

icmp idle-timeout through ip http ezvpn

- icmp idle-timeout, on page 3
- ida-client server url, on page 4
- identifier, on page 5
- identity local, on page 7
- identity (IKEv2 keyring), on page 9
- identity (IKEv2 profile), on page 11
- identity address ipv4, on page 13
- identity number, on page 14
- identity policy, on page 15
- identity profile, on page 16
- identity profile eapoudp, on page 18
- idle-timeout (WebVPN), on page 19
- if-state nhrp, on page 20
- import, on page 21
- include-local-lan, on page 22
- incoming, on page 24
- initial-contact force, on page 26
- initiate mode, on page 27
- inservice (WebVPN), on page 28
- inspect, on page 29
- inspect (config-profile), on page 31
- integrity, on page 32
- interface (RITE), on page 34
- interface (VASI), on page 36
- interface virtual-template, on page 38
- ip (webvpn url rewrite), on page 41
- ip access-group, on page 42
- ip access-list, on page 44
- ip access-list hardware permit fragments, on page 47
- ip access-list logging interval, on page 49
- ip access-list log-update, on page 50
- ip access-list match-local-traffic, on page 52
- ip access-list resequence, on page 53

- ip access-list logging hash-generation, on page 55
- ip-address (ca-trustpoint), on page 57
- ip address dhcp, on page 59
- ip address (WebVPN), on page 62
- ip admission, on page 64
- ip admission consent banner, on page 67
- ip admission name, on page 69
- ip admission name bypass regex, on page 74
- ip admission name http-basic, on page 75
- ip admission name method-list, on page 77
- ip admission name ntlm, on page 79
- ip admission name order, on page 81
- ip admission proxy http, on page 82
- ip admission virtual-ip, on page 85
- ip audit, on page 86
- ip audit attack, on page 87
- ip audit info, on page 88
- ip audit name, on page 89
- ip audit notify, on page 91
- ip audit po local, on page 92
- ip audit po max-events, on page 93
- ip audit po protected, on page 94
- ip audit po remote, on page 95
- ip audit signature, on page 97
- ip audit smtp, on page 98
- ip auth-proxy (global configuration), on page 99
- ip auth-proxy (interface configuration), on page 101
- ip auth-proxy auth-proxy-banner, on page 102
- ip auth-proxy max-login-attempts, on page 104
- ip auth-proxy name, on page 106
- ip auth-proxy watch-list, on page 109
- ip device tracking probe, on page 111
- ip dhcp client broadcast-flag (interface), on page 112
- ip dhcp support tunnel unicast, on page 113
- ip-extension, on page 114
- ip http ezvpn, on page 118
- ipv6 access-list match-local-traffic, on page 120

icmp idle-timeout

To configure the timeout for Internet Control Message Protocol (ICMP) sessions, use the **icmp idle-timeout** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

icmp idle-timeout *seconds* [**ageout-time** *seconds*]
no icmp idle-timeout

Syntax Description

seconds	ICMP timeout, in seconds. The default is 10. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for ICMP packets. Valid values are from 1 to 2147483.

Command Default

The timeout default is 10 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

When you configure an inspect parameter map, you can enter the **icmp idle-timeout** command after you enter the **parameter-map type inspect** command. For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to specify the ICMP session timeout as 90 seconds:

```
parameter-map type inspect insp-params
 icmp idle-timeout 90
```

The following example shows how to specify the ICMP session aging out time as 50 seconds:

```
parameter-map type inspect insp-params
 icmp idle-timeout 90 ageout 50
```

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.

ida-client server url

To specify the IDA-server url that the IOS IDA client communicates with to download files from the Cisco.com server, use the **ida-client server url** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ida-client server url *url*
no ida-client server url *url*

Syntax Description

url	Specifies the IDA-server url. You must enter the following URL: https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl

Command Default

The default IDA-server URL is: https://www.cisco.com/cgi-bin/ida/locator/locator.pl

Note Do not use the default URL in your configuration.

Command Modes

Global configuration

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)T	This command was modified to include a default IDA-server URL.

Usage Guidelines

Enter the following URL for the **ida-client server url**command to specify the IDA-server URL:

```
Router(config)# ida-client server url
https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl
```

Related Commands

Command	Description
ips signature update cisco	Initiates a one-time download of an IPS signatures from Cisco.com.
upgrade automatic abortversion	Cancels the scheduled reloading of the router with a new Cisco IOS software image.
upgrade automatic getversion	Downloads a Cisco IOS software image directly from www.cisco.com or from a non-Cisco server.
upgrade automatic runversion	Reloads the router with a new Cisco IOS software image.

identifier

To assign a GDOI key server (KS) sender identifier (KSSID) to a KS, use the **identifier** command in GDOI local server configuration mode. To disable a GDOI KS identifier, use the **no** form of this command.

identifier
no identifier

Syntax Description

This command has no arguments or keywords.

Command Default

No KSSIDs are assigned to the KS.

Command Modes

GDOI local server (gdoi-local-server)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command enters GDOI local server ID configuration mode, which contains several subcommands for setting the KSSID:

- **default** (sets the values to their defaults)
- **exit** (saves the KSSID configuration and exits)
- **no** (negates a command)
- **range** *lowest-kssid* - *highest-kssid* (assigns a range of KSSIDs (unique in the entire group))
- **value** *kssid* (assigns a KSSID (unique in the entire group))

Each KS must be assigned at least one KSSID when using GCM or GMAC. The following table shows that the range of KSSIDs available depends on the group size configuration.

Table 1: Ranges of Available KSSIDs Based on Group Size

Configured Group Size	Range of Available KSSIDs
Small (8 bits)	0 to 1
Small (12 bits)	0 to 3
Small (16 bits)	0 to 15
Medium	0 to 127
Large	0 to 511

Each KS must be assigned at least one KSSID when using GCM or GMAC. You can configure a single KSSID, a range of KSSIDs, or both. KSSID values are not assigned to (and usable by) the KS until you exit GDOI local server ID configuration mode.

If you remove KSSIDs that were previously used since the last reinitialization, the group reinitializes (without traffic loss), and KSSIDs that were used will be reset. You are prompted to confirm this before configuring the KSSID set. For example:

```
Device(gdoi-local-server-id)# no value 1
Device(gdoi-local-server-id)# exit

% The following Key Server SIDs being removed were previously used:
%   1
% Removing these KS SIDs will re-initialize the group (without traffic loss).

Are you sure you want to proceed? [yes/no]:
```

If the group is currently reinitializing, removal of KSSIDs that have been previously used since the last reinitialization is denied. For example:

```
Device(gdoi-local-server-id)# no value 0
Device(gdoi-local-server-id)# exit

% Key Server SID Configuration Denied:
%   Please wait for group getvpn to finish re-initialization
%   and try removing used KS SIDs again.
```

If cooperative KSs are configured and the secondary cooperative KS has configured a new group size, but the primary cooperative KS has not changed the group size so that the secondary cooperative KS is using the new group size, entering the **identifier** command on the secondary cooperative KS is denied. For example:

```
Device(gdoi-local-server)# identifier

% Key Server SID Configuration Denied:
%   Need Primary COOP-KS to change Group Size from MEDIUM to LARGE, OR
%   Need Local KS to change Group Size from LARGE to MEDIUM.
```

If cooperative KSs are is configured, the KSSIDs configured on each KS must be unique. No two KSs can have the same KSSID value configured, and if a cooperative KS tries to configure a KSSID that another cooperative KS peer has already assigned to itself, the configuration is denied. For example:

```
Device(gdoi-local-server-id)# range 0-127
Device(gdoi-local-server-id)# end

% Key Server SID Configuration Denied:
%   The following Key Server SIDs being added overlap:
%   0-9, 20-29  (COOP-KS Peer: 10.0.7.1)
%   10-19, 30-39  (COOP-KS Peer: 10.0.9.1)
```

Examples

The following example shows how to configure a single KSSID and a range of KSSIDs. In this example, the **value 0** command allots the pool of SIDs to the KS that begin with KSSID value 0 (meaning that it is allotted the pool of SID values beginning with 0x0 and ending with 0x1FFFF):

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# identifier
Device(gdoi-local-server-id)# range 10 - 20
Device(gdoi-local-server-id)# value 0
Device(gdoi-local-server-id)# end
```

identity local

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the **identity local**command in IKEv2 profile configuration mode. To remove the identity, use the **no** form of this command.

identity local {**address** {*ipv4-addressipv6-address*} | **dn** | **fqdn** *fqdn-string* | **email** *e-mail-string* | **key-id** *opaque-string*}
no identity

Syntax Description

address *{ipv4-address | ipv6-address}*	Uses the IPv4 or IPv6 address as the local identity.
dn	Uses the distinguished name as the local identity.
fqdn *fqdn-string*	Uses the Fully Qualified Domain Name (FQDN) as the local identity.
email *email-string*	Uses the e-mail ID as the local identity.
key-id *opaque-string*	Uses the proprietary type opaque string as the local identity.

Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6). If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.



Note You can configure one local IKEv2 identity type for a profile.

Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
```

```
Router(config-ikev2-profile)# identity local address 10.0.0.1
The following example shows how to specify an IPv6 address as the local IKEv2 identity:
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the **identity**command in IKEv2 keyring peer configuration mode. To remove the identity, use the **no** form of this command.

identity {**address** {*ipv4-addressipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *domain-name*}
no identity {**address** {*ipv4-addressipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address to identify the peer.
fqdn domain *domain-name*	Uses the Fully Qualified Domain Name (FQDN) to identify the peer.
email domain*domain-name*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietary types to identify the peer.

Command Default

Identity types are not specified to a peer.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.3(3)M	This command was modified. The **domain** *domain-name* keyword-argument pair was added.

Usage Guidelines

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an e-mail ID, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session, and the initiator looks up keys during session startup.

Examples

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 or IPv6 address or the range of the peers in an IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

identity (IKEv2 profile)

To specify how the local or remote router identifies itself to the peer and communicates with the peer in the Rivest, Shamir and Adleman (RSA) authentication exchange, use the **identity** command in IKEv2 profile configuration mode. To delete a match, use the **no** form of this command.

identity [**local** {**dn** [**trustpoint** *trustpoint-name* [**serial** *certificate-serial*]] | **address** *ip-address* | **fqdn** *string* | **email** *string*} | **remote** {**dn** [**ou=..., o=...**] | **address** *ip-address* | **fqdn** *string* | **email** *string*}]
no identity [**local** {**dn** [**trustpoint** *trustpoint-name* [**serial** *certificate-serial*]] | **address** *ip-address* | **fqdn** *string* | **email** *string*} | **remote** {**dn** [**ou=..., o=...**] | **address** *ip-address* | **fqdn** *string* | **email** *string*}]

Syntax Description

local	Specifies the local router.
dn	Specifies the distinguished name (DN) of the local or remote router.
trustpoint *trustpoint-name*	(Optional) Specifies the PKI trustpoint name to use with the RSA signature authentication method on the local router.
serial *certificate-serial*	(Optional) Specifies the serial number of the trustpoint certificate on the local router.
address *ip-address*	Specifies the IP address of the remote or local router.
fqdn *fqdn-name*	Specifies the Fully Qualified Domain Name (FQDN) of the remote or local router.
email *e-mail ID*	Specifies the email ID of the remote or local router.
ou= ..., **o=**...	(Optional) Specifies the organizational Unit (OU) field of the subject name in the trustpoint certificate.

Command Default

An identity profile is not specified for a local or remote router regarding the RSA authentication exchange.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)#

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **local**, **dn**, **trustpoint**, **serial**, and **ou=** keywords were added to this command.

Usage Guidelines

Use the **identity** command to identify the local or remote router by its DN, trustpoint, IP address, FQDN, or email address.

Examples

The following example shows how an IKEv2 profile is matched on the remote identity. The following profile caters to peers that identify using **fqdn example.com** and authenticate with **rsa-signature** using **trustpoint-remote**. The local node authenticates with **pre-share** using **keyring-1**.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
match (IKEv2 profile)	Matches a profile on front-door VPN routing and forwarding (FVRF) or local parameters such as IP address or peer identity or peer certificate.
authentication (IKEv2 profile)	Specifies the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile.
keyring (IKEv2 profile)	Specifies a locally defined or accounting, authentication and authorization (AAA) based keyring.
pki trustpoint	Specifies the router to use the PKI trustpoints in the RSA signature authentication.

identity address ipv4

To identify a Group Domain of Interpretation (GDOI) group address, use the **identity address ipv4** command in GDOI group configuration mode. To remove the group address, use the **no** form of this command.

identity address ipv4 *address*
no identity address ipv4 *address*

Syntax Description

address	IP address of the group.

Command Default

A group address is not identified.

Command Modes

GDOI group configuration

Command History

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

Usage Guidelines

This command or the **identity number** command is required for a GDOI configuration.

Examples

The following example shows that the identity address is 10.2.2.2:

