. |
| **decrement** *value* | Specifies the value that the priority will be decremented. The range is from 1 to 255. |
| **shutdown** | Shuts down a redundancy group if the tracked object goes down instead of changing the priority. |

## Command Default

Objects and decrement priority per object are not tracked.

## Command Modes

Redundancy application group configuration (config-red-app-grp)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.1S | This command was introduced. |

## Usage Guidelines

The redundancy group can track an object and decrease the priority value per object. Multiple objects can be tracked by the redundancy group to influence the priority appropriately. You can shut down a redundancy group if the tracked object goes down instead of changing the priority.

## Examples

The following example shows how to track the redundancy group named group1 and assign a decrement value:

```
Router# configure terminal
Router(config)# redundancy

Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# track 200 decrement 50
```

## Related Commands

| Command | Description |
|---|---|
| **application redundancy** | Enters redundancy application configuration mode. |
| **authentication** | Configures clear text authentication and MD5 authentication for a redundancy group. |
| control | Configures the control interface type and number for a redundancy group. |
| data | Configures the data interface type and number for a redundancy group. |

| Command | Description |
|---|---|
| **group(firewall)** | 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. |
| **redundancy rii** | Configures the RII for the redundancy group. |

# tracking

To override the default tracking policy on a port, use the **tracking**command in Neighbor Discovery (ND) inspection policy configuration mode.

**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

## Syntax Description

| | |
|---|---|
| **enable** | Tracking is enabled. |
| **reachable-lifetime** | (Optional) The maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability.<br>• The **reachable-lifetime** keyword can be used only with the **enable** keyword.<br>• Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command. |
| *value* | Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300. |
| **infinite** | Keeps an entry in a reachable or stale state for an infinite amount of time. |
| **disable** | Disables tracking. |
| **stale-lifetime** | (Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration.<br>• The stale lifetime is 86,400 seconds.<br>• The **stale-lifetime** keyword can be used only with the **disable** keyword.<br>• Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command. |

## Command Default

The time entry is kept in a reachable state.

## Command Modes

ND inspection policy configuration (config-nd-inspection)

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |
| 15.0(2)SE | This command was integrated into Cisco IOS Release 15.0(2)SE. |
| 15.3(1)S | This command was integrated into Cisco IOS Release 15.3(1)S. |

## Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through ND inspection. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **stale-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

## Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 nd inspection policy** | Defines the ND inspection policy name and enters ND inspection policy configuration mode. |
| **ipv6 nd raguard policy** | Defines the RA guard policy name and enters RA guard policy configuration mode. |
| **ipv6 neighbor binding** | Changes the defaults of neighbor binding entries in a binding table. |
| **ipv6 neighbor tracking** | Enables tracking of entries in the binding table. |

# traffic-export

To control the operation of IP traffic capture mode in IP traffic export, use the **traffic-export** command in privileged EXEC mode.

**traffic-export interface** *type number* {**start** | **stop** | **clear** | **copy** *memory-device*}

## Syntax Description

| | |
|---|---|
| *type number* | Type and number of the interface over which the packets being captured travel. |
| start | Initiates a packet capture sequence. |
| stop | Halts a packet capture sequence. |
| clear | Clears the packet capture buffer. |
| **copy** | Copies the contents of the packet capture buffer to an external device. |
| *memory-device* | External memory device to which captured packets are transmitted. Options are *flash:*, *tftp:*, or *usbflash0:*. |

## Command Default

This command has no defaults.

## Command Modes

Privileged EXEC.

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Use the **traffic-export** command to control the operation of IP traffic capture mode in IP traffic export. The operator uses CLI commands to start or stop capture of packets flowing across a monitored interface, to copy the captured packets to an external memory device, or to clear the internal buffer which holds the captured packets.

## Examples

The following example illustrates the use of the **traffic-export** command to initiate the capture of packets on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 start
%RITE-5-CAPTURE_START: Started IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to halt the packet capture sequence on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 stop
%RITE-5-CAPTURE_STOP: Stopped IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to copy the contents of the packet capture buffer to an external memory device. The example of the interactive dialog identifies the external memory device and the remote host in which it resides.

```
Router# traffic-export interface fastethernet0/0 copy tftp:

Address or name of remote host []? 172.18.207.15

Capture buffer filename []? atmcapture

Copying capture buffer to tftp://172.18.207.15/atmcapture !!
router#
```

The following example illustrates the use of the **traffic-export** command to clear the packet capture buffer that is in local memory.

```
Router# traffic-export interface fastethernet 0/0 clear
%RITE-5-CAPTURE_CLEAR: Cleared IP traffic capture buffer for interface FastEthernet0/0
router#
```

## Related Commands

| Command | Description |
|---|---|
| **ip traffic-export apply profile** | Applies an IP traffic export or IP traffic capture profile to a specific interface. |
| **ip traffic-export profile** | Creates an IP traffic export or IP traffic capture profile on an ingress interface. |

# transfer-encoding type

To permit or deny HTTP traffic according to the specified transfer-encoding of the message, use the **transfer-encoding type**command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

**transfer-encoding type** {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**reset** | **allow**} [**alarm**]
**no transfer-encoding type** {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**reset** | **allow**} [**alarm**]

## Syntax Description

| | |
|---|---|
| **chunked** | Encoding format (specified in RFC 2616, *Hypertext Transfer Protocol--HTTP/1* ) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator. |
| **compress** | Encoding format produced by the UNIX "compress" utility. |
| deflate | "ZLIB" format defined in RFC 1950, *ZLIB Compressed Data Format Specification version 3.3* , combined with the "deflate" compression mechanism described in RFC 1951, *DEFLATE Compressed Data Format Specification version 1.3* . |
| gzip | Encoding format produced by the "gzip" (GNU zip) program. |
| identity | Default encoding, which indicates that no encoding has been performed. |
| default | All of the transfer encoding types. |
| action | Encoding types outside of the specified 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 a given type is not specified, all transfer-encoding types are supported with the reset alarm action.

## Command Modes

appfw-policy-http configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Only encoding types specified by the **transfer-encoding-type**command are allowed through the firewall.

## 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
!
!
```

# transport port

To configure the transport protocol for establishing a connection with the Diameter peer, use the **transport port**command in Diameter peer configuration mode. To block all sessions that are bound to the peer from using the connection, use the no form of this command.

**transport tcp port port-number**
**no transport tcp port port-number**

## Syntax Description

| | |
|---|---|
| **tcp** | Currently, TCP is the only supported transport protocol for establishing the connection with the Diameter peer. |
| *port-number* | Character string identifying the peer connection port. |

## Command Default

TCP is the default transport protocol.

## Command Modes

Diameter peer configuration

## Command History

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

## Examples

The following example configures TCP as the transport protocol and port 4100 as the peer connection port:

```
Router (config-dia-peer)# transport tcp port
 4100
```

## Related Commands

| Command | Description |
|---|---|
| **diameter peer** | Defines a Diameter peer and enters Diameter peer configuration mode. |

# transport port (ldap)

To configure the transport protocol for establishing a connection with the Lightweight Directory Access Protocol (LDAP) server, use the **transport port** command in LDAP server configuration mode. To delete all sessions that are bound to the server from using the connection, use the **no** form of this command.

**transport port** *port-number*
**no transport port** *port-number*

## Syntax Description

| | |
|---|---|
| *port-number* | Server connection port number. Valid port numbers range from 1 to 65535. The default is 389. |

## Command Default

The default port number is 389.

## 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 configure the transport protocol and port 200 as the peer connection port:

```
Router(config)# ldap server server1
Router(config-ldap-server)# transport port 200
```

## 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. |

# trm register

To allow the user to manually register the platform with the Trend Router Provisioning Server (TRPS), use the **trm register**command in privileged EXEC mode.

**trm register** [**force**]

## Syntax Description

| | |
|---|---|
| **force** | Sends a new registration request to TRPS. |

## Command Default

This command is not enabled.

## Command Modes

Privileged EXEC (#)

## 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. |
| 15.1(2)T | This command was modified. The **force**keyword was added. |

## Usage Guidelines

Use the **trm register** command to enable manual registration of the platform with the TRPS. If you do not use this command, the system sends a registration request to the TRPS every minute after boot-up until the registration is successful.

## Examples

The following is sample output from the **trm register**command:

```
Router# trm register
Processing registration request.
Please run 'show ip trm subscription" status to get more info
```

# trustpoint (tti-petitioner)

To specify the trustpoint that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the Secure Device Provisioning (SDP) petitioner and the SDP registrar, use the **trustpoint**command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

**trustpoint** *trustpoint-label*
**no trustpoint** *trustpoint-label*

## Syntax Description

| | |
|---|---|
| *trustpoint-label* | Name of trustpoint. |

## Command Default

If a trustpoint is not specified, a default trustpoint called "tti" is generated.

## Command Modes

tti-petitioner configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

Use the **trustpoint** command in tti-petitioner configuration mode to associate a trustpoint with the SDP petitioner.

## Examples

The following example shows how specify the trustpoint "mytrust":

```
crypto wui tti petitioner
 trustpoint mytrust
```

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 which generates 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 wui tti petitioner** | Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode. |

# trustpoint signing

To specify the trustpoint and associated certificate to be used when signing all introduction data during the Secure Device Provisioning (SDP) exchange, use the **trustpoint signing**command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

**trustpoint signing** *trustpoint-label*
**no trustpoint signing** *trustpoint-label*

## Syntax Description

| | |
|---|---|
| *trustpoint-label* | Name of trustpoint. |

## Command Default

If a trustpoint is not specified, any existing device certificate is used. If none is available, a self-signed certificate is generated.

## Command Modes

tti-petitioner configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Use the **trustpoint** signing command in tti-petitioner configuration mode to associate a specific trustpoint with the petitioner for signing its certificate.

## Examples

The following example shows how to specify the trustpoint mytrust:

```
crypto provisioning petitioner
 trustpoint signing 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. |
| trustpoint (tti-petitioner) | Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar. |

# trusted-port (IPv6 NDP Inspection Policy)

To configure a port to become a trusted port, use the **trusted-port** command in Neighbor Discovery Protocol ( NDP) inspection policy configuration mode . To disable this function, use the **no** form of this command.

**trusted-port**
**no trusted-port**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No ports are trusted.

## Command Modes

NDP inspection policy configuration
(config-nd-inspection)

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |
| 15.0(2)SE | This command was integrated into Cisco IOS Release 15.0(2)SE. |
| 15.3(1)S | This command was integrated into Cisco IOS Release 15.3(1)S. |

## Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Use the **trusted-port** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

## Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# trusted-port
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 nd inspection policy** | Defines the NDP inspection policy name and enters NDP inspection policy configuration mode. |

# trusted-port (IPv6 RA Guard Policy)

To configure a port to become a trusted port, use the **trusted-port**command in router advertisement (RA) guard policy configuration . To disable this function, use the **no** form of this command.

**trusted-port**
**no trusted-port**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No ports are trusted.

## Command Modes

RA guard policy configuration
(config-ra-guard)

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |
| 15.0(2)SE | This command was integrated into Cisco IOS Release 15.0(2)SE. |
| 15.3(1)S | This command was integrated into Cisco IOS Release 15.3(1)S. |

## Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, the **device-role** command takes precedence over the **trusted-port** command; if the device role is configured as host, messages will be dropped regardless of **trusted-port** command configuration.

## Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-ra-guard)# trusted-port
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 nd inspection policy** | Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode. |
| **ipv6 nd raguard policy** | Defines the RA guard policy name and enter RA guard policy configuration mode. |

# tunnel-limit (GTP)

To specify the maximum number of General Packet Radio Service (GPRS) Tunneling Protocol (GTP) tunnels that can be configured, use the **tunnel-limit** command in parameter-map type inspect configuration mode. To return to the default tunnel limit, use the **no** form of this command.

**tunnel-limit** *max-tunnels*
**no tunnel-limit**

## Syntax Description

| | |
|---|---|
| *max-tunnels* | Number of GTP tunnels that can be configured. Valid values are from 1 to 4294967295. The default is 500. |

## Command Default

A tunnel limit of 500 is configured.

## Command Modes

Parameter-map type inspect configuration (config-profile)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.7S | This command was introduced. |

## Examples

The following example shows how to limit the number of configured GTP tunnels to 23456:

```
Device(config)# parameter-map type inspect-global gtp
Device(config-profile)# tunnel-limit 23456
Device(config-profile)#
```

## Related Commands

| Command | Description |
|---|---|
| **parameter-map type inspect-global** | Configures a global parameter map and enters parameter-map type inspect configuration mode. |

# tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the no form of this command.

**tunnel mode** {**aurp** | **auto** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
**no tunnel mode**

## Syntax Description

| | |
|---|---|
| **aurp** | Specifies AppleTalk Update-Based Routing Protocol. |
| **auto** | Enables auto tunneling mode. |
| **cayman** | Specifies Cayman TunnelTalk AppleTalk encapsulation. |
| **dvmrp** | Specifies Distance Vector Multicast Routing Protocol. |
| **eon** | Specifies EON compatible Connectionless Network Protocol (CLNS) tunnel. |
| **gre** | Specifies generic routing encapsulation (GRE) protocol. This is the default. |
| **gre multipoint** | Specifies Multipoint GRE (mGRE). |
| **gre ip** | Specifies GRE tunneling using IPv4 as the delivery protocol. |
| **gre ipv6** | Specifies GRE tunneling using IPv6 as the delivery protocol. |
| **ipip** | Specifies IP-over-IP encapsulation. |
| **decapsulate-any** | (Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination. |
| **ipsec ipv4** | Specifies tunnel mode is IPsec, and the transport is IPv4. |
| **iptalk** | Specifies Apple IPTalk encapsulation. |
| **ipv6** | Specifies static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6. |
| **ipsec ipv6** | Specifies tunnel mode is IPsec, and the transport is IPv6. |
| **mpls** | Specifies Multiprotocol Label Switching (MPLS) encapsulation. |
| **nos** | Specifies KA9Q/NOS compatible IP over IP. |
| **rbscp** | Specifies Rate Based Satellite Control Protocol (RBSCP). |

## Command Default

The default is GRE tunneling.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 10.3 | This command was modified. The **aurp**, **dvmrp**, and **ipip** keywords were added. |
| 11.2 | This command was modified. The optional **decapsulate-any** keywords were added. |
| 12.2(13)T | This command was modified. The **gre multipoint** keywords were added. |
| 12.3(7)T | This command was modified. The following keywords were added:<br>• **gre ipv6** to support GRE tunneling using IPv6 as the delivery protocol.<br>• **ipv6** to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6.<br>• **rbscp** to support RBSCP. |
| 12.3(14)T | This command was modified. The **ipsec ipv4** keywords were added. |
| 12.2(18)SXE | This command was modified. The **gre multipoint** keywords were added. |
| 12.2(30)S | This command was integrated into Cisco IOS Release 12.2(30)S. |
| 12.2(25)SG | This command was integrated into Cisco IOS Release 12.2(25)SG. |
| 12.4(4)T | This command was modified. The **ipsec ipv6** keywords were 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 implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |
| 15.4(2)T | This command was modified. The **auto** keyword was added. |
| 15.4(2)S | This command was implemented on the Cisco ASR 901 Series Aggregation Services Router. |
| Cisco IOS XE Release 3.12S | This command was integrated into Cisco IOS XE Release 3.12S. |

## Usage Guidelines

### Auto Tunneling

Auto tunneling mode eases the configuration and spares you about knowing the responder's details. It automatically applies the tunneling protocol (GRE or IPsec) and transport protocol (IPv4 or IPv6) on the virtual template as soon as the IKE profile creates the virtual access interface.

### Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco devices to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two devices or between a Cisco device and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

### DVMRP

Use DVMRP when a device connects to an mrouted (multicast) device to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

### GRE with AppleTalk

GRE tunneling can be done between Cisco devices only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

### IPsec in IPv6 Transport

IPv6 IPsec encapsulation provides site-to-site IPsec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 devices to work as a security gateway, establishes IPsec tunnels between another security gateway device, and provides crypto IPsec protection for traffic from an internal network when being transmitting across the public IPv6 Internet. IPv6 IPsec is very similar to the security gateway model using IPv4 IPsec protection.

### Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPsec profile. Combining mGRE tunnels and IPsec encryption allows a single mGRE interface to support multiple IPsec tunnels, thereby simplifying the size and complexity of the configuration.



**Note** GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

### RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPsec, over satellite links without breaking the end-to-end model.

### Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

## Examples

The following example shows how to enable auto tunneling mode:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode auto
```

The following example shows how to enable Cayman tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode cayman
```

The following example shows how to enable GRE tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# appletalk cable-range 4160-4160 4160.19
Device(config-if)# appletalk zone Engineering
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode gre
```

The following example shows how to configure a tunnel using IPsec encapsulation with IPv4 as the transport mechanism:

```
Device(config)# crypto ipsec profile PROF
Device(config)# set transform tset
Device(config)# interface Tunnel0
Device(config)# ip address 10.1.1.1 255.255.255.0
Device(config)# tunnel mode ipsec ipv4
Device(config)# tunnel source Loopback0
Device(config)# tunnel destination 172.16.1.1
Device(config-if)# tunnel protection ipsec profile PROF
```

The following example shows how to configure an IPv6 IPsec tunnel interface:

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Device(config-if)# tunnel destination 10.0.0.1
Device(config-if)# tunnel source Ethernet 0/0
Device(config-if)# tunnel mode ipsec ipv6
Device(config-if)# tunnel protection ipsec profile profile1
```

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the ! receiving
 router would have to do the reassembly.
 ip mtu 1416
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not ! advertise
 routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets IPSec peer address to Ethernet interface’s public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

The following example shows how to enable RBSCP tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode rbscp
```

## Related Commands

| Command | Description |
|---|---|
| **appletalk cable-range** | Enables an extended AppleTalk network. |

| Command | Description |
|---|---|
| **appletalk zone** | Sets the zone name for the connected AppleTalk network. |
| **tunnel destination** | Specifies the destination for a tunnel interface. |
| **tunnel protection** | Associates a tunnel interface with an IPsec profile. |
| **tunnel source** | Sets the source address of a tunnel interface. |

# tunnel mode ipsec dual-overlay

To configure the tunnel mode as dual-overlay, use the **tunnel mode ipsec dual-overlay** command in interface configuration mode. To restore the default mode, use the no form of this command.

**tunnel mode ipsec dual-overlay**
**no tunnel mode ipsec dual-overlay**

## Syntax Description

| | |
|---|---|
| **ipsec** | Tunnel mode is IPsec. |
| **dual-overlay** | Specifies a dual-overlay tunnel. |

## Command Default

None.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.9.1a | This command was introduced. |

## Usage Guidelines

Use the **tunnel mode ipsec dual-overlay** command to specify the encapsulation protocol for the tunnel. IPsec dual-overlay tunnel modes provides the capabilities to carry both IPv4 and IPv6 traffic using a single IPsec Security Association (SA) that is tunnelled over IPv4.

## Examples

The following example shows how to configure the tunnel mode as dual-overlay:

```
Device(config)# interface tunnel 1
Device(config-if)# ipv6 enable
Device(config-if)# tunnel source ethernet 0/0
Device(config-if)# tunnel mode ipsec dual-overlay
Device(config-if)# tunnel destination 10.108.164.19 255.255.255.255.0
Device(config-if)# tunnel protection IPsec profile ipsecprof
```

## Related Commands

| Command | Description |
|---|---|
| **tunnel protection** | Associates a tunnel interface with an IPsec profile. |
| **tunnel mode** | Sets the encapsulation mode for the tunnel interface. |

# tunnel protection

To associate a tunnel interface with an IP Security (IPsec) profile, use the **tunnel protection** command in interface configuration mode. To disassociate a tunnel with an IPsec profile, use the **no** form of this command.

**tunnel protection { ipsec profile** *name* **[shared | { isakmp-profile | ikev2-profile }** *name* **] } | { timeout pending-connection** *<timeout>* **}**
**no tunnel protection { ipsec profile** *name* **[shared | { isakmp-profile | ikev2-profile }** *name* **] } | { timeout pending-connection** *<timeout>* **}**

## Syntax Description

| | |
|---|---|
| **ipsec profile** | Enables generic routing encapsulation (GRE) tunnel encryption via IPsec. |
| *name* | Name of the IPsec profile. This value must match the *name* specified in the **crypto ipsec profile** command. |
| **shared** | (Optional) Allows the tunnel protection IPsec Security Association Database (SADB) to share the same dynamic crypto map instead of creating a unique crypto map per tunnel interface. |
| **isakmp-profile** | Specifies the isakmp profile for the crypto connection. |
| **ikev2-profile** | Specifies the ikev2 profile for the crypto connection. |
| *shared name* | Name of the shared socket for the crypto connection. |
| **timeout pending-connection** *seconds* | Specifies the timeout to terminate pending connections. The default value is 300 seconds. The range is 60-3600 |

## Command Default

Tunnel interfaces are not associated with IPsec profiles.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| XE 17.3.4 | The **timeout pending-connection** keyword was introduced. |
| 12.2(13)T | This command was introduced. |
| 12.3(5)T | The shared keyword was added. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.4(5) | The **shared** keyword was changed so that if it is used with the **tunnel protection** command, the **tunnel source** command must specify an interface instead of an IP address. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.(33)SRA. |
| Cisco IOS XE Release 2.5 | This command was modified. This command was integrated into Cisco IOS XE Release 2.5. |

| Release | Modification |
|---|---|
| 15.4(2)S | This command was implemented on the Cisco ASR 901 Series Aggregation Services Router. |

## Usage Guidelines

Use the **tunnel protection** command to specify that IPsec encryption will be performed after the GRE has been added to the tunnel packet. The **tunnel protection** command can be used with multipoint GRE (mGRE) and point-to-point GRE (p-pGRE) tunnels. With p-pGRE tunnels, the tunnel destination address will be used as the IPsec peer address. With mGRE tunnels, multiple IPsec peers are possible; the corresponding Next Hop Resolution Protocol (NHRP) mapping nonbroadcast multiaccess (NBMA) destination addresses will be used as the IPsec peer addresses.

### The shared Keyword

If you want to configure two Dynamic Multipoint VPN (DMVPN) mGRE and IPsec tunnels on the same router with the same local endpoint (tunnel source) configuration, you *must* issue the **shared** keyword.

The dynamic crypto map that is created by the **tunnel protection** command is always different from a crypto map that is configured directly on the interface.

Unlike with the **tunnel protection** command, which specifies that IPsec encryption will be performed after GRE encapsulation, configuring a crypto map on a tunnel interface specifies that encryption will be performed before GRE encapsulation.

If the **shared** keyword is used, the **tunnel source** command must specify an interface instead of an IP address. Crypto sockets are not shared if the tunnel source is not specified as an interface.

**Note** GRE keepalive is supported only with crypto map. GRE tunnel keepalives (configured with the **keepalive** command under the GRE interface) are not supported in combination with the **tunnel protection** command.

The **tunnel mode** command must be configured before running the **tunnel protection** command. Changing the sequence by configuring this command followed by the **tunnel mode** command results in the tunnel not having connectivity.

## Examples

The following example shows how to associate the IPsec profile "vpnprof" with an mGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. There is a static NHRP mapping from IP address 10.0.0.3 to IP address 172.16.2.1, so for this NHRP mapping the IPsec destination peer address will be 172.16.2.1. The IPsec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**. Other NHRP mappings (static or dynamic) will automatically create additional IPsec security associations (SAs) with the same source peer address and the destination peer address from the NHRP mapping. The IPsec proxy for these NHRP mappings will be as follows: **permit gre host** *ethernet0-ip-address* **host** *NHRP-mapping-NBMA-address*.

```
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
```

```
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets the IPSec peer address to the Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

The following example shows how to associate the IPsec profile "vpnprof" with a p-pGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. The IPsec destination peer address will be 172.16.1.10 (per the **tunnel destination address** command). The IPsec proxy will be as follows: **permit gre host** *ethernet0-ip-address* **host** *ip-address*.

```
interface Tunnel1
 ip address 10.0.1.1 255.255.255.252
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
 ip mtu 1420
 tunnel source Ethernet0
 tunnel destination 172.16.1.10
 tunnel protection ipsec profile vpnprof
```

In the following example, the crypto sockets are shared between the Tunnel0 and Tunnel1 interfaces because the **tunnel protection** command on both interfaces uses the same profile and is configured with the **shared** keyword. Both tunnels specify the tunnel source to be an Ethernet0/0 interface.

```
interface Tunnel0
ip address 10.255.253.3 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication h1there
ip nhrp map 10.255.253.1 192.168.1.1
ip nhrp map multicast 192.168.1.1
ip nhrp network-id 253
ip nhrp holdtime 600
ip nhrp nhs 10.255.253.1
ip ospf message-digest-key 1 md5 wellikey
ip ospf network broadcast
ip ospf cost 35
ip ospf priority 0
no ip mroute-cache
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 253
tunnel protection ipsec profile dmvpn-profile shared
interface Tunnel1
ip address 10.255.254.3 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication h1there
ip nhrp map multicast 192.168.1.3
ip nhrp map 10.255.254.1 192.168.1.3
ip nhrp network-id 254
```

```
ip nhrp holdtime 600
ip nhrp nhs 10.255.254.1
ip ospf message-digest-key 1 md5 wellikey
ip ospf network broadcast
ip ospf priority 0
no ip mroute-cache
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 254
tunnel protection ipsec profile dmvpn-profile shared
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec profile** | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers. |
| **interface** | Configures an interface type and enters interface configuration mode. |
| **keepalive (tunnel interfaces)** | Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing the tunnel protocol down for a specific interface. |
| **permit** | Sets conditions for a named IP access list. |
| **tunnel source** | Sets the source address for a tunnel interface. |

# tunnel protection ipsec policy

To associate an ACL with a Static Virtual Tunnel Interface (SVTI), use the **tunnel protection ipsec policy** command in the interface configuration mode. To disassociate an ACL from an SVTI, use the **no** form of this command.

**tunnel protection ipsec policy** {**ipv4** | **ipv6**} *acl*
**no tunnel protection ipsec policy** {**ipv4** | **ipv6**} *acl*

## Syntax Description

| | |
|---|---|
| **ipv4** | Specifies that the traffic selector is of type IPv4. |
| **ipv6** | Specifies that the traffic selector is of type IPv6. |
| *acl* | Name or number identifying the ACL to be associated. |

## Command Default

By default, an ACL is not associated with an SVTI and a traffic selector of 'any any' is used.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 16.12.1 | Command introduced. |

## Usage Guidelines

By default, an SVTI supports a single IPSec SA with 'any any' as the traffic selector. To create IPSec SAs for non-any-any proxies, define the non-any-any proxies in ACLs and associate the ACL with an SVTI using this command.

To disassociate an ACL from an SVTI use the **no** form of the command. When an ACL is disassociated from an SVTI, the SVTI resumes the default behavior of supporting a single IPSec SA with 'any any' as the traffic selector.

### Example

The following example shows how to configure multi-SA support for an SVTI with an IPv4 traffic selector:

```
Device(conf)# interface Tunnel0
Device(config-if)# ip address 11.1.1.2 255.255.255.0
Device(config-if)# tunnel source Ethernet0/0
Device(config-if)# tunnel mode ipsec ipv4
Device(config-if)# tunnel destination 172.168.17.1
Device(config-if)# tunnel protection ipsec policy ipv4 ipsec_acl1
Device(config-if)# tunnel protection ipsec profile ipsec_prof


ip access-list extended ipsec_acl1
permit ip 30.0.0.0 0.0.0.255 40.0.0.0 0.0.0.255
permit ip 50.0.0.0 0.0.0.255 60.0.0.0 0.0.0.255
```

The following example shows how to configure multi-SA support for an SVTI with an IPv6 traffic selector:

```
Device(config)# interface Tunnel0
Device(config-if)# ipv6 address 400::10:1/112
Device(config-if)# tunnel destination 2003::8:2
Device(config-if)# tunnel source Ethernet 0/0
Device(config-if)# tunnel mode ipsec ipv6
Device(config-if)# tunnel protection ipsec policy ipv6 ipsec_acl2
Device(config-if)# tunnel protection ipsec profile ipsec_prof

ipv6 access-list ipsec_acl2
sequence 10 permit ipv6 host 2005::10:1 host 2005::11:1
sequence 20 permit ipv6 host 2005::15:1 host 2005::16:1
sequence 30 permit ipv6 host 2005::20:1 host 2005::21:1
```

# type echo protocol ipIcmpEcho

**Note** Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type echo protocol ipIcmpEcho**command is replaced by the **icmp-echo** command. See the **icmp- echo** command for more information.

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **type echo protocol ipIcmpEcho**command in IP SLA monitor configuration mode.

**type echo protocol ipIcmpEcho** {*destination-ip-addressdestination-hostname*} [**source-ipaddr** {*ip-addresshostname*} | **source-interface** *interface-name*]

## Syntax Description

| | |
|---|---|
| *destination-ip-address* \| *destination-hostname* | Destination IP address or hostname for the operation. |
| **source-ipaddr** {*ip-address* \| *hostname*} | (Optional) Specifies the source IP address or hostname . When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination. |
| **source-interface** *interface-name* | (Optional) Specifies the source interface for the operation. |

## Command Default

No IP SLAs operation type is configured for the operation being configured.

## Command Modes

IP SLA monitor configuration (config-sla-monitor)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.0(5)T | The following keyword and arguments were added:<br>• **source-ipaddr** {*ip-address* \| *hostname* |
| 12.3(7)XR | The **source-interface** keyword and *interface-name* argument were added. |
| 12.3(11)T | The **source-interface** keyword and *interface-name* argument were added. |
| 12.4(4)T | This command was replaced by the **icmp-echo** command. |
| 12.2(33)SRB | This command was replaced by the **icmp-echo** command. |
| 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)SB | This command was replaced by the **icmp-echo** command. |
| 12.2(33)SXI | This command was replaced by the **icmp-echo** command. |

## Usage Guidelines

The default request packet data size for an ICMP echo operation is 28 bytes. Use the **request-data-size** command to modify this value. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.

You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla monitor** global configuration command) and then reconfigure the operation with the new operation type.

## Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175.

```
ip sla monitor 10
 type echo protocol ipIcmpEcho 172.16.1.175
!
ip sla monitor schedule 10 start-time now
```

## Related Commands

| Command | Description |
|---|---|
| **ip sla monitor** | Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode. |

# udp half-open

To configure timeout values for UDP half-opened sessions, use the **udp half-open** command in parameter-map type inspect configuration mode. To disable the timeout values for UDP half-opened sessions, use the **no** form of this command.

**udp half-open idle-time** *milliseconds* [**ageout-time** *miliiseconds*]
**udp half-open idle-time**

## Syntax Description

| | |
|---|---|
| **idle-time** | Specifies the idle timeout for UDP half-opened sessions going through the firewall. |
| *milliseconds* | Amount of time, in milliseconds, during which a UDP session will continue to be managed while there is no activity. Valid values are from 1 to 2147483. |
| **ageout-time** *milliseconds* | (Optional) Specifies the aggressive aging time for UDP half-opened sessions. Valid values are from 1 to 2147483. |

## Command Default

The timeout default is 30 seconds.

## Command Modes

Parameter-map type inspect configuration (config-profile)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

You must configure the **parameter-map type inspect** command before you can configure the **udp half-open** command.

An UDP half-opened session is when only one UDP packet is detected in the UDP flow.

## Examples

The following example shows how to configure the idle timeout and the aggressive aging time for UDP half-open sessions:

```
Router(config)# parameter-map type inspect pmap
Router(config-profile)# udp half-open idle-time 67800 ageout-time 67800
Router(config-profile)# end
```

## 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. |

# udp idle-time

To configure the idle timeout for UDP sessions, use the **udp idle-time** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

**udp idle-time** *seconds* [**ageout-time** *seconds*]
**no udp idle-time**

## Syntax Description

| | |
|---|---|
| *seconds* | Amount of time, in seconds, during which a UDP session will continue to be managed while there is no activity. Valid values are from 1 to 2147483. |
| **ageout-time** *seconds* | (Optional) Specifies the aggressive aging time for UDP packets. Valid values are from 1 to 2147483. |

## Command Default

The timeout default is 30 seconds.

## Command Modes

Parameter-map type inspect configuration

## 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. The **ageout-time** *seconds* keyword and argument pair was added. |

## Usage Guidelines

When you configure an inspect parameter map, you can enter the **udp idle-time** command after you enter the **parameter-map type inspect** command.

When the software detects a valid UDP packet, it establishes state information for a new UDP session. Because UDP is a connectionless service, there are no actual sessions, and the software examines the information in the packet and determines if the packet is similar to other UDP packets (for example, it has similar source or destination addresses and if the packet was detected soon after another similar UDP packet).

If the software detects no UDP packets for the UDP session for the period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

## Examples

The following example shows that there is no activity and the UDP session will continue to be managed for 75 seconds:

```
Router(config)# parameter-map type inspect eng-network-profile
Router(config-profile)# udp idle-time 75
Router(config-profile)# end
```

The following example shows how to configure the aging out time for UDP sessions:

```
Router(config)# parameter-map type inspect eng-network-profile
```

```
Router(config-profile)# udp idle-time 75 ageout-time 50
Router(config-profile)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip inspect udp idle-time** | Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity). |
| **parameter-map type inspect** | Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action. |

# unmatched-action

To define the action when the user request does not match the IP address or host site configuration, use the **unmatched-action** command in URL rewrite configuration mode. To disable the action, use the **no** form of this command.

**unmatched-action** [**direct-access** | **redirect**]
**no unmatched-action** [**direct-access** | **redirect**]

## Syntax Description

| | |
|---|---|
| **direct-access** | (Optional) Provides direct access to the URL and an information page stating that the user can access the URL directly. |
| **redirect** | (Optional) Provides the user with direct access to the URL, but the user does not receive the information page as with the **direct-access** keyword. |

## Command Default

Direct access to the URL

## Command Modes

URL rewrite configuration (config-webvpn-url-rewrite)

## Command History

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

## Examples

The following example shows that the user has direct access to the URL:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# unmatched-action direct-access
```

## Related Commands

| Command | Description |
|---|---|
| **host (webvpn url rewrite)** | Selects the hostname of the site to be mangled on an SSL VPN gateway. |
| **ip (webvpn url rewrite)** | Configures the IP address of the site to be mangled on an SSL VPN gateway. |

# url (ips-auto-update)

To define a location in which to retrieve the Cisco IOS Intrusion Prevention System (IPS) signature configuration files, use the **url**command in IPS-auto-update configuration mode.

**url** *url*

## Syntax Description

| | |
|---|---|
| *url* | Location in which the router retrieves the latest signature files. |

## Command Default

The default value is defined in the signature definition XML.

## Command Modes

IPS-auto-update configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

## Examples

In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

## Related Commands

| Command | Description |
|---|---|
| **ip ips auto-update** | Enables automatic signature updates for Cisco IOS IPS. |

# url rewrite

To mangle selective URL requests on a Secure Socket Layer virtual private network (SSL VPN) gateway and enter URL rewrite mode, use the **url rewrite** command in webvpn context configuration mode. To disable selected URL requests, use the **no** form of this command.

**url rewrite**
**no url rewrite**

## Syntax Description

This command has no arguments or keywords.

## Command Default

All requests are mangled.

## Command Modes

Webvpn context configuration (config-webvpn-context)

## Command History

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

## Usage Guidelines

Configuring the **url rewrite** command enters the url rewrite submode, in which selected IP addresses or hosts are defined for mangling.

## Examples

The following example shows that selective URL mangling has been configured for IP address 10.1.1.0 255.255.0.0:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# ip 10.1.0.0 255.255.0.0
```

## Related Commands

| Command | Description |
|---|---|
| **host (webvpn url rewrite)** | Selects the name of the host site to be mangled on an SSL VPN gateway. |
| **ip (webvpn url rewrite)** | Configures the IP address of the site to be mangled on an SSL VPN gateway. |
| **unmatched-action (webvpn url rewrite)** | Defines the action when the user request does not match the IP address or host site configuration. |

# urlfilter

To enable Cisco IOS URL filtering, use the **urlfilter** command in policy-map-class configuration mode. To disable URL filtering, use the **no** form of this command.

**urlfilter** *parameter-map-name*
**no urlfilter** *parameter-map-name*

## Syntax Description

| | |
|---|---|
| *parameter-map-name* | Name of the parameter map for the URL filter. |

## Command Default

None

## Command Modes

Policy-map-class configuration

## Command History

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

## Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

## Examples

The following example enables Cisco IOS firewall URL filtering:

```
policy-map type inspect p1
 class type inspect c1
  urlfilter param1
```

## Related Commands

| Command | Description |
|---|---|
| **class type inspect** | Specifies the traffic (class) on which an action is to be performed. |
| **policy-map type inspect** | Creates Level 3 and Level 4 inspect type policy maps. |

# url-list

To enter webvpn URL list configuration mode to configure a list of 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 **url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

**url-list** *name*
**no 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 a SSL VPN website is not configured. If the command is not used to attach a URL list to a policy group, then a URL list is not attached to a group policy.

## Command Modes

Webvpn context configuration
Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Entering this command places the router in SSL VPN URL list configuration mode. In this mode, the list of 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 URL list configurations must have unique names.

## Examples

The following example creates a URL list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS

Router(config-webvpn-url)# heading "Quick Links"

Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com

Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

The following example attaches a URL list to a policy group configuration:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS

Router(config-webvpn-url)# heading "Quick Links"
```

```
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com

Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
Router(config-webvpn-url)# exit

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# url-list ACCESS
```

## 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-list | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website. |
| url-text | Adds an entry to a URL list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# url-profile

To specify a URL profile that configures the SDP registrar to run HTTPS, use the **url-profile**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

**url-profile** {**start** *profile-name* | **intro** *profile-name*}
**nourl-profile** {**start** *profile-name* | **intro** *profile-name*}

## Syntax Description

| | |
|---|---|
| **start** | Indicates that a URL profile is to be associated with the Start SDP deployment phase of iPhone deployment. |
| **intro** | indicate that a URL profile is to be associated with the Introduction SDP deployment phase of iPhone deployment. |
| *profile-name* | Specifies the name of a unique URL profile. |

## Command Default

No URL profile is defined for the iPhone deployment.

## Command Modes

Tti-registrar configuration mode (tti-registrar)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)T | This command was introduced. |

## Usage Guidelines

The SDP Registrar is enabled to run HTTPs. It is recommended that the **ip http secure-server** command is issued to enable the HTTPS web server. If a secure server is enabled, then the **ip http secure-trustpoint** command should also be issued. Disable standard HTTP server through the **no ip http server** command (if the standard server is enabled). The specified trustpoint is a registrar local trustpoint appropriate for HTTPS communication between the registrar and the iPhone's browser.

The **url-profile command can use the same or a different URL profile for**the Introduction and Start SDP deployment phases.

## Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

## Related Commands

| Command | Description |
|---|---|
| **crypto provisioning registrar** | Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode. |
| **match url** | Specifies the URL to be associated with the URL profile. |
| **match authentication trustpoint** | Enters the trustpoint name that should be used to authenticate the peer's certificate. |
| **match certificate** | Enters the name of the certificate map used to authorize the peer's certificate. |
| **mime-type** | Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile. |
| **template location** | Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile. |
| **template variable p** | Specifies the value that goes into the OU field of the subject name in the certificate to be issued. |

# validate source-mac

To check the source media access control (MAC) address against the link-layer address, use the **validate source-mac**command in Neighbor Discovery ( ND) inspection policy configuration mode .

**validate source-mac**
**no validate source-mac**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is disabled by default.

## Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration
(config-ra-guard)

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |

## Usage Guidelines

When the router receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. Use the **validate source-mac** command to drop the packet if the link-layer address and the MAC addresses are different from each other.

## Examples

The following example enables the router to drop an ND message whose link-layer address does not match the MAC address:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# validate source-mac
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 nd inspection policy** | Defines the ND inspection policy n ame and enters ND inspection policy configuration mode. |
| **ipv6 nd raguard policy** | Defines the RA guard policy name and enter RA guard policy configuration mode. |

# url-text

To add an entry to a URL list, use the **url-text** command in webvpn URL list configuration mode. To remove the entry from a URL list, use the **no** form of this command.

**url-text** *name* **url-value** *url*
**no url-text** *name* **url-value** *url*

## Syntax Description

| | |
|---|---|
| *name* | Text label for the URL. The label must be inside quotation marks if it contains spaces. |
| **url-value** *url* | An HTTP URL. |

## Command Default

An entry is not added to a URL list.

## Command Modes

Webvpn URL list configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"

Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com

Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

## Related Commands

| Command | Description |
|---|---|
| **url-list** | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website. |

# usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

**usage** *method1* [*method2* [*method3*]]
**no usage** *method1* [*method2* [*method3*]]

## Syntax Description

| | |
|---|---|
| *method1 method2 method3* ]] | Intended use for the certificate; the available options are **ike**, **ssl-client**, and **ssl-server**.<br>You must choose at least one method, and you may choose all three methods. |

## Command Default

**ike**

## Command Modes

Ca-trustpoint configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |

## Usage Guidelines

Before you can issue the usage command, you must enable the **crypto ca trustpoint**command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command may be used as a hint to set or clear key usage or other attributes in the certificate request.

## Examples

The following example shows how to specify the certificate named "frog" for Internet Key Exchange (IKE):

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca trustpoint** | Declares the CA that your router should use. |

# user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user**command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

**user** *username* {**password** | **nthash**} *password* [**group** *group-name* | **mac-auth-only**]
**no user** *username* {**password** | **nthash**} **password** [**group group-name** | **mac-auth-only**]

## Syntax Description

| | |
|---|---|
| *username* | Name of the user that is allowed to authenticate using the local authentication server. |
| **password** | Indicates that the user password will be entered. |
| **nthash** | Indicates that the NT value of the password will be entered. |
| *password* | User password. |
| **group** *group-name* | (Optional) Name of group to which the user will be added. |
| **mac-auth-only** | (Optional) Specifies that the user is allowed to authenticate using only MAC authentication. |

## Command Default

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

## Command Modes

Local RADIUS server 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. |
| 12.2(15)JA | This command was modified to support MAC address authentication on the local authenticator. |
| 12.3(2)JA | This command was modified to support EAP-FAST authentication on the local authenticator. |
| 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

This command is not supported on bridges.

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

## Examples

The following example shows that the user named "user1" has been allowed to authenticate using the local authentication server (using the password "userisok"). This user will be added to the group named "team1".