```
identity address ipv4 10.2.2.2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group.
identity number	Identifies a GDOI group number.

identity number

To identify a Group Domain of Interpretation (GDOI) group number, use the **identity number** command in GDOI group configuration mode. To remove the group number, use the **no** form of this command.

identity number *number*
no identity number *number*

Syntax Description

number	Number of the group.

Command Default

A GDOI group number is not identified.

Command Modes

GDOI group configuration

Command History

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

Usage Guidelines

This command or the **identity address ipv4** command is required for a GDOI configuration.

Examples

The following example shows the group number is 3333:

```
identity number 3333
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
identity address ipv4	Identifies a GDOI group address.

identity policy

To create an identity policy and to enter identity policy configuration mode, use the **identity policy** command in global configuration mode. To remove the policy, use the **no** form of this command.

identity policy *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url*]
no identity policy *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url*]

Syntax Description

policy-name	Name of the policy.
access-group *group-name*	(Optional) Access list to be applied.
description *line-of-description*	(Optional) Description of the policy.
redirect *url*	(Optional) Redirects clients to a particular URL.

Command Default

An identity policy is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.2(1)E	This command was modified. The **template** keyword was removed.

Usage Guidelines

An identity policy has to be associated with an identity profile.

Examples

The following example shows that an access policy named "policyname2" is being created. The access-group attribute is set to "allow-access". The redirect URL is set to "http://remediate-url.com". This access policy will be associated with a statically authorized device in the identity profile.

```
Device (config)# identity policy policyname2
Device (config-identity-policy)# access-group allow-access
Device (config-identity-policy)# redirect url http://remediate-url.com
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

identity profile

To create an identity profile and to enter identity profile configuration mode, use the **identity profile**command in global configuration mode. To disable an identity profile, use the **no** form of this command.

identity profile {**default** | **dot1x** | **eapoudp** | **auth-proxy**}
no identity profile {**default** | **dot1x** | **eapoudp** | **auth-proxy**}

Syntax Description

default	Service type is default.
dot1x	Service type for 802.1X.
eapoudp	Service type for Extensible Authentication Protocol over UDP (EAPoUDP).
auth-proxy	Service type for authentication proxy.

Command Default

An identity profile is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **eapoudp** keyword was added.
12.4(6)T	The **dot1x** keyword was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **identity profile** command and **default** keyword allow you to configure static MAC addresses of a client computer that does not support 802.1X and to authorize or unauthorize them statically. After you have issued the **identity profile** command and **default** keyword and the router is in identity profile configuration mode, you can specify the configuration of a template that can be used to create the virtual access interface to which unauthenticated supplicants (client computers) will be mapped.

The **identity profile** command and the **dot1x** keyword are used by the supplicant and authenticator. Using the **dot1x** keyword, you can set the username, password, or other identity-related information for an 802.1X authentication.

Using the **identity profile** command and the **eapoudp** keyword, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an identity profile and its description have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity policy eapoudp
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
dot1x max-start	Sets the maximum number of times the authenticator sends an EAP request/identity frame (assuming that no response is received) to the client.
dot1x pae	Sets the PAE type during 802.1X authentication.
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthtication of the specified 802.1X-enabled ports.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
dot1x timeout	Sets retry timeouts.
identity policy	Creates an identity policy.
show dot1x	Displays details for an identity profile.
template (identity profile)	Specifies a virtual template from which commands may be cloned.

identity profile eapoudp

To create an identity profile and to enter Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) profile configuration mode, use the **identity profile eapoudp**command in global configuration mode. To remove the policy, use the **no** form of this command.

identity profile eapoudp
no identity profile eapoudp

Syntax Description

This command has no arguments or keywords.

Command Default

No EAPoUDP identity profile exists.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Using this command, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity profile eapoudp
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

idle-timeout (WebVPN)

Note Effective with Cisco IOS Release 12.4(6)T, the **idle-timeout (WebVPN)** command is not available in Cisco IOS software.

To set the default idle timeout for a Secure Sockets Layer Virtual Private Network (SSLVPN) if no idle timeout has been defined or if the idle timeout is zero (0), use the **idle-timeout** command in Web VPN configuration mode. To revert to the default value, use the **no** form of this command.

idle-timeout [**never***seconds*]
no idle-timeout [**never***seconds*]

Syntax Description

never	(Optional) The idle timeout function is disabled.
seconds	(Optional) Idle timeout in seconds. The values are from 180 seconds (3 minutes) to 86400 seconds (24 hours).

Command Default

If command is not configured, the default idle timeout is 1800 seconds (30 minutes).

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was removed.

Usage Guidelines

Configuring this command prevents stale sessions.

Examples

The following example shows that the idle timeout has been set for 1200 seconds:

```
Router (config)#
webvpn
Router (config-webvpn)# idle-timeout 1200
The following example shows that the idle timeout function is disabled:
Router (config)# webvpn
Router (config-webvpn)# idle-timeout never
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

if-state nhrp

To enable the Next Hop Resolution Protocol (NHRP) to control the state of the tunnel interface, use the **if-state nhrp** command in interface configuration mode. To disable NHRP control of the tunnel interface state, use the **no** form of this command.

if-state nhrp
no if-state nhrp

Syntax Description

This command has no arguments or keywords.

Command Default

NHRP tunnel interface state control is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

If the system detects that one or more of the Next Hop Servers (NHSs) configured on the interface is up, then the tunnel interface state is also declared as ‘up’. If all NHSs configured on the interface are down, then the tunnel interface state is also declared as ‘down’.

The system does not consider NHSs configured with ‘no-reply’ when determining the interface state.

Examples

The following example shows how to enable NHRP control of the tunnel interface state:

```
Router(config)# interface tunnel 1
Router(config-if)# if-state nhrp
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.
show ip nhrp nhs	Displays NHRP NHS information.

import

To import a user-defined URL list into a webvpn context, use the **import** command in the webvpn URL list configuration mode. To disable the URL list, use the **no** form of this command.

import *device* **:** *file*
no import *device* **:** *file*

Syntax Description

device **:** *file*	• *device* **:** *file* --Storage device on the system and the file name. The file name should include the directory location.

Command Default

A user-defined URL list is not imported.

Command Modes

Webvpn URL list configuration (config-webvpn-url)

Command History

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

Usage Guidelines

If this command is used under the **url-list** command, the **url-text** command is not allowed. The **import** command and the **url-list** commands are mutually exclusive when used for a particular URL list. (If you use them together, you will receive this message: "Please remove the imported url-list.")

Also, if a URL list is configured using the **url-text** command, the **import** command is not allowed. (If you use them together, you will receive this message: "Please remove all the URLs before importing a file.")

Examples

The following example shows that the URL list file "test-url.xml" is being imported from flash:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# url-list test
 Router (config-webvpn-url)# import flash:est-url.xml
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

include-local-lan

To configure the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client, use the **include-local-lan** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode or Internet Key Exchange Version 2 (IKEv2) authorization policy configuration mode. To disable the attribute that allows the nonsplit-tunneling connection, use the **no** form of this command.

include-local-lan
no include-local-lan

Syntax Description

This command has no arguments or keywords.

Command Default

A nonsplit-tunneling connection is not able to access the local subnet at the same time as the client.

Command Modes

ISAKMP group configuration (config-isakmp-group)

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

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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 split tunneling is not in use (that is, the SPLIT_INCLUDE attribute was not negotiated), you lose not only Internet access, but also access to resources on the local subnetworks. The Include-Local-LAN attribute allows the server to push the attribute to the client, which allows for a nonsplit-tunneling connection to access the local subnetwork at the same time as the client (that is, the connection is to the subnetwork to which the client is directly attached).

The Include-Local-LAN attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure the Include-Local-LAN attribute, use the **include-local-lan** command.

An example of an attribute-value (AV) pair for the Include-Local-LAN attribute is as follows:

```
ipsec:include-local-lan=1
```

You must enable the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command, which specifies group policy information that has to be defined or changed, before enabling the **include-local-lan** command.

Note The Include-Local-LAN attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.

- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Include-Local-LAN has been configured:

```
crypto isakmp client configuration group cisco
 include-local-lan
```

Related Commands

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

incoming

To configure filtering for incoming IP traffic, use the **incoming** command in router IP traffic export (RITE) configuration mode. To disable filtering for incoming traffic, use the **no** form of this command.

incoming {**access-list** {*standardextendednamed*} | **sample one-in-every** *packet-number*}
no incoming {**access-list** {*standardextendednamed*} | **sample one-in-every** *packet-number*}

Syntax Description

access-list *standard* | *extended named*	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic, not normal router traffic.
sample one-in-every *packet-number*	Exports only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets. By default, all traffic is exported.