```
Router(config-radsrv)# user user1 password userisok group team1
```

The following example shows how to add a user to the list of clients allowed to authenticate using MAC-based authentication on the local authenticator.

```
AP(config-radsrv)# user 00074218d01b password 00074218d01b group cashiers
```

## Related Commands

| Command | Description |
|---|---|
| **block count** | Configures the parameters for locking out members of a group to help protect against unauthorized attacks. |
| **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. |
| **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. |
| **vlan** | Specifies a VLAN to be used by members of a user group. |

# user-group

To define a user group for dynamically authenticating and enforcing security policies on a per user basis, use the **user-group**command in identity policy configuration mode. To delete the user-group, use the **no** form of this command.

**user-group** *group-name*
**no user-group** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the user-group. |

## Command Default

None

## Command Modes

Identity policy configuration (config-identity policy)

## Command History

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

## Usage Guidelines

The **user-group** command is used if the Tag and Template method of user-group support is used. The Tag and Template method associates IP addresses with user-groups using locally defined policies. A tag is received from the access control server (ACS), and this tag matches a template (identity policy with defined user-group) on the network access device (NAD).

To use the **user-group** command, you must first enter identity policy configuration mode by using the **identity policy**command. The identity policy defines one or more user-groups, to which source IP addresses are associated.

**Note** Another method of user-group association is available. User-group support can be achieved by configuring the supplicant-group attribute on the ACS.

## Examples

The following example creates the identity policy "auth_proxy_ip" and configures the user-group "auth_proxy_ug":

```
Router(config)# identity policy auth_proxy_ip
Router(config-identity-policy)# user-group auth_proxy_ug
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| identity policy | Creates an identity policy. |

# user-group (parameter-map)

To configure the user group associations for Cloud Web Security content scanning, use the **user-group** command in parameter-map type inspect configuration mode. To disable the user group association, use the **no** form of this command.

**user-group** {*group-name* [**username**] | **exclude** | **include**} *username*
**no user-group** {**name** [**username**] | **exclude** | **include**} *username*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the default user group. |
| **username** | (Optional) Specifies the default username. |
| **exclude** | Excludes the specified user group. |
| **include** | Includes the specified user group. |
| *username* | Username. |

## Command Default

A user group is not configured.

## Command Modes

Parameter-map type inspect configuration (config-profile)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T1 | This command was introduced. |

## Usage Guidelines

Use the *group-name* argument to have the same content scanning policy for all users in a branch office. A prefix of LDAP:// is attached the *group-name* argument when this information is sent to Cloud Web Security to match the configured directory groups.

The **username** keyword is the global username that is sent to Cloud Web Security when there is no content scanning session specific to the configured username.

By default, all the configured user groups of a user are sent to Cloud Web Security. Use the **user-group** command to allow the administrator to filter the user groups sent to Cloud Web Security by configuring the **include** or the **exclude** keywords. When you configure the **include** keyword, only user groups that are in the include list are sent to Cloud Web Security. User groups in the exclude list are filtered from the list of user groups that is sent to Cloud Web Security. The default value for the include list is everything and the exclude list is empty. You can configure multiple instances of include and exclude user groups.

You can configure only one group on an interface. The static user group that is configured on the interface takes precedence over the group name configured in the Cloud Web Security parameter map.

## Examples

The following example shows how to exclude a user group from being sent to Cloud Web Security:

```
Device(config)# parameter-map type cws global
Device(config-profile)# user-group exclude group1
```

**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. |

# user-group logging

To enable user-group syslogs, use the **user-group logging**command in global configuration mode. To disable user-group syslogs, use the **no** form of this command.

**user-group logging** [**group** *group-name*]
**no user-group logging** [**group** *group-name*]

## Syntax Description

| | |
|---|---|
| **group** | (Optional) Configures logging for a specific user group. |
| *group-name* | (Optional) Name of the user-group. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

## Examples

The following example enables syslogs for the user-group "auth_proxy_ug":

```
Router(config)# user-group logging group auth_proxy_ug
```

## Related Commands

| Command | Description |
|---|---|
| **user-group** | Creates a user-group for dynamically authenticating and enforcing security policies on a per user basis |

# username

To establish a username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

**username** *name* [**aaa attribute list** *aaa-list-name*]
**username** *name* [**access-class** *access-list-number*]
**username** *name* [**autocommand** *command*]
**username** *name* [**callback-dialstring** *telephone-number*]
**username** *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]
**username** *name* [**callback-rotary** *rotary-group-number*]
**username** *name* [**dnis**]
**username** *name* [**mac**]
**username** *name* [**nocallback-verify**]
**username** *name* [**noescape**]
**username** *name* [**nohangup**]
**username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*]
**username** *name* [**one-time** {**password** {**0** | **7***password*} | **secret** {**0** | **5***password*}}]
**username** *name* [**password** *secret*]
**username** *name* [**privilege** *level*]
**username** *name* [**secret** {**0** | **5***password*}]
**username** *name* [**user-maxlinks** *number*]
**username** [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
**no username** *name*

## Syntax Description

| | |
|---|---|
| *name* | Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed. |
| **aaa attribute list** *aaa-list-name* | Uses the specified authentication, authorization, and accounting (AAA) method list. |
| **access-class** *access-list-number* | (Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** command available in line configuration mode. It is used for the duration of the user's session. |
| **autocommand** *command* | (Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line. |
| **callback-dialstring** *telephone-number* | (Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device. |
| **callback-line** *line-number* | (Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you enable a specific username for callback. Numbering begins with zero. |

| | |
|---|---|
| *ending-line-number* | (Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as **tty**), then line-number and ending-line-number are absolute rather than relative line numbers. |
| **tty** | (Optional) For asynchronous callback only: standard asynchronous line. |
| **callback-rotary** *rotary-group-number* | (Optional) For asynchronous callback only: permits you to specify a rotary group number on which you want to enable a specific username for callback. The next available line in the rotary group is selected. Range: 1 to 100. |
| **dnis** | Does not require a password when obtained via Dialed Number Identification Service (DNIS). |
| **mac** | Allows a MAC address to be used as the username for MAC filtering done locally. |
| **nocallback-verify** | (Optional) Specifies that the authentication is not required for EXEC callback on the specified line. |
| **noescape** | (Optional) Prevents a user from using an escape character on the host to which that user is connected. |
| **nohangup** | (Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another EXEC prompt. |
| **nopassword** | No password is required for this user to log in. This is usually the most useful keyword to use in combination with the **autocommand** keyword. |
| **password** | Specifies the password to access the *name* argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command. |
| *password* | Password that a user enters. |
| *encryption-type* | Single-digit number that defines whether the text immediately following is encrypted and if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm. |
| *encrypted-password* | Encrypted password that a user enters. |
| **one-time** | Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations. |
| **0** | Specifies that an unencrypted password or secret (depending on the configuration) follows. |
| **7** | Specifies that a hidden password follows. |
| **5** | Specifies that a hidden secret follows. |

| | |
|---|---|
| **secret** | Specifies a secret for the user. |
| *secret* | For Challenge Handshake Authentication Protocol (CHAP) authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated. |
| **privilege** *privilege-level* | (Optional) Sets the privilege level for the user. Range: 1 to 15. |
| **user-maxlinks** *number* | Maximum number of inbound links allowed for a user. |
| **lawful-intercept** | (Optional) Configures lawful intercept users on a Cisco device. |
| *name* | Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed. |
| **view** *view-name* | (Optional) For CLI view only: associates a CLI view name, which is specified with the **parser view** command, with the local AAA database. |
| **password** *password* | Password to access the CLI view. |

## Command Default

No username-based authentication system is established.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 11.1 | This command was modified. The following keywords and arguments were added:<br>• **callback-dialstring** *telephone-number*<br>• **callback-rotary** *rotary-group-number*<br>• **callback-line** [**tty**] *line-number* [*ending-line-number*<br>• **nocallback-verify** |
| 12.3(7)T | This command was modified. The following keywords and arguments were added:<br>• **lawful-intercept**<br>• **view**<br>• *view-name* |

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB:<br>• **lawful-intercept**<br>• **view**<br>• *view-name* |
| 12.2(33)SB | This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SB:<br>• **lawful-intercept**<br>• **view**<br>• *view-name* |
| 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. |
| 12.4 | This command was modified. The following keywords were integrated into Cisco IOS Release 12.4:<br>• **one-time**<br>• **secret**<br>• **0, 5, 7** |
| 15.1(1)S | This command was modified. Support for the **nohangup** keyword was removed from Secure Shell (SSH). |
| Cisco IOS XE Release 3.2SE | This command was modified. The **mac** keyword was added. |

## Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router’s entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for CHAP. Add a username entry for each remote system from which the local router requires authentication.

**Note** To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** entry that has already been assigned to the other router.

- To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).
- Per-user privilege levels override virtual terminal privilege levels.

In Cisco IOS Release 15.1(1)S and later releases, the **nohangup** keyword is not supported with SSH. If the **username** *user* **autocommand** *command-name* command is configured and SSH is used, the session disconnects after executing the configured command once. This behavior with SSH is opposite to the Telnet behavior, where Telnet continuously asks for authentication and keeps executing the command until the user exits Telnet manually.

**CLI and Lawful Intercept Views**

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Simple Network Management Protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If no value is specified for the *secret* argument and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The CHAP debugging information is available using the **debug ppp negotiation , debug serial-interface ,** and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference* .

## Examples

The following example shows how to implement a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example shows how to implement an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of "server_l." It also defines a password for a remote server named "server_r."

```
hostname server_l
username server_r password theirsystem
interface serial 0
```

```
 encapsulation ppp
 ppp authentication chap
```

The following is output from the **show running-config** command displaying the passwords that are encrypted:

```
hostname server_l
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In the following example, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

The following example shows how to remove the username-based authentication for user2:

```
no username user2
```

## Related Commands

| Command | Description |
|---|---|
| **arap callback** | Enables an ARA client to request a callback from an ARA client. |
| **callback forced-wait** | Forces the Cisco IOS software to wait before initiating a callback to a requesting client. |
| **debug ppp negotiation** | Displays PPP packets sent during PPP startup, where PPP options are negotiated. |
| **debug serial-interface** | Displays information about a serial connection failure. |
| **debug serial-packet** | Displays more detailed serial interface debugging information than you can obtain using **debug serial interface** command. |
| **ppp callback (DDR)** | Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests. |
| **ppp callback (PPP client)** | Enables a PPP client to dial into an asynchronous interface and request a callback. |
| **show users** | Displays information about the active lines on the router. |

# username (dot1x credentials)

To specify the username for an 802.1X credentials profile, use the **username** command in dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

**username** *name*
**no username**

## Syntax Description

| | |
|---|---|
| *name* | Name of the credentials profile. |

## Command Default

A username is not specified.

## Command Modes

Dot1x credentials configuration

## Command History

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

## Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

## Examples

The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

## Related Commands

| Command | Description |
|---|---|
| **dot1x credentials** | Specifies an 802.1X credentials profile to be used. |

# username (ips-autoupdate)

To define a username and password in which to access signature files from the server, use the **username**command in IPS-auto-update configuration mode.

**username** *name* **password** *password*

## Syntax Description

| | |
|---|---|
| *name* | Username required to access the latest updated signature file package. |
| **password** *password* | Password required to access the latest updated signature file package. |

## Command Default

The default value is defined in the signature definition XML.

## Command Modes

IPS-auto-update configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, you can optionally issue the **username** command to specify a username and password to access signature files.

## Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration:

```
Router# clock set ?
hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on console.
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml

Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
```

```
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

## Related Commands

| Command | Description |
|---|---|
| **ip ips auto-update** | Enables automatic signature updates for Cisco IOS IPS. |

# username algorithm-type

To set the algorithm type to hash a user password configured using the **username secret** command, use the **username algorithm-type** command in global configuration mode.

**username** *name* **algorithm-type** {**md5** | **scrypt** | **sha256**}

**Syntax Description**

| | |
|---|---|
| **md5** | Selects the message digest algorithm 5 (MD5) as the hashing algorithm. |
| **scrypt** | Selects scrypt as the hashing algorithm. |
| **sha256** | Selects Password-Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, 26-bits (SHA-256) as the hashing algorithm. |

**Command Default**

No algorithm type is established for the username-based authentication system.

**Command Modes**

Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 15.3(3)M | This command was introduced. |
| 15.3(3)S | This command was integrated into the Cisco IOS Release 15.3(3)S. |

**Usage Guidelines**

You must configure the password using the **username secret** command before hashing the password with the **username algorithm-type** command.

Use the **username algorithm-type** command to generate the following types of passwords:

| Command keyword | Type of password |
|---|---|
| md5 | Type 5 |
| sha256 | Type 8 |
| scrypt | Type 9 |

**Note** Type 5, 8, and 9 passwords are not reversible.

If you configure type 8 or type 9 passwords and then downgrade to a release that does not support type 8 and type 9 passwords, you must configure the type 5 passwords before downgrading. If not, you are locked out of the device and a password recovery is required.

**Note** If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

## Examples

The following example shows how to generate a type 8 (PBKDF2 with SHA-256) or a type 9 (SCRYPT) password:

```
Device# configure terminal
Device(config)# enable algorithm-type sha256 secret cisco
Device(config)# enable algorithm-type scrypt secret cisco
Device(config)# end
Device# show running-config | inc username

enable secret 8 $8$dsYGNam3K1SIJO$7nv/35M/qr6t.dVc7UY9zrJDWRVqncHub1PE9UlMQFs
enable secret 9 $9$nhEmQVczB7dqsO$X.HsgL6x1il0RxkOSSvyQYwucySCt7qFm4v7pqCxkKM
```

## Related Commands

| Command | Description |
|---|---|
| **enable algorithm-type** | Sets the algorithm type to hash a user password configured using the **enable secret** command. |
| **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. |
| **username** | Establishes a username-based authentication system. |

# username secret

To encrypt a user password with irreversible encryption, use the **username secret** command in global configuration mode.