Command Default

If this command is not enabled, all incoming IP traffic will be filtered via sampling.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for exporting IP traffic, you can issue the **incoming** command to filter unwanted traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
```

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
outgoing	Configures filtering for outgoing export traffic.

initial-contact force

To process an initial contact notification in Internet Key Exchange Version 2 (IKEv2) IKE_AUTH exchange to an IKEv2 client by deleting unwanted security associations (SAs) and previous IKEv2 sessions, use the **initial-contact force** command in IKEv2 profile configuration mode. To not process the initial contact notification, use the **no** form of this command.

initial-contact force
no initial-contact

Syntax Description

This command has no arguments or keywords.

Command Default

IKEv2 processes the initial contact notification received in an IKE_AUTH exchange after successful authentication and deletes the old IKEv2 SA and IPsec SAs for the same local and remote IKEv2 peer or identity.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Before using the **initial-contact force** command, you must configure the **crypto ikev2 profile** command. Configuring this command in the IKEv2 profile enforces the default behavior of initial contact processing, even if initial contact notification is not received.

Examples

The following example shows how to configure the **initial-contact force** command:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# initial-contact force
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

initiate mode

To configure the Phase 1 mode of an Internet Key Exchange (IKE), use the **initiate mode**command in ISAKMP profile configuration mode. To remove the mode that was config ured, use the **no** form of this command.

initiate mode aggressive
no initiate mode aggressive

Syntax Description

aggressive	Aggressive mode is initiated.

Command Default

IKE initiates main mode.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command if you want to initiate an IKE aggressive mode exchange instead of a main mode exchange.

Examples

The following example shows that aggressive mode has been configured:

```
crypto isakmp profile vpnprofile
 initiate mode aggressive
```

inservice (WebVPN)

To enable a SSL VPN gateway or context process, use the **inservice**command in webvpn gateway configuration or webvpn context configuration mode. To disable a SSL VPN gateway or context process without removing the configuration from the router configuration file, use the **no** form of this command.

inservice
no inservice

Syntax Description

This command has no arguments or keywords.

Command Default

A SSL VPN gateway or context process is not enabled.

Command Modes

Webvpn gateway configuration
Webvpn context configuration

Command History

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

Usage Guidelines

The enable form of this command initializes required system data structures, initializes TCP sockets, and performs other start-up tasks related to the SSL VPN gateway or context process. The gateway and context processes must both be “inservice” to enable SSL VPN.

Examples

The following example enables the SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY

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

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
webvpn context	Enters webvpn configuration mode to configure the SSL VPN context.
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect [*parameter-map-name*]
no inspect[*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of a previously configured inspect parameter map. If you do not specify a parameter map name, the software uses the default values for all the parameters.

Command Default

Cisco IOS stateful packet inspection is disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

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

To enable Cisco IOS stateful packet inspection, enter the name of an inspect parameter map that was previously configured with the **parameter-map type inspect** command.

This command lets you specify the attributes that will be used for the inspection.

Examples

The following example specifies inspection parameters for alert and audit-trail, and requests the **inspect** action with the specified inspect parameter:

```
parameter-map type inspect insp-params
 alert on
 audit-trail on
policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect inspect-params
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

Command	Description
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map.

inspect (config-profile)

To enable Cisco IOS stateful packet inspection, use the **inspect** command in parameter-map type inspect configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect {*parameter-map-name* | **vrf** *vrf-name parameter-map-name*}
no inspect {*parameter-map-name* | **vrf** *vrf-name parameter-map-name*}

Syntax Description

parameter-map-name	Parameter map name.
vrf	Binds a VPN routing and forwarding (VRF) instance to a parameter map.
vrf-name	VRF name.

Command Default

VRF instances are not bound to parameter maps.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-global** command before you can configure the **inspect** command.

Examples

The following example shows how to enable Cisco IOS stateful packet inspection:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect pmap1
```

The following example shows how to bind an inspect-VRF parameter map to the default VRF:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect vrf vrf1 pmap1
```

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map.

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity** command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the **no** form of this command.

integrity *integrity type*
no integrity

Syntax Description

integrity type	Specifies the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5. The integrity algorithms can be one of the following:

Integrity Type	Description
sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm (No longer recommended).
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
sha512	Specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.

Integrity Type	Description
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.

Note You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

Examples

The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# integrity md5
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the Diffie-Hellman group identifier in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

interface (RITE)

To specify the outgoing interface for exporting traffic, use the **interface** command in router IP traffic export (RITE) configuration mode. To disable an interface, use the **no** form of this command.

interface *interface-name*
no interface *interface-name*

Syntax Description

interface-name	Name of interface in which IP packets are exported.

Command Default

If this command is not enabled, the exported IP traffic profile does not recognize an interface in which to send captured IP traffic.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

After you configure an IP traffic export profile via the **ip traffic-export profile** global configuration command, you should issue the **interface** command; otherwise, the profile will be unable to export the captured IP packets. If you do not specify the **interface** command, you will receive a warning, which states that the profile is incomplete, when you attempt to apply the profile to an interface via the **ip traffic-export apply profile** interface configuration command.



Note Currently, only Ethernet and Fast Ethernet interfaces are supported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

interface (VASI)

To configure a virtual routing and forwarding (VRF)-Aware Software Infrastructure (VASI) interface, use the **interface** command in global configuration mode. To remove a VASI configuration, use the **no** form of this command.

interface {**vasileft** | **vasiright**} *number*
no interface {**vasileft** | **vasiright**} *number*

Syntax Description

vasileft	Configures the vasileft interface.
vasiright	Configures the vasiright interface.
number	Identifier of the VASI interface pair. The range is from 1 to 2000.

Command Default

The VASI interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. The *number* argument was modified to accept 500 VASI interface pairs.
Cisco IOS XE Release 3.3S	This command was modified. The *number* argument was modified to accept 1000 VASI interface pairs.
Cisco IOS XE Release 3.10S	This command was modified. The *number* argument was modified to accept 2000 VASI interface pairs.

Usage Guidelines

The vasileft and vasiright interfaces must be configured before the VASI interface becomes active. The two halves of the interface pair must be configured separately. If only one half of the interface is configured and not the other half, then the VASI interface does not become active.

Examples

The following example shows how to configure vasileft and vasiright interfaces:

```
Device(config)# interface vasileft 200
Device(config-if)# vrf forwarding table1
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface vasiright 200
Device(config-if)# vrf forwarding table2
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# exit
```

Related Commands

Command	Description
debug adjacency (VASI)	Displays debugging information for VASI adjacency.
debug interface (VASI)	Displays debugging information for a VASI interface descriptor block.
debug vasi	Displays VASI debugging information.
ip address	Sets a primary or secondary IP address for an interface.
show vasi pair	Displays the status of a VASI pair.
vrf forwarding	Associates a VRF instance or a virtual network with an interface or subinterface.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number* [**type** *virtual-template-type*]
no interface virtual-template *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.
type *virtual-template-type*	(Optional) Specifies the type of virtual template.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's default configuration was modified for SNMP and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Cisco 10000 Series Router

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the **keepalive** command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.
- Disable link-status event messaging using the **no logging event link-status**command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** *number* **subinterface** command.

In Cisco IOS Release 12.2(33)SB, the default configuration for the **virtual-template snmp** command was changed to **no virtual-template snmp**. This prevents large numbers of entries into the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs. If you configure the **no virtual-template snmp** command, the router no longer accepts the **s nmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

Cisco 10000 Series Router

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

Virtual Template with PPP Authentication Example

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

IPsec Virtual Template Example

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol (CDP) on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip (webvpn url rewrite)

To configure the IP address of the site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **ip** command in webvpn url rewrite configuration mode. To deselect the IP address, use the **no** form of this command.

ip *ip-address*
no ip *ip-address*

Syntax Description

ip-address	IP address of the site to be mangled.

Command Default

A site is not selected for mangling.

Command Modes

Webvpn url rewrite (config-webvpn-url-rewrite)

Command History

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

Examples

The following example shows that the IP address 10.1.0.0 255.255.0.0 has been selected for mangling:

```
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 host name 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.

ip access-group

To apply an IP access list or object group access control list (OGACL) to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list or OGACL, use the **no** form of this command.

ip access-group {*access-list-nameaccess-list-number*} {**in** | **out**}
no ip access-group {*access-list-numberaccess-list-name*} {**in** | **out**}

Syntax Description

access-list-name	Name of the existing IP access list or OGACL as specified by an **ip access-list** command.
access-list-number	Number of the existing access list. • Integer from 1 to 199 for a standard or extended IP access list. • Integer from 1300 to 2699 for a standard or extended IP expanded access list.
in	Filters on inbound packets.
out	Filters on outbound packets.

Command Default

An access list is not applied.

Command Modes

Interface configuration (config-if)
Service policy-map configuration (config-service-policymap)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.
12.2(28)SB	This command was made available in service policy-map configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The *access-list-name* keyword was modified to accept the name of an OGACL.
Cisco IOS XE 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

If the specified access list does not exist, all packets are passed (no warning message is issued).

Applying Access Lists to Interfaces

Acc ess lists or OGACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after an interface receives a packet, the Cisco IOS software checks the source address of the packet

against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software continues to process the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an Internet Control Management Protocol (ICMP) host unreachable message.

For standard outbound access lists, after a device receives and routes a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software sends the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you enable outbound access lists or OGACLs, you automatically disable autonomous switching for that interface. When you enable inbound access lists or OGACLs on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception--a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

Applying Access Lists or OGACLs to Service Policy Maps

You can use the **ip access-group** command to configure Intelligent Services Gateway (ISG) per-subscriber firewalls. Per-subscriber firewalls are Cisco IOS IP access lists or OGACLs that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports.

ACLs and OGACLs can be configured in user profiles or service profiles on an authentication, authorization, and accounting (AAA) server or in service policy maps on an ISG. OGACLS or numbered or named IP access lists can be configured on the ISG, or the ACL or OGACL statements can be included in the profile configuration.

When an ACL or OGACL is added to a service, all subscribers of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list { {**standard** | **extended**} {*access-list-nameaccess-list-number*} | **helper egress check**}
no ip access-list { {**standard** | **extended**} {*access-list-nameaccess-list-number*} | **helper egress check**}

Syntax Description

standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list. Required for object-group ACLs.
access-list-name	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access list. • A standard IP access list is in the ranges 1-99 or 1300-1999. • An extended IP access list is in the ranges 100-199 or 2000-2699.
helper egress check	Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.

Command Default

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was modified. Object-group ACLs are now accepted when the **deny** and **permit** commands are used in standard IP access-list configuration mode or extended IP access-list configuration mode.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.
15.0(1)M5	This command was modified. The **helper**, **egress**, and **check** keywords were added.

Release	Modification
15.1(1)SY	This command was modified. The **helper**, **egress**, and **check** keywords were added.
15.1(3)T3	This command was modified. The **helper**, **egress**, and **check** keywords were added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny**and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Named access lists are not compatible with Cisco IOS software releases prior to Release 11.2.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

Examples

The following example defines a standard access list named Internetfilter:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_service_object_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
 my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or in an object-group ACL that will deny packets.
ip access-group	Applies an ACL or an object-group ACL to an interface or a service policy map.
object-group network	Defines network object groups for use in object-group ACLs.
object-group service	Defines service object groups for use in object-group ACLs.
permit	Sets conditions in a named IP access list or in an object-group ACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured.

ip access-list hardware permit fragments

To permit all noninitial fragments in the hardware, use the **ip access-list hardware permit fragments** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip access-list hardware permit fragments
no ip access-list hardware permit fragments

Syntax Description

This command has no arguments or keywords.

Command Default

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was changed to affect all ACLs currently applied to interfaces and not just newly-applied ACLs. See the "Usage Guidelines" section for more information.

Usage Guidelines

Flow fragments that match ACEs with Layer 4 ports and permit results are permitted in the hardware, and all other fragments are dropped. An entry is added in the TCAM for each ACE with Layer 4 ports and permit action. This action could cause large ACLs to not fit in the TCAM. If this is the case, use the **ip access-list hardware permit fragments** command to permit all noninitial fragments in the hardware.



Note Configurations that you modify after you entered the **ip access-list hardware permit fragments** command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the **ip access-list hardware permit fragments** command will not be changed.



Note Hardware configurations that you modify after you entered the **no ip access-list hardware permit fragments** command will return to the default settings. Hardware configurations that you modified before you entered the **no ip access-list hardware permit fragments** command do not change.

The initial flow fragments that match the ACEs with Layer 4 ports and permit results are permitted in the hardware. All other initial fragments are dropped in the hardware.

Catalyst 6500 Series Switches

The following restrictions apply to Cisco IOS releases before Cisco IOS Release 12.2(18)SX5:



Note Configurations that you modify after you entered the **ip access-list hardware permit fragments** command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the **ip access-list hardware permit fragments** command will not be changed.



Note Hardware configurations that you modify after you entered the **no ip access-list hardware permit fragments** command will return to the default settings. Hardware configurations that you modified before you entered the **no ip access-list hardware permit fragments** command do not change.

In Cisco IOS releases after Cisco IOS Release 12.2(18)SX5, this command affects all ACLs currently applied to interfaces and not just newly-applied ACLs.

Examples

This example shows how to permit all noninitial fragments in the hardware:

```
Router(config)# ip access-list hardware permit fragments
```

This example shows how to return to the default settings:

```
Router(config)# no ip access-list hardware permit fragments
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces that are configured for IP.

ip access-list logging interval

To configure the logging interval for access list entries, use the **ip access-list logging interval** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip access-list logging interval *interval*
no ip access-list logging interval

Syntax Description

interval	Access list logging interval, in milliseconds. The range is from 0 to 2147483647.

Command Default

Access list logging intervals are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the access list logging interval to 100 milliseconds:

```
Router# configure terminal
Router(config)# ip access-list logging interval 100
```

Related Commands

Command	Description
ip access-list logging hash-generation	Enables hash-value generation for ACE syslog entries.

ip access-list log-update

To set the threshold number of packets that generate a log message if they match an access list, use the **ip access-list log-update**command in global configuration mode. To remove the threshold, use the **no** form of this command.

ip access-list log-update threshold *number-of-matches*
no ip access-list log-update

Syntax Description

number-of-matches	Threshold number of packets necessary to match an access list before a log message is generated. The range is 0 to 2147483647. There is no default number of matches.

Command Default

Log messages are sent at the first matching packet and at 5-minute intervals after that.

Command Modes

Global configuration

Command History

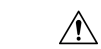
Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Log messages are generated if you have specified the **log** keyword in the **access-list (IP standard)**, **access-list (IP extended)**, **deny (IP)**, **dynamic**, or **permit** command.

Log messages provide information about the packets that are permitted or denied by an access list. By default, log messages appear at the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied, and other information.

By default, the log messages are sent at the first matching packet and after that, identical messages are accumulated for 5-minute intervals, with a single message being sent with the number of packets permitted and denied during that interval. However, you can use the **ip access-list log-update** command to set the number of packets that, when match an access list (and are permitted or denied), cause the system to generate a log message. You might want to do this to receive log messages more frequently than at 5-minute intervals.



Caution If you set the *number-of-matches* argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 is not recommended because the volume of log messages could overwhelm the system.

Even if you use the **ip access-list log-update** command, the 5-minute timer remains in effect, so the cache is emptied at the end of 5 minutes, regardless of the count of messages in the cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it is when a threshold is not specified.

If the syslog server is not directly connected to a LAN that the router shares, any intermediate router might drop the log messages because they are UDP (unreliable) messages.

Examples

The following example enables logging whenever the 1000th packet matches an access list entry:

```
ip access-list log-update threshold 1000
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet is denied by a named IP access list.
dynamic	Defines a named dynamic IP access list.
logging console	Limits messages logged to the console, based on severity.
permit	Sets conditions under which a packet passes a named IP access list.

ip access-list match-local-traffic

To enable Access Control List (ACL) matching for locally generated traffic, use the **ip access-list match-local-traffic** command.

ip access-list match-local-traffic

Syntax Description

This command has no arguments or keywords.

Command Default

Locally generated IPv4 traffic is not filtered by outgoing interface ACLs.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10.7S	This command was introduced.
Cisco IOS XE Release 16.1.1	This command was integrated into Cisco IOS XE Release 16.1.1

Usage Guidelines

By default, an IPv4 Access Control List (ACL) attached to a routed interface in the outgoing direction applies only to transit IPv4 traffic leaving the device. Traffic originating from the device bypasses outgoing ACLs on egress interfaces by default and leaves without being filtered.

To enable outgoing ACLs on routed interfaces to also filter IPv4 traffic originating from the device, use the **ip access-list match-local-traffic** global configuration command. This command causes locally generated IPv4 traffic to be filtered by the outgoing ACL on the egress interface. If no outgoing ACL is applied to the egress interface, locally generated traffic leaving through the interface will not be filtered.



Note The **ip access-list match-local-traffic** command applies globally to all IPv4 traffic originated by the device leaving through any of its routed interfaces. On any routed interface, any attached outgoing IPv4 ACL will apply to all locally generated traffic leaving through that interface.

Examples

The following example shows how to force locally originated IPv4 traffic to be filtered by outgoing IPv4 ACLs on egress interfaces:

```
Router# configure terminal
Router(config)# ip access-list match-local-traffic
```

ip access-list resequence

To apply sequence numbers to the access list entries in an access list, use the **ip access-list resequence** command in global configuration mode.

ip access-list resequence *access-list-name* **starting-sequence-number** *increment*

Syntax Description

access-list-name	Name of the access list. Names cannot contain a space or quotation mark.
starting-sequence-number	Access list entries will be resequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 2147483647.
increment	The number by which the sequence numbers change. The default value is 10. For example, if the increment value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 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 allows the **permit** and **deny** entries of a specified access list to be resequenced with an initial sequence number value determined by the *starting-sequence-number* argument, and continuing in increments determined by the *increment* argument. If the highest sequence number exceeds the maximum possible sequence number, then no sequencing occurs.

For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

```
Exceeded maximum sequence number.
```

If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.

If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.

If the user enters a sequence number that is already present, the following error message is generated:

```
Duplicate sequence number.
```

If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.

Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card (LC) are in synchronization at all times.

Sequence numbers are not saved in NVRAM. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment.

This command works with named standard and extended IP access lists. Because the name of an access list can be designated as a number, numbers are acceptable as names as long as they are entered in named access list configuration mode.

Examples

The following example resequences an access list named kmd1. The starting sequence number is 100, and the increment value is 5:

```
ip access-list resequence kmd1 100 5
```

Related Commands

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

ip access-list logging hash-generation

To enable hash-value generation for access control entry (ACE) syslog entries, use the **ip access-list logging hash-generation** command in global configuration mode. To disable hash value generation, use the **no** form of this command.

ip access-list logging hash-generation
no ip access-list logging hash-generation

Syntax Description

This command has no arguments or keywords.

Command Default

Hash value generation is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Cisco IOS routers generate syslog entries for log-enabled ACEs. The system appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to ACE syslog entries. This tag uniquely identifies the ACE, within an access control list (ACL), that generated the syslog entry.

Use this command to generate an MD5 hash value for all the log enabled ACEs in the system that do not have a user-defined cookie. The system attaches the router-generated hash value to the corresponding ACE. The hash value is stored locally in the router's NVRAM and persists through router reloads.

Examples

The following example shows how to enable hash value generation on the router, for IP access list syslog entries:

```
Router(config)# ip access-list logging hash-generation
Router(config)#
*Aug 7 01:10:12.077: %IPACL-HASHGEN: ACL: 101 seq no : 20 Hash code is 0x75F079
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.

Command	Description
debug ip access-list hash-generation	Displays debugging information about ACL hash generation.
show ip access-list	Displays the contents of all current access lists.

ip-address (ca-trustpoint)

To specify an IPv4 or IPv6 address, or the interface that is included as "unstructuredAddress" in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address {*ip-addressinterface* | **none**}
no ip-address

Syntax Description

ip-address	Specifies the IPv4 or IPv6 address that is included as "unstructuredAddress" in the certificate request.
interface	Specifies an interface, from which the router can get an IP address, that is included as "unstructuredAddress" in the certificate request.
none	Specifies that an IP address is not to be included in the certificate request.

Command Default

An IP address is not configured. You are prompted for the IP address during certificate enrollment.

Command Modes

Ca-trustpoint configuration (config-ca-trustpoint)

Command History

Release	Modification
12.2(8)T	This command was introduced.
15.2(1)T	This command was modified. Support for specifying the IPv6 address that is included as "unstructuredAddress" in the certificate request was added.

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca pki trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip-address** command allows a certificate enrollment parameter to be specified.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you are not prompted for an IP address during certificate enrollment.