**username** *name* **secret** {**0** *password* | **5** *secret-string* | **4** *secret-string* | **8** *secret-string* | **9** *secret-string*}

## Syntax Description

| | |
|---|---|
| *name* | Username. |
| **0** | Specifies an unencrypted secret. |
| *password* | Clear-text password. |
| **5** *secret-string* | message digest alogrithm5 (MD5) encrypted secret text string, which is stored as the encrypted user password. |
| **4** *secret-string* | Secure Hash Algorithm, 26-bits (SHA-256) encrypted secret text string, which is stored as the encrypted user password.<br>**Note**<br>NOTE: Effective with CSCue95644, the **4** keyword is deprecated. |
| **8** *secret-string* | Password-Based Key Derivation Function 2 (PBKDF2) with SHA-256 hashed secret text string, which is stored as the hashed user password. |
| **9** *secret-string* | Scrypt hashed secret text string, which is stored as the hashed user password. |

## Command Default

No username-based authentication system is established.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(18)S | This command was introduced. |
| 12.1(8a)E | This command was integrated into Cisco IOS Release 12.1(8a)E. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 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)S | This command was integrated into Cisco IOS Release 15.0(1)S. Algorithm types **0**, **4**, and **5** were added. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

| Release | Modification |
|---|---|
| 15.3(3)M | This command was modified.<br>• The **4** keyword was deprecated and support for type **8** and type **9** algorithms were added.<br>• The warning message for the type **5** algorithm was removed.<br>• The warning message for removal of support for the type **4** algorithm was added. |
| 15.3(3)S | The command modifications were integrated into Cisco IOS Release 15.3(3)S. |

## Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using non reversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Use this command to enable Enhanced Password Security for the specified, unretrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an “info” username that does not require a password but connects the user to a general-purpose information service.

With CSCue95644, you can use the **username secret** command to configure a username and hash the user password with MD5, PBKDF2 with SHA-256, or scrypt hashing algorithms.



**Note** If you use type 8 or type 9 passwords and then downgrade to an older version of Cisco IOS software that does not support type 8 and type 9 passwords, you must reconfigure the passwords to use type 5 hashing before downgrading. If not, you are locked out of the device and password recovery is required. If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

The **username** command provides username or secret authentication for login purposes only. The *name* argument can be one word only. Spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user.

## Examples

The following example shows how to configure username “abc” and enable MD5 encryption on the clear-text password “xyz”:

```
username abc secret 0 xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

The following example shows how to configure username “xyz” and enter an MD5 encrypted text string that is stored as the username password:

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

The following example shows the sample warning message that is displayed when a user enters the **username secret 4** *encrypted-password* command:

```
Device# configure terminal
Device(config)# username demo secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been
deprecated.
Migrate to a supported password type

Device(config)# end
Device# show running-config | inc username

username demo secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

## Related Commands

| Command | Description |
|---|---|
| **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. |
| **username** | Establishes a username-based authentication system. |
| **username algorithm-type** | Sets the algorithm type to hash a user password configured using the **username secret** command. |

# user-profile location

To store user bookmarks in a directory on a device, use the **user-profile location** command in webvpn context configuration mode. To remove a directory that has been configured, use the **no** form of this command.

**user-profile location device:***directory*
**nouser-profile location device:***directory*

## Syntax Description

| | |
|---|---|
| **device:** | Storage location on a device. See the table below for a list of acceptable storage locations. |
| *directory* | Name of the directory. |

## Command Default

The default location is flash:/webvpn/<context-name>/.

## Command Modes

Webvpn context configuration (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

The table below lists accept storage locations.

***Table 1: Type of Storage Location***

| Type of Storage Location | Description |
|---|---|
| **archive** | Archived file system. |
| **Bootflash** | Bootflash memory. |
| **disk0** | On Disk 0. |
| **disk1** | On Disk 1. |
| **Flash** | Flash memory. |
| **FTP** | FTP network server. |
| **HTTP** | HTTP file server. |
| **HTTPS** | HTTP secure server. |
| **null** | Null destination for copies. You can copy a remote file to null to determine its size. |
| **NVRAM** | Storage location is in NVRAM. |
| **PRAM** | Phase-change memory (PRAM)--type of nonvolatile computer memory. |
| **RCP** | Remote copy protocol network server. |

| Type of Storage Location | Description |
|---|---|
| **SCP** | Secure Copy--A means of securely transferring computer files between a local and a remote host or between two remote hosts using the Secure Shell (SSH) protocol. |
| **slot0** | On Slot 0. |
| **slot1** | On Slot 1. |
| **system** | System memory, including the running configuration. |
| **tmpsys** | Temporary system in a file system. |

## Examples

The following example shows bookmarks are stored in flash on the directory webvpn/sslvpn_context/.

```
Router# webvpn context context1
Router# user-profile location flash:/webvpn/sslvpn_context/
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# variable

To define the next-hop variable in a mitigation parameter map for Transitory Messaging Services (TMS), use the **variable** command in parameter-map configuration mode. To remove the next-hop variable from the mitigation parameter map, use the **no** form of this command.

**Note** Effective with Cisco IOS Release 12.4(20)T, the **variable** command is not available in Cisco IOS software.

**variable** *name* {*number* | **ipv4** *ip-address* | **null0**}
**no variable** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the variable name. |
| *number* | Specifies the number associated with this variable from 0 to 4294967295. |
| **ipv4***ip-address* | Sets the next hop action-variable type to a specific IP address. |
| **null0** | Sets the next hop to interface null 0 (null route). |

## Command Default

The next-hop variable in a mitigation parameter map for TMS is not defined.

## Command Modes

Parameter-map configuration (config-profile)

## 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. |

## Usage Guidelines

The **variable** command is configured to set the next-hop variable in a mitigation type parameter map. The next hop can be configured to route to a null 0 interface (null route) or route to a specific interface for collection and analysis.

**Note** If the next hop is defined in a threat file and as a variable by configuring this command, the next-hop value defined in the threat file will have precedence over the parameter map variable.

## Examples

The following example configures a variable that routes all priority 5 traffic to the null0 interface:

```
Router(config)# class-map type control mitigation match-all MIT_CLASS_2
Router(config-cmap)# match primitive any
Router(config-cmap)# match priority 5
```

```
Router(config-cmap)# exit
Router(config)# parameter-map type mitigation MIT_PAR_2
Router(config-profile)# variable RTBH null0
Router(config-profile)# exit
Router(config)# policy-map type control mitigation MIT_POL_2

Router(config-pmap)# class MIT_CLASS_2
Router(config-pmap-c)# redirect route $RTBH
Router(config-pmap-c)# source parameter MIT_PAR_2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **acl drop** | Configures an ACL drop enforcement action in a TMS Rules Engine configuration. |
| **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 tms** | Configures a TMS type policy map. |
| **redirect route** | Configures a redirect enforcement action in a mitigation type policy map. |
| **source parameter** | Attaches a mitigation type parameter map to a policy-map class configuration. |
| **tms-class** | Associates an interface with an ACL drop enforcement action. |

# view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

**view** *view-name*
**no view** *view-name*

## Syntax Description

| | |
|---|---|
| *view-name* | CLI view that is to be added to the given superview. |

## Command Default

A superview will not contain any CLI views until this command is enabled.

## Command Modes

View configuration (config-view)

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IO 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

Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:

- A password has been configured for the superview (via the **secret 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

## Examples

The following sample output from the **show running-config** command shows that "view_one" and "view_two" have been added to superview "su_view1," and "view_three" and "view_four" have been added to superview "su_view2":

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

**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. |

# virtual-template (IKEv2 profile)

To configure an Internet Key Exchange (IKEv2) profile with a virtual template to be used for cloning the virtual access interfaces, use the **virtual-template** command in IKEv2 profile configuration mode. To remove the virtual template from IKEv2 profile, use the **no** form of this command.

**virtual-template** *template-number* **mode auto**
**no virtual-template** *template-number*

## Syntax Description

| | |
|---|---|
| *template-number* | Identifying number of the virtual template that will be used to clone virtual access interfaces. |
| **mode auto** | Enables auto tunneling mode. |

## Command Default

A virtual template is not specified.

## 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. |
| 15.4(2)T | This command was modified. The **mode auto** keywords were added. |
| Cisco IOS XE Release 3.12S | This command was integrated into Cisco IOS XE Release 3.12S. |

## Usage Guidelines

Use this command to specify the virtual template for cloning a virtual access interface.

Auto tunneling mode eases the configuration and spares you about knowing the responder's details. It automatically applies the tunneling protocol (GRE or IPsec) and transport protocol (IPv4 or IPv6) on the virtual template as soon as the IKE profile creates the virtual access interface.

## Examples

The following example shows how virtual-template 1 is configured for profile1:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# virtual-template 1
```

The following example shows how auto tunneling mode is configured for profile A:

```
Device(config)# crypto ikev2 profile profile A
Device(config-ikev2-profile)# virtual-template 1 mode auto
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ikev2 profile** | Defines an IKEv2 profile. |
| **show ikev2 profile** | Displays the default or user-defined IKEv2 profile. |

# virtual-template (webvpn context)

To associate a virtual template with a Secure Socket Layer Virtual Private Network (SSL VPN) context, use the **virtual-template** command in webvpn context configuration mode. To disable the configuration, use the **no** form of this command.

**virtual-template** *template-number* [**tunnel**]
**no virtual-template**

## Syntax Description

| | |
|---|---|
| *template-number* | Number of the virtual template that will be used to clone virtual access interfaces. The range is from 1 to 1000. |
| **tunnel** | (Optional) Applies the virtual template for every full tunnel session. |

## Command Default

No virtual template is enabled.

## Command Modes

Webvpn context configuration (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 15.1(1)T | This command was modified. The **tunnel** keyword was added. |

## Usage Guidelines

You can configure the desired IP features in the virtual template and then use the **virtual-template** command to apply the configuration on a per-context or per-tunnel basis. The per-context configuration applies the IP features to all the users connecting to that WebVPN context and the per-tunnel configuration applies the IP features for each SSL VPN full tunnel established in the WebVPN context.

## Examples

The following example shows how to associate a virtual template with an SSL VPN context:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# virtual-template 1
```

## Related Commands

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

# vlan (local RADIUS server group)

To specify a VLAN to be used by members of the user group, use the **vlan** command in local RADIUS server group configuration mode. To reset the parameter to the default value, use the **no** form of this command.

**vlan** *vlan*
**no vlan** *vlan*

## Syntax Description

| | |
|---|---|
| *vlan* | VLAN ID. |

## 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 Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200. |
| 12.3(11)T | This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Usage Guidelines

The access point or router moves group members into the VLAN that you specify, overriding any other VLAN assignments. You can assign only one VLAN to a user group.

## Examples

The following example shows that VLAN "225" *is* to be used by members of the user group:

```
vlan 225
```

## Related Commands

| Command | Description |
|---|---|
| **block count** | Configures the parameters for locking out members of a group to help protect against unauthorized attacks. |
| **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. |
| **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. |

| Command | Description |
|---|---|
| **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 group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

**vlan group** *group-name* **vlan-list** *vlan-list*
**no vlan group** *group-name* **vlan-list** *vlan-list*

## Syntax Description

| | |
|---|---|
| *group-name* | VLAN group name. |
| *vlan-list* | VLAN list name. See the "Usage Guidelines" section for additional information about the *vlan-list*argument. |

## Command Default

This command has no default settings.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI1 | This command was introduced. |

## Usage Guidelines

The VLAN group name may contain up to 32 characters and must begin with a letter.

The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

## Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Router(config)# vlan group ganymede vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Router(config)# no vlan group ganymede vlan-list 7
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan group** | Displays the VLANs mapped to VLAN groups. |

# vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute**command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

**vpdn aaa attribute** {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}}
**no vpdn aaa attribute** {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port**}

## Syntax Description

| | |
|---|---|
| **nas-ip-address vpdn-nas** | Enables reporting of the VPDN NAS IP address to the AAA server. |
| **nas-ip-address vpdn-tunnel-client** | Enables reporting of the VPDN tunnel client IP address to the AAA server. |
| **nas-port vpdn-nas** | Enables reporting of the VPDN NAS port to the AAA server. |
| **nas-port physical-channel-id** | Enables reporting of the VPDN NAS port physical channel identifier to the AAA server. |

## Command Default

AAA attributes are not reported to the AAA server.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3NA | This command was introduced. |
| 11.3(8.1)T | This command was integrated into Cisco IOS Release 11.3(8.1)T. |
| 12.1(5)T | This command was modified to support the PPP extended NAS-Port format. |
| 12.2(13)T | The **physical-channel-id** 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(24)T | The **vpdn-tunnel-client** keyword was added. |
| 12.2(33)XND | The **vpdn-tunnel-client** keyword was added. |
| 12.2(33)SRE | The **vpdn-tunnel-client** keyword was added. |
| Cisco IOS XE Release 2.5 | The **vpdn-tunnel-client** keyword was added. |

## Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d**keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-nas** command, the L2TP network server (LNS) reports the IP address of the last multihop node for multihop over Layer 2 Forwarding (L2F). For multihop over Layer 2 Tunneling Protocol (L2TP), the IP address of the originating NAS is reported.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-tunnel-client** command, the LNS reports the IP address of the last multihop node in the RADIUS NAS-IP-Address attribute for the L2TP multihop. This eases the migration for customers moving from L2F to L2TP.



**Note** Reporting of NAS AAA attributes related to a VPDN on a AAA server is not supported for Point-to-Point Tunneling Protocol (PPTP) sessions with multihop deployment.

## Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
vpdn aaa attribute nas-port physical-channel-id
```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
```

```
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.16.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server attribute nas-port format** | Selects the NAS-Port format used for RADIUS accounting features. |

# vrf (ca-trustpoint)

To specify the VRF instance in the public key infrastructure (PKI) trustpoint to be used for enrollment, certificate revocation list (CRL) retrieval, and online certificate status protocol (OCSP) status, use the **vrf** command in ca-trustpoint configuration mode. To remove the VRF instance that was specified, use the **no** form of this command.

**vrf** *vrf-name*
**no vrf** *vrf-name*

## Syntax Description

| | |
|---|---|
| **vrf** *vrf-name* | Specifies the name of the VRF. |

## Command Default

No VRF is specified.

## Command Modes

Ca-trustpoint configuration (ca-trustpoint)

## Command History

| Release | Modification |
|---|---|
| 15.1T | This command was introduced. |

## Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpoint** command with and the *trustpoint-name* argument, which enters ca-trustpoint configuration mode.