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint "my_trustpoint":

```
crypto ca trustpoint my_trustpoint
 enrollment url http://my_trustpoint.cisco.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
```

The following example shows how to include the IPv6 address that is included as "unstructuredAddress" in the certificate request for the trustpoint "my_trustpoint":

```
crypto ca trustpoint my_trustpoint
```

```
 enrollment url http://[2001:DB8:1:1::1]:80/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address 2001:DB8:1:1::1
```

The following example shows that an IPv4 address is not to be included in the certificate request:

```
crypto ca trustpoint my_trustpoint
 enrollment url http://10.3.0.7:80
 fqdn none
 ip-address none
 subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

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

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp**command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]
no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the router. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The **client-id**keyword and *interface-type number*argument were added.
12.2(3)	This command was modified. The **hostname**keyword and *hostname*argument were added. The behavior of the **client-id** *interface-type number*option changed. See the "Usage Guidelines" section for details.
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelines

Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type*is the Ethernet interface where the command is configured and *interface-type number*is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the router. However, you can use the **ip address dhcp hostname** *hostname* command to place a different name in the DHCP option 12 field than the globally configured hostname of the router.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 2: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains “cisco- *mac-address* -Eth1” in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the router in the option 12 field.

Configuration Method	Contents of DISCOVER Messages
ip address dhcp hostname *hostname*	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the router in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- mac-address -Eth1" in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp hostname def
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address (WebVPN)

To configure a proxy IP address on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **ip address**command in webvpn gateway configuration mode. To remove the proxy IP address from the SSL VPN gateway, use the **no** form of this command.

ip address *ip-address* [**port** *port-number*] [**standby** *name*]
no ip address

Syntax Description

ip-address	IPv4 address.
port *port-number*	(Optional) Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument. The default port number 443 is used if this command is configured without entering the **port** keyword.
standby *name*	• (Optional) Indicates that the IP address is a virtual address configured on one of the router interfaces using Hot StandbyRouting Protocol (HSRP). • *name* --Must be the same as the HSRP group name that was configured on the router interface. **Note** Note that the *name* argument is not an optional parameter when the **standby** keyword is used.

Command Default

A proxy IP address is not configured.

Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	The **standby** keyword and *name*arguments were added.

Usage Guidelines

The **ip address** command is used to configure a proxy IP address for an SSL VPN gateway. The IP address is the termination point for all SSL VPN client connections. This IP address can be any routable IP address assigned to a valid interface.

Examples

The following example configures 192.168.1.1 as a proxy address on an SSL VPN gateway. Proxy traffic is directed over port 443.

```
Router(config)# webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)# ip address 192.168.1.1 port 443
```

The following example shows that Router 1 and Router 2 are configured for HSRP on Gateway Webvpn:

Router 1 Configuration

```
Router# configure terminal
Router config)# interface g0/1
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN
```

Router 2 Configuration

```
Router# configure terminal
Router (config)# interface g0/0
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN2
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN2
```

Related Commands

Command	Description
standby name	Configures the name of the standby group.
webvpn gateway	Defines an SSL VPN gateway and enters webvpn gateway configuration mode.

ip admission

To create a Layer 3 network admission control rule to be applied to the interface, or to create a policy that can be applied on an interface when the authentication, authorization and accounting (AAA) server is unreachable, use the **ip admission**command in interface configuration mode. To create a global policy that can be applied on a network access device, use the **ip admission command with the optional keywords**and argument in global configuration mode. To remove the admission control rule, use the **no** form of this command.

ip admission *admission-name* [**absolute-timer** *timeout* | **auth-proxy-audit** | **auth-proxy-banner {file** *file-name* | **http** *http-banner-text***}** | **init-state-time** *time* | **max-login-attempts** *login-attempts* | **name** *authentication-name* | **proxy http{failure page file** *filename* | **page file filename }** | **refresh-all** | **success{page file** *filename* | **redirect** *URL***}}** |**ratelimit** *sessions-limit* | **service-policy type tag** *policy-name* | **source-interface** *interface-type* | **virtual-ip** *ip-address* | **watch-list{add-item** *address* | **enable** | **expiry-time time}}**]
no ip admission *admission-name* [**absolute-timer** *timeout* | **auth-proxy-audit** | **auth-proxy-banner {file** *file-name* | **http** *http-banner-text***}** | **init-state-time** *time* | **max-login-attempts** *login-attempts* | **name** *authentication-name* | **proxy http{failure page file** *filename* | **page file filename }** | **refresh-all** | **success{page file** *filename* | **redirect** *URL***}}** |**ratelimit** *sessions-limit* | **service-policy type tag** *policy-name* | **source-interface** *interface-type* | **virtual-ip** *ip-address* | **watch-list{add-item** *address* | **enable** | **expiry-time time}}**]

Syntax Description

admission-name	Authentication or admission rule name.
absolute-timer	Configures the time in minutes for which the ip admission sessions can exist on the ISR irrespective of transactions. This is applicable for all the ip admission rules configured on the ISR.
auth-proxy-audit	Enables auditing for Authentication Proxy.
auth-proxy-banner	Configures banner for Authentication Proxy Login Page through file or text
consent-banner	Configures banner for Authentication Proxy Consent Page through file or text.
event	Specifiy an authentication policy to be applied to ip admission sessions when the AAA server is unreachable.
http	Specify number of http processes ranging from 1 to 16
inactivity-timer	Configures the time in minutes for which the ip admission sessions can exist on the ISR without any transactions. This is applicable for all the ip admission rules configured on the ISR
init-state-time	Configures the time in minutes for which the ip admission sessions can exist on the ISR until authentication is succeeded. This is applicable for all the ip admission rules configured on the ISR.
max-http-conns	Configures maximum number of HTTP connections per client ranging from 1 to 200
max-login-attempts	Configures maximum login attempts that are required before an ip admission session is moved to failed state.

max-nodata-conns	Configures maximum TCP NODATA Connections to be allowed ranging from 1 to 1000
max-nodata-conns	Configures an Authentication Proxy Rule
proxy	Configures various pages for Authentication Proxy
ratelimit	Configures session ratelimit ranging from 100 to 1000
service-policy	Associates a tag based service-policy to ip admission
source-interface	Specify source interface for ip admission
virtual-ip	Configure web-based proxy authentication virtual IP address
ratelimit	Configures session ratelimit ranging from 100 to 1000
watch-list	Enables and configures ip admission watch-list functionality.

Command Default

A network admission control rule is not applied to the interface.

Command Modes

Interface configuration (config-if)
Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified to include the **event timeout aaa policy identity** keywords and the *identity-policy-name* argument.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The admission rule defines how you apply admission control.

The optional keywords and argument define the network admission policy to be applied to a network access device or an interface when no AAA server is reachable. The command can be used to associate a default identity policy with Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions.

From the Cisco IOS XE Release 16.x, the IP admission feature is not supported on the Cisco ISR platforms.

Examples

The following example shows how to apply a network admission control rule named "nacrule1" to the interface:

```
Router (config-if)# ip admission nacrule1
```

The following example shows how to apply an identity policy named "example" to the device when the AAA server is unreachable:

```
Router (config)# ip admission nacrule1 event timeout aaa policy identity example
```

Related Commands

Command	Description
interface	Defines an interface.

ip admission consent banner

To display a banner on the authentication proxy consent webpage, use the **ip admission consent banner** command in global configuration mode. To disable the display of the banner, use the **no** form of this command.

ip admission consent banner {**file** *file-name* | **text** *banner-text*}
no ip admission consent banner

Syntax Description

file *file-name*	Specifies a file that is to be shown as the consent webpage.
text *banner-text*	Specifies a text string to replace the default banner, which is the name of the router. The text string must be in the following format: "C *banner-text* C," where "C" is a delimiting character.

Command Default

A banner is not displayed on the authentication proxy consent webpage.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release 12.4(15)T	This command was introduced.

Usage Guidelines

Use this command to configure one of the following two scenarios:

- The **ip admission consent banner** command is configured using a filename.

In this scenario, the administrator provides the location and name of the file that is to be used for the consent web page.

- The **ip admission consent banner** command is configured using a banner text.

In this scenario, the administrator provides a multiline text that is converted into HTML. Only the multiline text is displayed on the authentication proxy login page.

Note If the **ip admission consent banner**command is not enabled, nothing is displayed to the user on the consent login page, except two text boxes to enter the username and password, respectively.

Note When HTTP authentication proxy is configured along with the IOS Consent feature, any HTTP authentication proxy-related configurations or policies will override the consent page-related configurations or policies. For example, if the **ip admission name** *admission-name* **consent** command is configured, the **ip admission consent banner** command is ignored, and only the banner that is configured by the **ip admission auth-proxy-banner** command is displayed.

Examples

The following example shows how to display the file "consent_page.html" located in flash:

```
Device(config)# ip admission consent-banner file flash:consent_page.html
```

The following example shows how to specify the custom banner “Consent-Page-Banner-Text” to be displayed in the authentication proxy consent webpage:

```
Device(config)# ip admission consent-banner text ^C Consent-Page-Banner-Text ^C
```

Related Commands

Command	Description
ip auth-proxy auth-proxy-banner	Displays a banner, such as the router name, in the authentication proxy login page.

ip admission name

To create an IP network admission control rule, use the **ip admission name**command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** *service-policy-name*] [**list** {*aclacl-name*}] [**event**] [**timeout aaa**] [**policy identity identity-policy-name**]
no ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** *service-policy-name*] [**list** {*aclacl-name*}] [**event**] [**timeout aaa**] [**policy identity identity-policy-name**]

Syntax for Authentication Proxy Consent Webpage
ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*aclacl-name*}] [**parameter-map** *consent-parameter-map-name*]]
no ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*aclacl-name*}] [**parameter-map** *consent-parameter-map-name*]]

Syntax Description

admission-name	Name of network admission control rule.
eapoudp	(Optional) Specifies IP network admission control using Extensible Authentication Protocol over UDP (EAPoUDP).
bypass	(Optional) Admission rule bypasses EAPoUDP communication.
proxy	(Optional) Specifies authentication proxy.
ftp	Specifies that FTP is to be used to trigger the authentication proxy.
http	Specifies that HTTP is to be used to trigger authentication proxy.
telnet	Specified that Telnet is to be used to trigger authentication proxy.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag** {*policy name*} command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
acl-name	Applies a named access list to a named admission control rule.
event	(Optional) Identifies the condition that triggered the application of the policy.
timeout aaa	(Optional) Specifies that the AAA server is unreachable.

policy identity	Configures the application of an identity policy to be used while the AAA server is unreachable.
identity -policy -name	Specifies the identity policy to apply.
consent	Associates an authentication proxy consent webpage with the IP admission rule specified via the *admission-name* argument.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
parameter-map	(Optional) A parameter map policy is to be associated with consent profile.
consent-parameter-map-name	Specifies the consent profile parameters to apply.

Command Default

An IP network admission control rule is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **bypass** and **service-policy type tag** keywords and *service-policy-name* argument were added.
12.4(11)T	The **event**, **timeout aaa**, and **policy identity** keywords and the *identity -policy -name argument were added.*
12.4(15)T	The following keywords and arguments were added: **consent**, **absolute-timer ,** *minutes*, **inactivity-time**, *minutes*, **parameter-map**, and *consent-parameter-map-name*.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **bypass** keyword allows an administrator the choice of not having to use the EAPoUDP-based posture validation for the hosts that are trying to connect on the port. The bypass can be used if an administrator knows that the hosts that are connected on the port do not have the Cisco Trust Agent client installed.

The **service-policy type tag** {*service-policy-name*} keywords and argument allow you to associate the service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

The **event** keyword option allows you to specify the condition that triggered application of an identity policy.

The **timeout aaa** keyword option specifies that the AAA server is unreachable, and this condition is triggering the application of an identity policy.

The **policy identity** keyword and the *identity -policy -name argument* allow you to configure application of an identity policy and specify the policy type to be applied while the AAA server is unreachable.

The **consent** keyword and the **parameter-map** *consent-parameter-map-name* keyword and argument allow you to associate the authentication proxy consent feature with an IP admission rule. The consent feature enables customers to display a consent webpage to an end user, providing access to wireless services only after the end user accepts the agreement.

Examples

Tag and Template Feature Examples

The following example shows that an IP admission control rule is named "greentree" and that it is associated with ACL "101." Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

The following example shows that EAPoUDP bypass has been configured:

```
Router (config)# ip admission name greentree eapoudp bypass list 101
```

In the following service policy example, tags named "healthy" and "non_healthy" can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name "greentree."

Class Map Definition for the healthy class Type Tag

```
Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Class Map Definition for the non_healthy_class Type Tag

```
Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end
```

Policy Map Definition

```
! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
```

```
! The following line refers to the healthy class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router(config-pmap-c)# exit
The following line refers to the non_healthy class that was defined above.
Router (config-pmap)# class non_healthy_class
Router(config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end
```

Identity Policy Definition

```
Router (config)# identity policy healthy_policy
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy

Router (config-identity-policy)# end
```

Defining Access Lists

```
Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nac)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from
 accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nac)# end
```

Associating the Policy Map with the IP Admission Name

```
Router (config)# ip admission name greentree service-policy type tag global_class

! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree
```

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

NAC--Auth Fail Open Feature Examples

The following example shows how to define an IP admission control rule named "samplerule" and attach it to a specific interface:

```
Router (config)# ip admission name samplerule eapoudp list 101 event timeout aaa policy
identity aaa_fail_policy
```

Router (config)# **interface fastethernet 1/1**

Router (config-if)# **ip admission samplerule**

Router (config-if)# **end**

In the above configuration, if the specified interface is not already authorized when the AAA server becomes unreachable, it will operate under the specified policy until revalidation is possible.

Authentication Proxy Consent Webpage Example

The following example shows how to configure an IP admission consent rule and associate the consent rule with the definitions of the parameter map "consent_parameter_map":

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 parameter-map
 consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
 ip access-group 102 in
 ip admission consent-rule
 no shut
 exit
!
interface FastEthernet 0/1
 description ### AAA-DHCP-AUDIT-SERVER-N/W ###
 ip address 192.168.104.170 255.255.255.0
 no shut
 exit
!
line con 0
 exec-timeout 0 0
 login authentication noAAA
 exit
!
line vty 0 15
 exec-timeout 0 0
 login authentication noAAA
 exit
```

!

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name bypass regex

To configure browser-based authentication bypass on a Network Admission Control (NAC) rule, use the **ip admission name bypass regex** command in global configuration mode. To remove browser-based authentication bypass, use the **no** form of this command.

ip admission name *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*]

no ip admission name *admission-name* **bypass**

Syntax Description

admission-name	Name of a NAC rule.
regex-map	Regular expression (regex) parameter map with a regex pattern to enable bypass authentication for a web browser.
absolute-timer *minutes*	(Optional) Specifies the maximum time, in minutes, before a browser session times out. The maximum time ranges from 0 to 35791. Default value for an authentication session is 0. Default value for an authentication bypass session is 60.

Command Default

Authentication is required for all browsers.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

The **bypass regex** *regex-map* keyword and argument configures a regex pattern that can be compared to the user-agent field in the HTTP Get request to bypass authentication for a configured browser. This command defines the NAC policy to be applied to a network access device to bypass browser authentication.

The following example shows how to bypass browser authentication:

```
Device> enable
Device# configure terminal
Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10
```

ip admission name http-basic

To create a basic HTTP authentication network admission control rule, use the **ip admission name http-basic** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* **http-basic** [**passive**] [**absolute-timer** *minutes*] [**event timeout aaa policy identity** *identity-policy-name*] [**inactivity-time** *minutes*] [**list** {*acl-list extended-acl-list acl-name*}] [**service-policy type tag** *service-policy-name*]
no ip admission name *admission-name* **http-basic**

Syntax Description

admission-name	Name of the network admission control rule.
passive	(Optional) Specifies passive mode.
absolute-timer *minutes*	(Optional) Specifies the elapsed time, in minutes, before the external server time out. Valid values are from 0 to 35791. The default is 0.
event	(Optional) Specifies the event to be associated with a policy.
timeout	(Optional) Specifies timeout-based events.
aaa	(Optional) Specifies that the authentication, authorization, and accounting (AAA) server is unreachable.
policy identity	(Optional) Applies an identity policy to be used while the AAA server is unreachable.
identity-policy-name	(Optional) Name of the identity policy to be applied.
inactivity-time *minutes*	(Optional) Specifies the lapsed time, in minutes, before the external file server is deemed unreachable. Valid values are from 1 to 35791.
list	(Optional) Specifies an access control list (ACL) to apply to an authentication proxy.
acl-list	(Optional) Standard ACL number. Valid values are from 1 to 199.
extended-acl-list	(Optional) Expanded range of ACL numbers. Valid values are from 1300 to 2699.
acl-name	(Optional) ACL name.
service-policy	(Optional) Specifies a control plane service policy is to be configured.
type	(Optional) Specifies the type of the service policy.
tag	(Optional) Specifies the tag-based service policy type.
service-policy-name	(Optional) Name of the control plane service policy. This service policy is used to apply actions on the host when a tag is received.

Command Default

A basic HTTP authentication network admission control rule is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you configure the **ip admission name http-basic** command, client applications always prompt users to enter their credentials.

The absolute timeout value allows you to configure a time duration during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. The absolute timeout value can be configured per protocol or globally. The default value of the absolute timeout is zero. Hence the absolute timer is disabled by default and the authentication proxy is enabled indefinitely.

The **timeout aaa** keywords specify that the AAA server is unreachable, and this condition triggers the application of an identity policy.

The **service-policy type tag** *service-policy-name* keywords and argument allow you to associate a service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

Examples

The following example shows how to configure a basic HTTP network admission control rule:

```
Router(config)# ip admission name admission1 http-basic
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name method-list

To create a list of authentication, authorization, and accounting(AAA) method network admission control rules, use the **ip admission name method-list** command in global configuration mode. To remove the network admission control rules, use the **no** form of this command.

ip admission name *admission-name* **method-list** [**accounting**] [**authentication**] [**authorization**] {*list-name* | **default**}
no ip admission name *admission-name* **method-list**

Syntax Description

admission-name	Name of the network admission control rule.
accounting	(Optional) Specifies the accounting method.
authentication	(Optional) Specifies the authentication method.
authorization	(Optional) Specifies the authorization method.
list-name	Method list name.
default	Specifies the default method list.

Command Default

A list of AAA method network admission control rules is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **ip admission name method-list accounting** command defines the reference to the accounting method list of service type auth-proxy or the network that is configured using the **aaa accounting auth-proxy** and **aaa accounting network** commands respectively.

The **ip admission name method-list authentication** command defines the reference to the authentication method list of service type login that is configured using the **aaa authentication login** command.

The **ip admission name method-list authorization** command defines the reference to the authorization method list of service type auth-proxy or the network that is configured using the **aaa authorization auth-proxy** and **aaa authorization network** commands respectively.

Examples

The following example shows how to create an accounting method network admission control rule:

```
Router(config)# ip admission name admission1 method-list accounting accounting-method
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication login	Sets AAA authentication at login.
aaa authorization network	Sets the parameters that restrict user access to a network.
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name ntlm

To create a Windows network, NT LAN Manager (NTLM) authentication network admission control rule, use the **ip admission name ntlm** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* **ntlm** [**absolute-timer** *minutes*] [**event timeout aaa policy identity** *identity-policy-name*] [**list** {*acl-list* *extended-acl-list acl-name*}] [**service-policy type tag** *service-policy-name*]
no ip admission name *admission-name* **ntlm**

Syntax Description

admission-name	Name of the network admission control rule.
absolute-timer *minutes*	(Optional) Specifies the elapsed time, in minutes, before the external server times out. Valid values are from 0 to 35791.
event	(Optional) Specifies the event to be associated with a policy.
timeout	(Optional) Specifies timeout-based events.
aaa	(Optional) Specifies that the authentication, authorization, and accounting (AAA) server is unreachable.
policy identity	(Optional) Applies an identity policy to be used while the AAA server is unreachable.
identity-policy-name	(Optional) Name of the identity policy to be applied.
list	(Optional) Specifies an access control list (ACL) to apply to an authentication proxy.
acl-list	(Optional) Standard ACL number. Valid values are from 1 to 199.
extended-acl-list	(Optional) Expanded range of ACL numbers. Valid values are from 1300 to 2699.
acl-name	(Optional) ACL name.
service-policy	(Optional) Specifies a control plane service policy is to be configured.
type	(Optional) Specifies the type of the service policy.
tag	(Optional) Specifies the tag-based service policy type.
service-policy-name	(Optional) Name of the control plane service policy. This service policy is used to apply actions on the host when a tag is received.

Command Default

An NTLM Authentication network admission control rule is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you use the NTLM authentication method, the router tries to retrieve the user credentials transparently from the client application without prompting end users. If the client application cannot send user credentials transparently, it prompts users to enter their username and password.

The absolute timeout value allows you to configure a time duration during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. The absolute timeout value can be configured per protocol or globally. The default value of the absolute timeout is zero. Hence the absolute timer is disabled by default and the authentication proxy is enabled indefinitely.

The **timeout aaa** keyword specifies that the AAA server is unreachable, and this condition triggers the application of an identity policy.

The **service-policy type tag** *service-policy-name* keywords and argument allow you to associate a service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

Examples

The following example shows how to create an NTLM network admission control rule:

```
Router(config)# ip admission name admission1 ntlm
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name order

To create a fallback authentication order for the network admission control rule, use the **ip admission name order** command in global configuration mode. To remove the authentication order for the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* **order** [**http-basic**] [**ntlm**] [**proxy-http**]
ip admission name *admission-name* **order**

Syntax Description

admission-name	Name of the network admission control rule.
http-basic	(Optional) Specifies HTTP basic authentication.
ntlm	(Optional) Specifies Windows network, NT LAN Manager (NTLM) authentication.
proxy-http	(Optional) Specifies proxy HTTP authentication.