## Examples

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# vrf myvrf
```

## Related Commands

| Command | Description |
|---|---|
| **crypto pki trustpoint** | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |

# vrf (ca-trustpool)

To specify the VRF instance in the public key infrastructure (PKI) trustpool to be used for enrolment, certificate revocation list (CRL) retrieval, and online certificate status protocol (OCSP) status, use the **vrf** command in ca-trustpool configuration mode. To remove the VRF instance that was specified, use the **no** form of this command.

**vrf** *vrf-name*
**no vrf** *vrf-name*

## Syntax Description

| | |
|---|---|
| **vrf** *vrf-name* | Specifies the name of the VRF. |

## Command Default

No VRF is specified.

## 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 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.

## Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# vrf myvrf
```

## 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. |

| 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 (isakmp profile)

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf**command in Internet Security Association Key Management (ISAKMP) profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

**vrf** *ivrf*
**no vrf** *ivrf*

## Syntax Description

| | |
|---|---|
| *ivrf* | VRF to which the IPSec tunnel will be mapped. |

## Command Default

The VRF will be the same as the front door VRF (FVRF).

## 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

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

## Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
```

```
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
!
interface Ethernet1/2
 ip address 172.26.1.1 255.255.255.0
 duplex half
 no keepalive
 no cdp enable
 crypto map crypmap
```

# vrfname

To associate a Virtual Private Network (VPN) front-door routing and forwarding instance (FVRF) with a SSL VPN gateway, use the **vrfname** command in webvpn gateway configuration mode. To disassociate the FVRF from the SSL VPN gateway, use the **no** form of this command.

**vrfname** *name*
**no vrfname** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the VRF. |

## Command Default

A VPN FVRF is not associated with a SSL VPN gateway.

## Command Modes

Webvpn gateway (config-webvpn-gateway)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

Only one FVRF can be associated with each SSL VPN context configuration.

## Examples

The following example shows FVRF has been configured:

```
Router (config) ip vrf vrf_1
Router (config-vrf) end
Router (config) webvpn gateway mygateway
Router (config-webvpn-gateway) vrfname vrf_1
Router (cofig-webvpn-gateway) end
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Enters webvpn gateway configuration mode to configure a SSL VPN gateway. |

# vrf-name

To associate a Virtual Private Network (VPN) routing and forwarding instance (VRF) with a SSL VPN context, use the **vrf-name** command in webvpn context configuration mode. To remove the VRF from the WebVPN context configuration, use the **no** form of this command.

**vrf-name** *name*
**no vrf-name**

## Syntax Description

| | |
|---|---|
| *name* | Name of the VRF. |

## Command Default

A VPN VRF is not associated with a SSL VPN context.

## Command Modes

Webvpn context configuration

## Command History

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

## Usage Guidelines

The VRF is first defined in global configuration mode. Only one VRF can be associated with each SSL VPN context configuration.

## Examples

The following example associates a VRF with a SSL VPN context:

```
Router (config)# ip vrf BLUE
Router (config-vrf)# rd 10.100.100.1
Router (config-vrf)# webvpn context context1
Router (config-webvpn-context)# vrf-name BLUE
```

## Related Commands

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

# vsa vendor-id

To define vendor-specific attributes (VSAs), use the **vsa vendor-id** command in server-group configuration mode. To remove the configuration from the list, use the **no** form of this command.

**vsa vendor-id** *vendor-id* **vendor-type** *vendor-type*
**no vsa vendor-id** *vendor-id* **vendor-type** *vendor-type*

## Syntax Description

| | |
|---|---|
| *vendor-id* | Vendor-specific ID. Valid values are from 0 to 65535. |
| **vendor-type** *vendor-type* | Specifies the sub-attribute type for the vendor ID. |

## Command Default

Vendor ID is not defined.

## Command Modes

Server-group configuration (config-radius-attrl)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 12.2(33)SRA | This command was introduced. |

## Usage Guidelines

Vendor-specific ID 9 defines Cisco VSAs and 311 defines Microsoft VSAs. For more information about vendor-specific attributes, see the RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values chapter.

**Note** In Cisco IOS Release 15.1(1)SY, the Microsoft VSAs was defined as 8; however, it was changed to 311 in Cisco IOS Release 15.1(1)SY2.

## Examples

The following example shows how to define vendor-specific attributes:

```
Device(config)# aaa new-model
Device(config)# radius-server attribute list usage-only
Device(config-radius-attrl)# vsa vendor-id  311 vendor-type 11
Device(config-radius-attrl)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **attribute** (**server-group**) | Adds attributes to an accept or reject list. |
| **radius-server host** | Specifies a RADIUS server host. |

# web-agent-url

To configure the Netegrity agent URL to which Single SignOn (SSO) authentication requests will be dispatched, use the **web-agent-url** command in webvpn sso server configuration mode. To remove the Netegrity agent URL, use the **no** form of this command.

**web-agent-url** *url*
**no web-agent-url** *url*

## Syntax Description

| | |
|---|---|
| *url* | URL to which SSO authentication requests will be dispatched. |

## Command Default

Authentication requests will not be dispatched to a Netegrity agent URL.

## Command Modes

Webvpn sso server configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

**Note** A web agent URL and policy server secret key are required for a SSO server configuration. If they are not configured, a warning message is displayed. (See the warning message information in the Examples section below.)

## Examples

The following example shows that SSO authentication requests will be dispatched to the URL http://www.example.com/webvpn/:

```
webvpn context context1
 sso-server test-sso-server
  web-agent-url http://www.example.com/webvpn/
```

### Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

**Related Commands**

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

# webvpn



**Note** Effective with Cisco IOS Release 12.4(6)T, the **webvpn**command is replaced by the **webvpn context** and **webvpn gateway** commands. See the these commands for more information.

To enter Web VPN configuration mode, use the **webvpn** command in global configuration mode. To remove all commands that were entered in Web VPN configuration mode, use the **no** form of this command.

**webvpn**
**no webvpn**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Web VPN configuration mode is not entered.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(6)T | This command was replaced by the **webvpn context** and **webvpn gateway** commands. |

## Examples

The following example shows that Web VPN configuration mode has been entered:

```
Router (config)#
webvpn
Router (config-webvpn)#
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn enable** | Enables WebVPN in the system. |

# webvpn-homepage

To specify the WebVPN home page URL, use the **webvpn-homepage** command in WebVPN group policy configuration mode. To disable the configuration, use the **no** form of this command.

**webvpn-homepage** *homepage-url* [**redirection-time** *seconds*]
**no webvpn-homepage**

## Syntax Description

| | |
|---|---|
| *homepage-url* | Home page URL. |
| **redirection-time** *seconds* | (Optional) Specifies the home page redirection time, in seconds. The range is from 0 to 15. The default value is 5. |

## Command Default

The default reditection time is 5 seconds.

## Command Modes

WebVPN group policy configuration (config-webvpn-group)

## Command History

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

## Usage Guidelines

You can use the **webvpn-homepage** command to specify the WebVPN home page URL and apply the WebVPN redirection time to a particular policy group users. This command helps you to customize and have your own portal page.

The portal page is not displayed if you configure the **webvpn-homepage** command and set the redirection time to 0. If the redirection time is greater than 0, then the portal page is displayed for the time the redirection time is configured and then redirects you to the home page.

If the configuration is not successful, an appropriate error message is displayed.

## Examples

The following example shows how to specify the home page URL "http://192.0.2.0" with the redirection time of 12 seconds:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group policy1
Router(config-webvpn-group)# webvpn-homepage http://192.0.2.0 redirection-time 12
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters WebVPN group policy configuration mode. |
| **show webvpn policy group** | Displays the context configuration associated with a policy group. |
| **webvpn context** | Enters WebVPN context configuration mode. |

# webvpn cef

To enable Secure Socket Layer virtual private network (SSL VPN) full-tunnel Cisco Express Forwarding (CEF) support, use the **webvpn cef** command in global configuration mode. To disable full-tunnel CEF support, use the **no** form of this command.

**webvpn cef**
**no webvpn cef**

## Syntax Description

There are no arguments or keywords.

## Command Default

This command is set by default.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

IP CEF must be turned on before this command can take effect.

## Examples

The following example shows that full-tunnel CEF is being disabled:

```
Router (config)# no webvpn cef
```

## Related Commands

| Command | Description |
|---|---|
| **ip cef** | Enables CEF on the route processor card. |

# webvpn context

To enter webvpn context configuration mode to configure the Secure Sockets Layer Virtual Private Network (SSL VPN) context, use the **webvpn context**command in global configuration mode. To remove the SSL VPN configuration from the router configuration file, use the **no** form of this command.

**webvpn context** *name*
**no webvpn context** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the SSL VPN context configuration. |

## Command Default

Webvpn context configuration mode is not entered, and a SSL VPN context is not configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

The SSL VPN context defines the central configuration of the SSL VPN. Entering the **webvpn context** command places the router in webvpn context configuration mode.

**Note** The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while a SSL VPN gateway is in an enabled state (in service).

## Examples

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# inservice
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication (WebVPN)** | Configures AAA authentication for SSL VPN sessions. |
| **csd enable** | Enables CSD support for SSL VPN sessions. |
| **default-group-policy** | Specifies a default group policy for SSL VPN sessions. |
| **gateway (WebVPN)** | Specifies the gateway for SSL VPN sessions. |
| **inservice** | Enables a SSL VPN gateway or context process. |

| Command | Description |
|---|---|
| **login-message** | Configures a message for a user login text box on the login page. |
| **logo** | Configures a custom logo to be displayed on the login and portal pages of a SSL VPN website. |
| **max-users (WebVPN)** | Limits the number of connections to a SSL VPN that will be permitted |
| **nbns-list** | Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution. |
| **policy group** | Enters a webvpn group policy configuration mode to configure a group policy. |
| **port-forward** | Enters webvpn port-forward list configuration mode to configure a port-forwarding list. |
| **secondary-color** | Configures the color of the secondary title bars on the login and portal pages of a SSL VPN website. |
| **secondary-text-color** | Configures the color of the text on the secondary bars of a SSL VPN website. |
| **title** | Configures the HTML title string that is shown in the browser title and on the title bar of a SSL VPN website. |
| **title-color** | Configures the color of the title bars on the login and portal pages of a SSL VPN website. |
| **url-list** | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website. |
| **vrf-name** | Associates a VRF with a SSL VPN context. |

# webvpn create template

To create templates for multilanguage support for messages initiated by the head-end in a Secure Socket Layer Virtual Private Network (SSL VPN), configure the **webvpn create template** command in user EXEC or privileged EXEC mode.

**webvpn create template**
{**browser-attribute** | **language** | **url-list**}
*device:*

## Syntax Description

| | |
|---|---|
| **browser-attribute** | Creates a template file named "battr_tpl.xml". |
| **language** | Creates a template file named "lang.js". |
| **url-list** | Creates a template file named "url_list_tpl.xml". |
| *device* **:** | Storage device on the system for the templates, such as flash: or disk0. |

## Command Default

Template files are not created.

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |

## Usage Guidelines

After template files have been created, they can be copied to a PC for editing and then reimported to the storage device.

## Examples

The following example shows that a browser-attribute template file is to be created in flash:

```
Router# webvpn create template browser-attribute flash:
```

The following example shows that the language file is to be created in flash:

```
Router# webvpn create template language flash:
```

The following example shows that a URL list template is to be created in flash:

```
Router# webvpn create template url-list flash:
```

## Related Commands

| Command | Description |
|---|---|
| **browser-attribute import** | Imports user-defined browser attributes into a webvpn context. |
| **import** | Imports a user-defined URL list into a webvpn context. |

| Command | Description |
|---|---|
| **language** | Specifies the language to be used in a webvpn context. |
| **url-list** | Enters webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a SSL VPN and attaches the URL list to a policy group. |

# webvpn enable



**Note** Effective with Cisco IOS Release 12.4(6)T, the **webvpn enable**command is replaced by the **inservice**command. See the **inservice** command for more information.

To enable WebVPN in the system, use the **webvpn enable**command in global configuration mode. To disable WebVPN in the system, use the **no** form of this command.

**webvpn enable** [**gateway-addr** *ip-address*]
**no webvpn enable** [**gateway-addr** *ip-address*]

## Syntax Description

| | |
|---|---|
| **gateway-addr** *ip-address* | (Optional) Enables WebVPN on only the IP address that is specified. If this keyword and argument are not configured, WebVPN is enabled globally on all IP addresses. |

## Command Default

WebVPN is disabled in the system.

## Command Modes

Web VPN configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(6)T | This command was replaced by the **inservice** command. |

## Usage Guidelines

This command initializes the required system data structures, initializes TCP sockets, and performs other startup tasks related to WebVPN.

## Examples

The following example shows that WebVPN has been enabled in the system:

```
webvpn enable
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn** | Enters Web VPN configuration mode. |

# webvpn gateway

To enter webvpn gateway configuration mode to configure a SSL VPN gateway, use the **webvpn gateway** command in global configuration mode. To remove the SSL VPN gateway from the router configuration file, use the **no** form of this command.

**webvpn gateway** *name*
**no webvpn gateway** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the virtual gateway service. |

## Command Default

Webvpn gateway configuration mode is not entered, and a SSL VPN gateway is not configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Entering the **webvpn gateway** command places the router in webvpn gateway configuration mode. Configuration settings specific to the SSL VPN gateway are entered in this configuration mode.

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through a secure encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer.

The gateway is configured using an IP address at which SSL VPN remote-user sessions terminate. The gateway is not active until the inservice command has been entered in SSL VPN gateway configuration mode. Only one gateway can be configured in a SSL VPN-enabled network.

## Examples

The following example creates and enables a SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)# ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN

Router(config-webvpn-gateway)# http-redirect 80

Router(config-webvpn-gateway)# inservice
```

## Related Commands

| Command | Description |
|---|---|
| **hostname (WebVPN)** | Configures a SSL VPN hostname. |
| **http-redirect** | Configures HTTP traffic to be carried over HTTPS. |
| **inservice** | Enables a SSL VPN gateway or context process. |

| Command | Description |
|---|---|
| **ip address (WebVPN)** | Configures a proxy IP address on a SSL VPN gateway. |
| **ssl encryption** | Configures the specify the encryption algorithms that the SSL protocol will use for an SSL VPN. |
| **ssl trustpoint** | Configures the certificate trust point on a SSL VPN gateway. |

# webvpn import svc profile

To enable an AnyConnect profile to be imported from a router, use the **webvpn import svc profile** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**webvpn import svc profile** *profile-name device-name*
**no webvpn import svc profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Name of the AnyConnect profile. |
| *device-name* | Device name and filename of the AnyConnect profile thats needs to be imported. |

## Command Default

AnyConnect profiles are not imported to the Cisco IOS headend.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

You can use the **webvpn import svc profile** command to import the AnyConnect profile to the Cisco IOS headend. In order to import the AnyConnect profile to the Cisco IOS headend, the administrator must download the AnyConnect profile from an AnyConnect client (this profile comes by default with AnyConnect), update the profile file to enable the AnyConnect support, and then import the modified profile into the Cisco IOS software.