Command Default

A fallback authentication order for the network admission control rule is not configured.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example shows how to create an authentication order for a network admission control rule:

```
Router(config)# ip admission name admission1 order http-basic
```

Related Commands

Command	Description
ip admission name	Creates an authentication network admission control rule.
ip admission name http-basic	Creates a basic HTTP authentication network admission control rule.
ip admission name ntlm	Creates an NTLM authentication network admission control rule.

ip admission proxy http

To specify the display of custom authentication proxy web pages during web-based authentication, use the **ip admission proxy http** command in global configuration mode. To specify the use of the default web page, use the **no** form of this command.

ip admission proxy http { {**login** | **success** | **failure** | **login expired**} **page file** *device:file-name* | **success redirect** *url*}
no ip admission proxy http { {**login** | **success** | **failure** | **login expired**} **page file** *device:file-name* | **success redirect** *url*}

Cisco IOS Release 12.2(52)SG, 12.2SE, 15.2(1)E, and later releases

ip admission proxy http { {**login** | **success** | **failure** | **login expired**} **page file** *device:file-name* | **success redirect** *url* | **refresh-all**}
no ip admission proxy http { {**login** | **success** | **failure** | **login expired**} **page file** *device:file-name* | **success redirect** *url* | **refresh-all**}

Syntax Description

login	Specifies a locally stored web page to be displayed during login.
success	Specifies a locally stored web page to be displayed when the login is successful.
failure	Specifies a locally stored web page to be displayed when the login has failed.
login expired	Specifies a locally stored web page to be displayed when the login has expired.
device	Specifies a disk or flash memory in the switch memory file system where the custom HTML file is stored.
file-name	Specifies the name of the custom HTML file to be used in place of the default HTML file for the specified condition.
success redirect *url*	Specifies an external web page to be displayed when the login is successful.
refresh-all	Specifies the refresh of all custom HTML pages to reflect the updates made to the pages in the disk or flash memory in the switch memory file system. **Note** Effective with CSCtj25327, the **refresh-all** keyword was introduced for Cisco IOS Release 12.2(52)SG, 12.2SE, 15.2(1)E, and later releases.

Command Default

The internal default authentication proxy web pages are displayed during web-based authentication.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Release	Modification
12.2(52)SG	The **refresh-all** keyword was introduced.

Usage Guidelines

When configuring the use of customized authentication proxy web pages, consider the following guidelines:

- To enable the custom web pages feature, you must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages will be used.
- The four custom HTML files must be present on the disk or flash of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.
- Any external link from a custom page will require configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.
- If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.
- Because the custom login page is a public web form, consider the following guidelines for this page:
  - The login form must accept user input for the username and password and must POST the data as uname and pwd.
  - The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.
- When configuring a redirection URL for successful login, consider the following guidelines:
  - If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available in the CLI. You can perform redirection in the custom login success page.
  - If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.
- Effective with CSCtj25327, when a custom HTML page is replaced with a new page with the exact same name in the disk or flash memory in the switch memory file system, use the **ip admission proxy http refresh-all** command to refresh the custom HTML pages and view the new pages.

Examples

The following example shows how to configure custom authentication proxy web pages:

```
Device(config)# ip admission proxy http login page file disk1:login.htm
Device(config)# ip admission proxy http success page file disk1:success.htm
Device(config)# ip admission proxy http fail page file disk1:fail.htm
Device(config)# ip admission proxy http login expired page file disk1:expired.htm
```

The following example shows how to verify the configuration of custom authentication proxy web pages:

```
Device# show ip admission configuration

Authentication proxy webpage
 Login page         : disk1:login.htm
 Success page       : disk1:success.htm
 Fail Page          : disk1:fail.htm
 Login expired Page : disk1:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following example shows how to configure a redirection URL for successful login:

```
Device(config)# ip admission proxy http success redirect www.example.com
```

The following example shows how to verify the redirection URL for successful login:

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.example.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Related Commands

Command	Description
ip http server ip https server	Enables the HTTP server within the switch.
show ip admission configuration	Displays the configuration of web-based authentication ip admission.

ip admission virtual-ip

To configure a web-based proxy authentication virtual IP address, use the **ip admission virtual-ip** command in global configuration mode. To remove the address, use the **no** form of this command.

ip admission virtual-ip *ip-address* [**virtual-host** *host-name*]
no ip admission virtual-ip *ip-address* [**virtual-host** *host-name*]

Syntax Description

ip-address	Virtual IP address.
virtual-host *ip-address*	(Optional) Specifies the name of the virtual host to connect to.

Command Default

A web-based proxy authentication virtual IP address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.4(2)T	This command was modified. The **virtual-host** *host-name* keyword and argument pair was added in a release prior to Cisco IOS Release 15.4(2)T.

Usage Guidelines

A virtual IP address is used only in communication between the Cisco IOS HTTP authentication and clients. For the web-based proxy authentication to operate you must set the virtual IP address, and no other device on the network can have the same IP address as the virtual IP address.

Examples

The following example shows how to configure the web-based proxy authentication virtual IP address:

```
Device(config)# ip admission virtual-ip 10.1.1.1
```

Related Commands

Command	Description
content-scan out	Enables content scanning on an egress interface.

ip audit

To apply an audit specification created with the **ip audit**command to a specific interface and for a specific direction, use the **ip audit**command in interface configuration mode. To disable auditing of the interface for the specified direction, use the **no** version of this command.

ip audit *audit-name* {**in** | **out**}
no ip audit *audit-name* {**in** | **out**}

Syntax Description

audit-name	Name of an audit specification.
in	Inbound traffic.
out	Outbound traffic.

Command Default

No audit specifications are applied to an interface or direction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit**interface configuration command to apply an audit specification created with the **ip audit**command to a specific interface and for a specific direction.

Examples

In the following example, the audit specification MARCUS is applied to an interface and direction:

```
interface e0
 ip audit MARCUS in
```

In the following example, the audit specification MARCUS is removed from the interface on which it was previously added:

```
interface e0
 no ip audit MARCUS in
```

ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** command in global configuration mode. To set the default action for attack signatures, use the **no** form of this command.

ip audit attack action [**alarm**] [**drop**] [**reset**]
no ip audit attack

Syntax Description

action	Specifies an action for the attack signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Command Default

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit attack** global configuration command to specify the default actions for attack signatures.

Examples

In the following example, the default action for attack signatures is set to all three actions:

```
ip audit attack action alarm drop reset
```

ip audit info

To specify the default actions for info signatures, use the **ip audit info** command in global configuration mode. To set the default action for info signatures, use the **no** form of this command.

ip audit info action [**alarm**] [**drop**] [**reset**]
no ip audit info

Syntax Description

action	Sets an action for the info signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Command Default

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit info** global configuration command to specify the default actions for info signatures.

Examples

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```

ip audit name

To create audit rules for info and attack signature types, use the **ip audit name** command in global configuration mode. To delete an audit rule, use the **no** form of this command.

ip audit name *audit-name* {**info** | **attack**} [**list** *standard-acl*] [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit name *audit-name* {**info** | **attack**}

Syntax Description

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for info signatures.
attack	Specifies that the audit rule is for attack signatures.
list	(Optional) Specifies an ACL to attach to the audit rule.
standard-acl	(Optional) Integer representing an access control list. Use with the **list** keyword.
action	(Optional) Specifies an action or actions to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the **action** keyword.
drop	(Optional) Drops the packet. Use with the **action** keyword.
reset	(Optional) Resets the TCP session. Use with the **action** keyword.

Command Default

If an action is not specified, the default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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

Any signatures disabled with the **ip audit signature** command do not become a part of the audit rule created with the **ip audit name** command.

Examples

In the following example, an audit rule called INFO.2 is created, and configured with all three actions:

```
ip audit name INFO.2 info action alarm drop reset
```

In the following example, an info signature is disabled and an audit rule called INFO.3 is created:

```
ip audit signature 1000 disable
ip audit name INFO.3 info action alarm drop reset
```

In the following example, an audit rule called ATTACK.2 is created with an attached ACL 91, and the ACL is created:

```
ip audit name ATTACK.2 list 91
access-list 91 deny 10.1.0.0 0.0.255.255
access-list 91 permit any
```

ip audit notify

To specify the method of event notification, use the **ip audit notify** command in global configuration mode. To disable event notifications, use the **no** form of this command.

ip audit notify {**nr-director** | **log**}
no ip audit notify {**nr-director** | **log**}

Syntax Description

nr-director	Send messages in NetRanger format to the NetRanger Director or Sensor.
log	Send messages in syslog format.

Command Default

The default is to send messages in syslog format.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If messages are sent to the NetRanger Director, then you must also configure the NetRanger Director's Post Office transport parameters using the **ip audit po remote** command.

Examples

In the following example, event notifications are specified to be sent in NetRanger format:

```
ip audit notify nr-director
```

Related Commands

Command	Description
ip audit po local	Specifies the local Post Office parameters used when sending event notifications to the NetRanger Director.
ip audit po remote	Specifies one or more sets of Post Office parameters for NetRanger Directors receiving event notifications from the router.

ip audit po local

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the **ip audit po local** command in global configuration mode. To set the local Post Office parameters to their default settings, use the **no** form of this command.

ip audit po local hostid *id-number* **orgid** *id-number*
no ip audit po local [**hostid** *id-number* **orgid** *id-number*]

Syntax Description

hostid	Specifies a NetRanger host ID.
id-number	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the local host. The default host ID is 1.
orgid	Specifies a NetRanger organization ID.
id-number	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the group to which the local host belongs. The default organization ID is 1.

Command Default

The default organization ID is 1. The default host ID is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit po local** global configuration command to specify the local Post Office parameters used when sending event notifications to the NetRanger Director.

Examples

In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip audit po local hostid 10 orgid 500
```

ip audit po max-events

To specify the maximum number of event notifications that are placed in the router's event queue, use the **ip audit po max-events**command inglobal configuration mode. To set the number of recipients to the default setting, use the **no** version of this command.

ip audit po max-events *number-of-events*
no ip audit po max-events

Syntax Description

number-of-events	Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events.

Command Default

The default number of events is 100.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Examples

In the following example, the number of events in the event queue is set to 250:

```
ip audit po max-events 250
```

ip audit po protected

To specify whether an address is on a protected network, use the **ip audit po protected** command in global configuration mode. To remove network addresses from the protected network list, use the **no** form of this command.

ip audit po protected *ip-addr* [**to** *ip-addr*]
no ip audit po protected [*ip-addr*]

Syntax Description

ip-addr	IP address of a network host.
to *ip-addr*	(Optional) Specifies a range of IP addresses.

Command Default

If no addresses are defined as protected, then all addresses are considered outside the protected network.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source or destination of the packet belongs to a protected network or not.