## Examples

The following example shows how to import the AnyConnect profile to the Cisco IOS headend:

```
Router> enable

Router# configure terminal
Router(config)# webvpn import svc profile profile1 disk0:filename
```

## Related Commands

| Command | Description |
|---|---|
| **svc profile** | Applies a particular AnyConnect profile to the webvpn gateway. |

# webvpn install

To install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client package file to a Secure Socket Layer virtual private network (SSL VPN) gateway for distribution to end users, use the **webvpn install** command in global configuration mode. To remove a package file from the SSL VPN gateway, use the **no** form of this command.

**webvpn install** [**csd** *location-name* | **svc** *location-name* [**sequence** *sequence-number*]]
**no webvpn install** [**csd** *location-name* | **svc** *location-name* [**sequence** *sequence-number*]]

## Syntax Description

| | |
|---|---|
| **csd** *location-name* | (Optional) Installs the CSD client software package. The filename and path are entered. |
| **svc** *location-name* | (Optional) Installs the Cisco AnyConnect VPN Client software package. The filename and path are entered. |
| **sequence** *sequence-number* | (Optional) Allows for multiple packages to be installed to one gateway. If the **sequence**keyword and the *sequence-number*argument are not configured, a sequence number of 1 is applied to the package. |

## Command Default

Neither a CSD nor a Cisco AnyConnect VPN Client package file is installed to a WebVPN gateway.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(20)T | The **sequence** *sequence-number*keyword and argument were added. |

## Usage Guidelines

The 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** Secure Sockets Layer Virtual Private Network (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 to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg

SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example shows how to install the CSD package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg

SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

The following example shows how to install Cisco AnyConnect VPN Client package to an SSL VPN gateway. The file is being copied to a USB file system.

```
Router(config)# webvpn install csd usbflash0:securedesktop-ios-3.1.1.45-k9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

## Related Commands

| Command | Description |
|---|---|
| **show webvpn install status** | Displays the installation status of SVC or CSD client software packages. |

# webvpn sslvpn-vif nat

To enable Network Address Translation (NAT) on the WebVPN virtual interface, use the **webvpn sslvpn-vif nat**command in global configuration mode. To disable NAT on the WebVPN virtual interface, use the **no** form of this command.

**webvpn sslvpn-vif nat** {**enable** | **inside** | **outside**}
**no webvpn sslvpn-vif nat** {**enable** | **inside** | **outside**}

## Syntax Description

| | |
|---|---|
| *enable* | Enables address translation. |
| inside | Enables the inside interface for address translation. |
| outside | Enables the outside interface for address translation. |

## Command Default

NAT is disabled by default on the WebVPN virtual interface.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

Use the show running-config command to verify if NAT has been enabled.

## Examples

The following example shows that NAT has been enabled on the WebVPN virtual interface:

```
Router(config)# webvpn sslvpn-vif nat enable
```

## Related Commands

| Command | Description |
|---|---|
| show running-config | Displays the contents of the current running configuration file. |

# whitelist (cws)

To configure allowed listing of traffic based on the access control list (ACL) and the HTTP header whose header matches the configured regular expression, use the **whitelist** command in Cloud Web Security allowed listing configuration mode. To disable allowed listing of traffic, use the **no** form of this command.

**whitelist** {**acl** {*acl-list extended-acl-list acl-name*} | [**header** | {**host** | **user-agent**} | **user** | **user-group**] **regex** *regex-host* | **notify-tower**}
**no whitelist** {**acl** {*acl-list extended-acl-list acl-name*} | [**header** | {**host** | **user-agent**} | **user** | **user-group**] **regex** *regex-host* | **notify-tower**}

## Syntax Description

| | |
|---|---|
| **acl** | Specifies the ACL. The IP addresses that are used are the pre-NAT IP addresses for matching the access control list. |
| *acl-list* | Access list to create allowed listing of content scanning traffic. Valid values are from 1 to 199. |
| *extended-acl-list* | Extended access list to allowed listing of content-scan traffic. Valid values are from 1300 to 2699. |
| *acl-name* | Access list name. |
| **header** | Specifies the allowed list using the HTTP header. |
| **host** | Specifies the allowed list using the host header field. |
| **user-agent** | Specifies the allowed list using the user agent header field. |
| **user** | Specifies the name of the user whose content appears in the allowed list. |
| **user-group** | Specifies the user-group whose content appears on the allowed list. |
| **regex** | Specifies the HTTP header host, user, and user group values as regular expression (regex). |
| *regex-host* | Name of the host regular expression. |
| **notify-tower** | Specifies the allowed list to notify Cloud Web Security. |

**Command Default**

Allowed listing is not configured.

**Command Modes**

Cloud Web Security allowed listing configuration (config-cws-wl)

**Command History**

| Release | Modification |
|---|---|
| 15.3(3)M | This command was introduced. |
| 15.4(2)T | This command was modified. The **notify-tower** keyword was removed. |

**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 is on the allowed list is not sent for content scanning to Cloud Web Security.

The **header** keyword specifies the allowed listing attribute on the HTTP header that matches the configured regular expression.

The **notify-tower** keyword specifies whether ScanSafe needs to be notified about allowed listing.

**Examples**

The following example shows how to configure allowed listing based on the ACL for Cisco IOS Release 15.3(3)M:

```
Device(config)# content-scan whitelisting
Device(config-cws-wl)# whitelist acl 199
```

The following example shows how to configure whitelisting based on the ACL for Cisco IOS Release 15.4(2)T and later:

```
Device(config)# cws whitelisting
Device(config-cws-wl)# whitelist acl 199
```

**Related Commands**

| Command | Description |
|---|---|
| **content-scan whitelisting** | Enables allowed listing of incoming traffic and enters Cloud Web Security allowed listing configuration mode. |
| **cws whitelisting** | Enables allowed listing of incoming traffic and enters Cloud Web Security allowed listing configuration mode. |

# wins

To specify the primary and secondary Windows Internet Naming Service (WINS) servers, use the **wins**command in ISAKMP group configuration mode or IKEv2 client group configuration mode. To remove this command from your configuration, use the **no** form of this command.

**wins** *primary-server* [*secondary-server*]
**no wins** *primary-server* [*secondary-server*]

## Syntax Description

| | |
|---|---|
| *primary-server* | Name of the primary WINS server. |
| *secondary-server* | (Optional) Name of the secondary WINS server. |

## Command Default

No primary or secondary WINS server is specified.

## Command Modes

ISAKMP group configuration (config-isakmp-group)
IKEv2 client group configuration (config-ikev2-client-config-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. |
| 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 primary and secondary WINS server for the remote access client. You must enable the following commands before enabling the **wins** command:

- **crypto isakmp client configuration group --Specifies the group policy information that has to be defined or changed.**
- **crypto ikev2 authorization policy** --Specifies the local group policy authorization parameters.

## Examples

The following example shows how to define a primary and secondary WINS server for the group "cisco":

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  wins 10.1.1.2 10.1.1.3
```

**Related Commands**

| Command | Description |
|---|---|
| **acl** | Configures split tunneling. |
| **crypto ikev2 authorization policy** | Specifies an IKEv2 client configuration group. |
| **crypto isakmp client configuration group** | Specifies the DNS domain to which a group belongs. |

# wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. To disable the server list, use the **no**form of this command.

**wlccp authentication-server client** {**any** | **eap** | **leap** | **mac**} *list*
**no wlccp authentication-server client** {**any** | **eap** | **leap** | **mac**} *list*

## Syntax Description

| | |
|---|---|
| **any** | Specifies client devices that use any authentication. |
| **eap** | Specifies client devices that use Extensible Authentication Protocol (EAP) authentication. |
| **leap** | Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication. |
| **mac** | Specifies client devices that use MAC-based authentication. |
| *list* | List of client devices. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)JA | This command was introduced. |
| 12.3(11)T | This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Usage Guidelines

You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication).

## Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
Router (config)# wlccp authentication-server client leap leap-list1
```

## Related Commands

| Command | Description |
|---|---|
| **debug wlccp packet** | Displays packet traffic to and from the WDS router. |
| **debug wlccp wds** | Displays either WDS debug state or WDS statistics messages. |
| **show wlccp wds** | Shows information about access points and client devices on the WDS router. |
| **wlccp authentication-server infrastructure** | Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices. |

| Command | Description |
| --- | --- |
| **wlccp wds priority interface** | Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate. |

# wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. To disable the server list, use the **no**form of this command.

**wlccp authentication-server infrastructure** *list*
**no wlccp authentication-server infrastructure** *list*

## Syntax Description

| | |
|---|---|
| *list* | List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)JA | This command was introduced on Cisco Aironet access points. |
| 12.3(11)T | This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Examples

This example shows how to configure the server list for 802.1X authentication for infrastructure devices participating in Cisco Centralized Key Management:

```
Router (config)# wlccp authentication-server infrastructure wlan-list1
```

## Related Commands

| Command | Description |
|---|---|
| **debug wlccp packet** | Displays packet traffic to and from the WDS router. |
| **debug wlccp wds** | Displays either WDS debug state or WDS statistics messages. |
| **show wlccp wds** | Shows information about access points and client devices on the WDS router. |
| **wlccp authentication-server client** | Configures the list of servers to be used for 802.1X authentication. |
| **wlccp wds priority interface** | Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate. |

# wlccp wds priority interface

To configure the router or access point to provide WDS, use the **wlccp wds priority interface**command in global configuration mode. To remove the WDS configuration from the router or access point, use the **no** form of the command .

**wlccp wds priority** *priority* **interface interface**
**no wlccp wds priority** *priority* **interface interface**

## Syntax Description

| | |
|---|---|
| *priority* | Priority of this WDS candidate. The valid range is from 1 to 255. The greater the priority value, the higher the priority. |
| *interface* | Interface on which the router sends out WDS advertisements. Supported interface types are as follows:<br>• For access points--bvi<br>• For wireless-aware routers--bvi, svi, Fast Ethernet, and Gigabit Ethernet. |

## Command Default

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)JA | This command was introduced with support for Cisco Aironet access points. |
| 12.3(11T | This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

## Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS with priority 200:

```
Router (config)# wlccp wds priority 200 interface bvi 1
```

## Related Commands

| Command | Description |
|---|---|
| **debug wlccp packet** | Displays packet traffic to and from the WDS router. |
| **debug wlccp wds** | Displays either WDS debug state or WDS statistics messages. |
| **show wlccp wds** | Shows information about access points and client devices on the WDS router. |
| **wlccp authentication-server client** | Configures the list of servers to be used for 802.1X authentication. |

| Command | Description |
|---|---|
| **wlccp authentication-server infrastructure** | Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices. |

# xauth userid mode

To specify how the Easy VPN client handles extended authentication (Xauth) requests, use the **xauth userid mode**command in Cisco IOS Easy VPN remote configuration mode. To remove the setting, use the **no** form of this command.

**xauth userid mode** {**http-intercept** | **interactive** | **local**}
**no xauth userid mode** {**http-intercept** | **interactive** | **local**}

## Syntax Description

| | |
|---|---|
| **http-intercept** | HTTP connections are intercepted from the user through the inside interface and the prompt. |
| interactive | To authenticate, the user must use the command-line interface (CLI) prompts on the console. Interactive is the default behavior. |
| **local** | The saved username or password is used in the configuration. |

## Command Default

If the command is not configured, the default behavior is interactive.

## Command Modes

Cisco IOS Easy VPN remote configuration (config-crypto-ezvpn)

## 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 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 you want to be prompted by the console, use the **interactive** keyword.

If you want to use a saved username or password, use the **local**keyword. If a local username or password is defined, the mode changes to that username or password.

## Examples

The following example shows that HTTP connections will be intercepted from the user and that the user can authenticate using web-based activation:

```
crypto ipsec client ezvpn tunnel22
  connect manual
  group tunnel22 key 22tunnel
  mode client
  peer 192.168.0.1
  xauth userid mode http-intercept
!
!
interface Ethernet0
  ip address 10.4.23.15 255.0.0.0
  crypto ipsec client ezvpn tunnel22 inside !
interface Ethernet1
  ip address 192.168.0.13 255.255.255.128
```

```
  duplex auto
  crypto ipsec client ezvpn catch22
!
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ipsec client ezvpn** | Creates a Cisco Easy VPN remote configuration. |
| debug crypto ipsec client ezvpn | Displays information about voice control messages that have been captured by the Voice DSP Control Message Logger. |
| debug ip auth-proxy ezvpn | Displays information related to proxy authentication behavior for web-based activation. |
| show crypto ipsec client ezvpn | Displays the Cisco Easy VPN Remote configuration. |
| show ip auth-proxy | Displays the authentication proxy entries or the running authentication proxy configuration. |

# xsm

To enable XML Subscription Manager (XSM) client access to the device, use the **xsm** command in global configuration mode. To disable XSM client access to the device, use the **no** form of this command.

**xsm**
**no xsm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

XSM client access to the device is enabled.

## 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

This command requires that the **ip http server** command is enabled. Enabling the **xsm** command also enables the **xsm vdm** and **xsm edm** commands. This command must be enabled for the XSM client (such as VPN Device Manager [VDM]) to operate.

## Examples

In the following example, access by remote XSM clients to XSM data on the device is disabled:

```
Router# no xsm
```

## Related Commands

| Command | Description |
|---|---|
| **ip http server** | Enables a device to be reconfigured through the Cisco browser interface. |
| **show xsm status** | Displays information and status about clients subscribed to the XSM server. |
| **show xsm xrd-list** | Displays all XRDs for clients subscribed to the XSM server. |
| **xsm dvdm** | Grants access to switch operations. |

| Command | Description |
| --- | --- |
| **xsm edm** | Grants access to EDM monitoring and configuration data. |
| **xsm vdm** | Grants access to VPN-specific monitoring and configuration data. |

# xsm dvdm

To enable switch-specific configuration data (for example, configuring switch ports and VLANs) when running VPN Device Manager (VDM) on a switch, use the **xsm dvdm**command in global configuration mode. To disable switch-specific configuration data for VDM, use the **no** form of this command.

**xsm dvdm**
**no xsm dvdm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Access to switch-specific configuration data is enabled when XSM is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(9)YO1 | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

## Usage Guidelines

Access to switch-specific configuration data (dVDM) is enabled by default when XSM is enabled.

The **no xsm dvdm** command allows you to disable only switch-specific XSM data. Note however that disabling dVDM will prevent the VDM application from communicating properly with the device (switch). There is minimal performance impact associated with leaving dVDM enabled.

## Examples

In the following example, access to switch-specific configuration data is disabled in XSM:

```
Router(config)# no xsm dvdm
```

## Related Commands

| Command | Description |
|---|---|
| **xsm** | Enables XSM client access to the router. |
| **xsm edm** | Grants access to EDM monitoring and configuration data. |
| **xsm history vdm** | Enables specific VPN statistics collection on the XSM server. |
| **xsm vdm** | Grants access to VPN-specific monitoring and configuration data. |

# xsm edm

To grant access to Embedded Device Manager (EDM) monitoring and configuration data, use the **xsm edm**command in global configuration mode. To cancel access to EDM monitoring and configuration data, use the **no** form of this command.

**xsm edm**
**no xsm edm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Access to EDM monitoring and configuration data is granted by default if XSM is enabled.

## 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

This command exists to allow you to disable EDM using the **no xsm edm** form of the command. EDM is enabled by default when XSM is enabled.

EDM provides the following generic information to the VPN Device Manager (VDM):

- Relevant interfaces
- IP routing
- Access-list details
- Basic device health

Note that disabling EDM prevents XSM clients (such as VDM) from working properly and also disables the **xsm history edm**command. There is minimal performance impact associated with leaving EDM enabled.

## Examples

In the following example, access to EDM data is disabled:

```
Router(config)# xsm
```

```
Router(config)# no xsm edm
```

## Related Commands

| Command | Description |
|---|---|
| **xsm** | Enables XSM client access to the router. |
| **xsm dvdm** | Grants access to switch operations. |
| **xsm history edm** | Enables statistics collection for the EDM on the XSM server. |
| **xsm vdm** | Grants access to VPN-specific monitoring and configuration data. |

# xsm history vdm

To enable specific VPN statistics collection on the XML Subscription Manager (XSM) server, use the **xsm history vdm** command in global configuration mode. To disable collection of specific selected VPN statistics on the XSM server, use the **no** form of this command.

**xsm history vdm**
**no xsm history vdm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

VPN statistics collecting is disabled.

## 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

With this command enabled, you can save up to five days of data. Historical information on items such as the number of active IKE tunnels, IPSec tunnels, total crypto throughput, and total throughput is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data. The XSM server does not save history data across reloads.

## Examples

The following example shows how to enable specific VPN statistics collection on the XSM server:

```
Router(config)# xsm

Router(config)# xsm history vdm
```

## Related Commands

| Command | Description |
|---|---|
| **xsm** | Enables XSM client access to the router. |

| Command | Description |
|---|---|
| **xsm history edm** | Enables statistics collection for the EDM on the XSM server. |
| **xsm vdm** | Grants access to VPN-specific monitoring and configuration data. |

# xsm history edm

To enable statistics collection for the Embedded Device Manager (EDM) on the XML Subscription Manager (XSM) server, use the **xsm history edm**command in global configuration mode. To disable statistics collection for the EDM on the XSM server, use the **no** form of this command.

**xsm history edm**
**no xsm history edm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

EDM statistics collection is disabled.

## 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 save up to five days of data. Historical information on items such as RAM and CPU utilization is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data, as the XSM server does not save this data between reloads.

## Examples

In the following example, statistics collection for the EDM is enabled on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history edm
```

## Related Commands

| Command | Description |
|---|---|
| **xsm** | Enables XSM client access to the router. |
| **xsm edm** | Grants access to EDM monitoring and configuration data. |

| Command | Description |
| --- | --- |
| **xsm history vdm** | Enables specific VPN statistics collection on the XSM server. |

# xsm privilege configuration level

To enable the XML Subscription Manager (XSM) configuration privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege configuration level** command in global configuration mode. To remove a previously configured XSM configuration privilege level, use the **no** form of this command.

**xsm privilege configuration level** *number*
**no xsm privilege configuration level** *number*

## Syntax Description

| | |
|---|---|
| *number* | Integer in the range from 1 to 15 that identifies the privilege level. The default is 15. |

## Command Default

The default level is 15.

## 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. |

## Usage Guidelines

The privilege level for the **xsm privilege configuration level**command must be greater than or equal to the privilege level for the **xsm privilege monitor level** command. For example, if the **xsm privilege configuration 7**command is enabled, you need a minimum privilege level of 7 to subscribe to configuration XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.



**Note** The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

## Examples

The following example shows how to set a configuration privilege level of 15, and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

## Related Commands

| Command | Description |
|---|---|
| **privilege** | Configures IOS privilege parameters. |
| **xsm privilege monitor level** | Enables monitor privilege level to subscribe to XRDs. |

# xsm privilege monitor level

To enable the XML Subscription Manager (XSM) monitoring privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege monitor level** command in global configuration mode. To remove a previously configured XSM monitoring privilege level, use the **no** form of this command.

**xsm privilege monitor level** *number*
**no xsm privilege monitor level** *number*

## Syntax Description

| | |
|---|---|
| *number* | Integer in the range from 1 to 15 that identifies the privilege level. The default is 15. |

## Command History

The default is level 1.

## 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. |

## Usage Guidelines

The privilege level for the **xsm privilege monitor level**command must be less than or equal to the privilege level for the **xsm privilege configuration level** command. For example, if the **xsm privilege monitor 7**command is enabled, you need a minimum privilege level of 7 to subscribe to monitor XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.



**Note** The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

## Examples

The following example shows how to set a configuration privilege level of 15 and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

## Related Commands

| Command | Description |
|---|---|
| **privilege** | Configures IOS privilege parameters. |
| **xsm privilege configuration level** | Enables configuration privilege level to subscribe to XRDs. |

# xsm vdm

To grant access to VPN-specific monitoring and configuration data for the VPN Device Manager (VDM), use the **xsm vdm**command in global configuration mode. To cancel access to VPN-specific monitoring and configuration data for VDM, use the **no** form of this command.

**xsm vdm**
**no xsm vdm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled (Access to VPN-specific monitoring and configuration data for the VDM is granted when XSM is enabled.)

## 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. |

## Usage Guidelines

This command enables access to the following VPN-specific information:

- IPSec
- IKE
- Tunneling
- Encryption
- Keys and certificates

If XSM is enabled, this command is enabled by default. Access to VPN-specific monitoring and configuration data within XSM can be disabled by using the **no** form of the command. However, disabling this command will prevent VDM from working properly and will also disable the **xsm history vdm**command. Leaving this command enabled has minimal performance impact.

## Examples

In the following example, access to VPN-specific monitoring and configuration data is disabled:

```
Router(config)# xsm
```

```
Router(config)# no xsm dvm
```

## Related Commands

| Command | Description |
|---|---|
| **xsm** | Enables XSM client access to the router. |
| **xsm dvdm** | Grants access to switch operations. |
| **xsm edm** | Grants access to EDM monitoring and configuration data. |
| **xsm history vdm** | Enables specific VPN statistics collection on the XSM server. |

# zone-member security

To attach an interface to a security zone, use the **zone-member security** command in interface configuration mode. To detach the interface from a zone, use the **no** form of this command.

**zone-member security** *zone-name*
**no zone-member security** *zone-name*

## Syntax Description

| | |
|---|---|
| *zone-name* | Name of the security zone to which an interface is attached. |

## Command Default

None

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)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 **zone-member security** command attaches an interface into a security zone. When an interface is in a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone-pair to which you apply a policy. If the policy permits traffic (via **inspect** or **pass** actions), traffic can flow through the interface.

## Examples

The following example attaches interface GigabitEthernet 0/0/1 to zone z1:

```
Device(config)# interface gigabitethernet 0/0/1
 Device(config-if)# zone-member security z1
```

## Related Commands

| Command | Description |
|---|---|
| **zone security** | Creates a zone. |

# zone-mismatch drop

To validates the zone pair that is attached to an existing session, and allow traffic that matches the zone pair into the network, use the **zone-mismatch drop** command. To disable the configuration, use the **no** form of this command.

**zone-mismatch drop**
**no zone-mismatch drop**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The traffic that do not belong to a zone pair are inspected by the zone-based firewall.

## Command Modes

Parameter map type inspect (config-profile)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.15S | This command was introduced. |
| Cisco IOS 15.5(2)T | This command was implemented on Cisco IOS Release 15.5(2)T. |

## Usage Guidelines

The command allows you to validate the zone pair that is associated with an existing session, and allows traffic that matches the zone pair into the network. When you configure the command, the firewall drops all packets (IPv4 and IPv6) that match an existing session but whose zone pair does not match the zone through which these packets arrive or leave.

When you configure the**zone-mismatch drop** command under the **parameter-map type inspect-global** command, the zone mismatch handling configuration applies to the global firewall configuration. Traffic between all zones are inspected for zone-pair mismatch.

When you configure the**zone-mismatch drop** command under the **parameter-map type inspect** command the zone mismatch handling configuration is applied on a per-policy basis.

When you configure this command, the configuration is effective only for new sessions. For existing sessions, traffic is not dropped if the sessions do not belong to the same zone pair.

## Examples

The following example shows how configure the **zone-mismatch drop** command:

```
Device# configure terminal
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# zone-mismatch drop
Device(config-profile)# end
```

The following example shows how configure the zone mismatch handling configuration for the global firewall configuration:

```
Device# configure terminal
Device(config)# parameter-map type inspect-global
Device(config-profile)# zone-mismatch drop
Device(config-profile)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **parameter-map type inspect** *parameter-map-name* | Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action. |
| **parameter-map type inspect-global** | Configures a global parameter map and enters parameter-map type inspect configuration mode. |

# zone pair security

To create a zone pair, use the **zone-pair security** command in global configuration mode. To delete a zone pair, use the **no** form of this command.

**zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
**no zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}

## Syntax Description

| | |
|---|---|
| *zone-pair-name* | Name of the zone being attached to an interface. |
| **source** *source-zone-name* | Specifies the name of the router from which traffic is originating. |
| **default** | Specifies the name of the default security zone. Interfaces without configured zones belong to the default zone. |
| **destination** *destination-zone-name* | Specifies the name of the device to which traffic is bound. |
| **self** | Specifies the system-defined zone. Indicates whether traffic will be going to or from a device. |

## Command Default

A zone pair is not created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| Cisco IOS XE Release 2.6S | This command was modified. The **default** keyword was added. |
| 15.1(2)T | This command was modified. Support for IPv6 was added. |
| Cisco IOS XE Release 3.9S | This command was modified to define a zone pair and attach a service policy to the zone pair. |

## Usage Guidelines

This command creates a zone pair, which permits a unidirectional firewall policy between a pair of security zones. After you enter this command, you can enter the **service-policy type inspect** command.

If you created only one zone, you can use the system-defined default zone (self) as part of a zone pair. Such a zone pair and its associated policy applies to traffic directed to the router or generated by the router. It does not affect traffic through the router.

You can specify the **self** keyword for the source or destination, but not for both. You cannot modify or remove configuration from the self zone. You can specify the **default** keyword to include all the interfaces that are not configured with any other zones. However, the default zone needs to be defined before it can be used in a zone pair.

## Examples

The following example shows how to create zones z1 and z2, identify them, and create a zone pair where z1 is the source and z2 is the destination:

```
zone security z1
 description finance department networks
zone security z2
 description engineering services network
zone-pair security zp source z1 destination z2
zone-pair security
```

The following example shows how to define zone pair z1-z2 and attach the service policy p1 to the zone pair:

```
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
```

The following example shows how to define a zone pair z1 and z2 and attach the service policy gtp_l4p to the zone pair:

```
zone-pair security clt2srv1 source z1 destination z2
  service-policy type inspect gtp_l4p
interface GigabitEthernet0/0/0
ip address 172.168.0.1 255.255.255.0
zone-member security z1
interface GigabitEthernet0/0/2
ip address 172.168.0.1 255.255.255.0
zone-member security z2
```

The following example shows how the zone pair is configured between system-defined and default zones:

```
zone security default
class-map type inspect match-all tcp-traffic
   match protocol tcp
   match access-group 199
policy-map type inspect p1
   class type inspect tcp-traffic
zone-pair security self-default-zp source self destination default
   service-policy type inspect p1
```

## Related Commands

| Command | Description |
|---|---|
| **zone-member security** | Attaches an interface to a security zone. |
| **zone-pair** | Creates a zone pair. |

# zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

**zone security** {*zone-name* | **default**}
**no zone security** {*zone-name* | **default**}

## Syntax Description

| | |
|---|---|
| *zone-name* | Name of the security zone. You can enter up to 256 alphanumeric characters. |
| **default** | Specifies the name of a default security zone. Interfaces that are not configured on any of the security zones belong to the default zone. |

## Command Default

There is a system-defined "self" zone.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was modified. The **default** keyword was added. |
| 15.1(2)T | Support for IPv6 was added. |

## Usage Guidelines

We recommend that you create at least two security zones so that you can create a zone pair. If you create only one zone, you can use the default system-defined self zone. The self zone cannot be used for traffic going through a router. You can specify the **default**keyword to include all the interfaces that are not configured with any other zones.

To configure an interface to be a member of a security zone, use the **zone-member security** command.

## Examples

The following example shows how to create and describe zones x1 and z1:

```
zone security x1
 description testzonex
zone security z1
 description testzonez
```

The following example shows how to create a default zone:

```
zone security default
 description system level default zone
```

## Related Commands

| Command | Description |
|---|---|
| **description (identify zone)** | Contains a description of a zone. |

| Command | Description |
|---|---|
| **zone-member security** | Attaches an interface to a zone. |
| **zone-pair security** | Creates a zonepair. |