If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

Examples

In the following example, a range of addresses is added to the protected network list:

```
ip audit po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip audit po protected 10.4.1.1
ip audit po protected 10.4.1.8
ip audit po protected 10.4.1.25
```

In the following example, an address is removed from the protected network list:

```
no ip audit po protected 10.4.1.1
```

ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** global configuration command. To remove a NetRanger Director's Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

ip audit po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address* **localaddress** *ip-address* [**port** *port-number*] [**preference** *preference-number*] [**timeout** *seconds*] [**application** {**director** | **logger**}]
no ip audit po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address*

Syntax Description

host-id	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. Use with the **hostid** keyword.
hostid	Specifies a NetRanger host ID.
org-id	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the **orgid** keyword.
orgid	Specifies a NetRanger organization ID.
rmtaddress	Specifies the IP address of the NetRanger Director.
localaddress	Specifies the IP address of the Cisco IOS Firewall IDS router.
ip-address	IP address of the NetRanger Director or Cisco IOS Firewall IDS router's interface. Use with the **rmtaddress**and **localaddress**keywords.
port-number	(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. Use with the **port** keyword.
port	(Optional) Specifies a User Datagram Protocol port through which to send messages.
preference	(Optional) Specifies a route preference for communication.
preference-number	(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the **preference** keyword.
seconds	(Optional) Integer representing the heartbeat timeout value for Post Office communications. Use with the **timeout** keyword.
timeout	(Optional) Specifies a timeout value for Post Office communications.
application	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages.
director	(Optional) Specifies that the receiving application is the NetRanger Director interface.
logger	(Optional) Specifies that the receiving application is a NetRanger Sensor.

Command Default

The default organization ID is 1.

The default host ID is 1.

The default UDP port number is 45000.

The default preference is 1.

The default heartbeat timeout is 5 seconds.

The default application is **director**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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

A router can report to more than one NetRanger Director. In this case, use the **ip audit po remote** command to add each NetRanger Director to which the router sends notifications.

More than one route can be established to the same NetRanger Director. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

A router can also report to a NetRanger Sensor. In this case, use the **ip audit po remote** command and specify **logger** as the application.

Examples

In the following example, two communication routes for the same dual-homed NetRanger Director are defined:

```
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1
preference 1
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1 preference
 2
```

The router uses the first entry to establish communication with the NetRanger Director defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different Director is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip audit po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout
 10 application director
```

ip audit signature

To attach a policy to a signature, use the **ip audit signature** command in global configuration mode. To remove the policy, use the **no** form of this command. If the policy disabled a signature, then the **no** form of this command reenables the signature. If the policy attached an access list to the signature, the **no** form of this command removes the access list.

ip audit signature *signature-id* {**disable** | **list** *acl-list*}
no ip audit signature *signature-id*

Syntax Description

signature-id	Unique integer specifying a signature as defined in the NetRanger Network Security Database.
disable	Disables the ACL associated with the signature.
list	Specifies an ACL to associate with the signature.
acl-list	Unique integer specifying a configured ACL on the router. Use with the **list** keyword.

Command Default

No policy is attached to a signature.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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 allow you to set two policies: disable the audit of a signature or qualify the audit of a signature with an access list.

If you are attaching an access control list to a signature, then you also need to create an audit rule with the **ip audit name**command and apply it to an interface with the **ip audit** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip audit signature 6150 disable
ip audit signature 1000 list 99
access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip audit smtp

To specify the number of recipients in a mail message over which a s pam attack is suspected, use the **ip audit smtp** command in global configuration mode. To set the number of recipients to the default setting, use the **no** form of this command.

ip audit smtp spam *number-of-recipients*
no ip audit smtp spam

Syntax Description

spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
number-of-recipients	Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the **spam** keyword. The default is 250 recipients.

Command Default

The default number of recipients is 250.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit smtp** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.

Examples

In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```

ip auth-proxy (global configuration)

To set the the authenticatio proxy idle timeout or maximum number of idle connections, use the **ip auth-proxy**command in global configuration mode. To return the idle timeout or maximum number of idle connections to their default values, use the **no** form of this command.

ip auth-proxy {**absolute-timer** *min* | **inactivity-timer** *min* | **init-state-timer** *min* | **max-nodata-conns** *number*}
no ip auth-proxy [**absolute-timer**] [**inactivity-timer**] [**init-state-timer**] [**max-nodata-conns**]

Syntax Description

absolute-timer *min*	Length of time in minutes that an ingress IP authentication proxy session can remain active. After this timer expires, each session must go through the entire process of establishing its connection as if it was a new request. The range is 0 to 35,791. The default is 0.
inactivity-timer *min*	L ength of time in minutes that an active ingress session can be present with no activity or data from the end client. If this timer expires without activity or data, the session is cleared. The range is 1 to 2,147,483,647. The default is 60. **Note** This keyword and argument pair replaces the auth-cache-time *min* keyword and argument pair.
init-state-timer *min*	Length of time in minutes that an ingress authentication proxy session can stay in the INIT state. An ingress session is first registered in the INIT state until the user enters their username and password credentials. If the timer expires before the credentials are entered, the session is removed. The range is 1 to 15. The default is 2.
max-nodata-conns *number*	Maximum number of idle (“no data”) TCP connections that can exist globally for the IP authentication feature. The range is 1 to 1,000. The default is 3.

Command Default

The absolute timer is enabled indefinitely. The inactivity timer, and the INIT state timer are enabled. The limit on the number of global idle TCP connections is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The **inactivity-timer**and **absolute-timer** keywords were added .
12.4(6)T	The **init-state-timer**keyword was added

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

Usage Guidelines

You use the **ip auth-proxy**command to set the global idle timeout value for the authentication proxy. The idle timeout value is the length of time an authentication cache entry, along with its associated dynamic user access control list, is cleared after a period of inactivity.

You use the **absolute-timer** keyword to configure the length of time during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. You can override the global absolute timeout value with the local (per protocol) value, which you can enable by using the **ip auth-proxy name** command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

You must set the value of the **inactivity-timer**keyword to a higher value than the idle timeout of any Context-Based Access Control (CBAC) protocols. Otherwise, when the authentication proxy removes the user profile (and its associated dynamic user ACLs), there might be idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

You use the **init-state-timer** keyword to configure the amount of time that the authentication proxy is allowed to clear connections that are in the INIT state. Authentication attempts can remain in the INIT state when the router is loaded heavily and the authentication is not completed in two minutes. This problem is more likely if HTTPS is used for authenticating users. The default value of two minutes is usually sufficient to handle most cases, but if not, you should use the **init-state-timer** keyword to increase this value.

You use the **max-nodata-conns** keyword to limit the number of idle TCP connections (TCP sessions that are active but do not transmit data for a long period of time). There is no timer associated with this number.

Examples

The following example sets the inactivity timer to 30 minutes:

```
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy inactivity-timer 30
```

The following example sets the INIT state timer to 15 minutes:

```
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy init-state-timer 15
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy (interface configuration)

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy**command in interface configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

ip auth-proxy *auth-proxy-name*
no ip auth-proxy *auth-proxy-name*

Syntax Description

auth-proxy-name	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the **ip auth-proxy name** command.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip auth-proxy** command to enable the named authentication proxy rule at the firewall interface. Traffic passing through the interface from hosts with an IP address matching the standard access list and protocol type (HTTP) is intercepted for authentication if no corresponding authentication cache entry exists. If no access list is defined, the authentication proxy intercepts traffic from all hosts whose connection initiating packets are received at the configured interface.

Use the no form of this command with a rule name to disable the authentication proxy for a given rule on a specific interface. If a rule is not specified, the **no** form of this command disables the authentication proxy on the interface.

Examples

The following example configures interface Ethernet0 with the HQ_users rule:

```
interface e0
 ip address 172.21.127.210 255.255.255.0
 ip access-group 111 in
 ip auth-proxy HQ_users
 ip nat inside
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy auth-proxy-banner

To display a banner, such as the router name, in the authentication proxy login page, use the **ip auth-proxy auth-proxy-banner** command in global configuration mode. To disable display of the banner, use the **no** form of this command.

ip auth-proxy auth-proxy-banner {**ftp** | **http** | **telnet**} [*banner-text*]
no ip auth-proxy auth-proxy-banner {**ftp** | **http** | **telnet**}

Syntax Description

ftp	Specifies the FTP protocol.
http	Specifies the HTTP protocol.
telnet	Specifies the Telnet protocol.
banner-text	(Optional) Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C banner-text C," where "C" is a delimiting character.

Command Default

This command is not enabled, and a banner is not displayed on the authentication proxy login page.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The following keywords were added: **ftp**, **http**, and **telnet**.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip auth-proxy auth-proxy-banner** command allows users to configure one of two possible scenarios:

- The **ip auth-proxy auth-proxy-banner** command is enabled.

In this scenario, the administrator has not supplied any text. Thus, a default banner that states the following: "Cisco Systems, <router's hostname> Authentication" will be displayed in the authentication proxy login page. This scenario is most commonly used.

- The **ip auth-proxy auth-proxy-banner** command with the *banner-text* argument is enabled.

In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, only the multiline text will displayed in the authentication proxy login page. You will not see the default banner, "Cisco Systems, <router's hostname> Authentication."

Note If the **ip auth-proxy auth-proxy-banner** command is not enabled, there will not be any banner configuration. Thus, nothing will be displayed to the user on authentication proxy login page except a text box to enter the username and a text box to enter the password.

Examples

The following example causes the router name to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner ftp
```

The following example shows how to specify the custom banner “whozat” to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner telnet CwhozatC
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy max-login-attempts

To limit the number of login attempts at a firewall interface in the interface configuration command mode, use the **ip auth-proxy max-login-attempts** command. Use the **no** form of this command to return to the default settings.

ip auth-proxy max-login-attempts *number*
no ip auth-proxy max-login-attempts

Syntax Description

number	Maximum number of login attempts. The range is 1 to 100. The default value depends on the authentication mechanism: • FTP: 5 • HTTP: 30 • Telnet: 3

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SE	This command was modified. The maximum number of login attempts was changed to 100.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

This command is supported on the firewall interfaces only.

The maximum login attempt functionality is independent of the watch-list feature (you create a watch list with the **ip access-list hardware permit fragments** command). If you do not configure a watch list, the existing authentication proxy behavior occurs, but it displays the new number for retries. If you configure a watch list, when the maximum is reached, the session is blocked and the IP address is put in the watch list.

Examples

This example shows how to set a limit to the number of login attempts at a firewall interface:

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)# end
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip auth-proxy name

To create an authentication proxy rule, use the **ip auth-proxy name**command in global configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

Cisco IOS 12.4(6)T and Later Releases
ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**} [**event timeout aaa policy identity** *id-policy-name*] [**absolute-timer** *timeout*] [**auth-cache-time** *timeout*] [**inactivity-time** *timeout*] [**list** {*list-num* [**service-policy type tag** *policy-name*]*std-list-numlist-name*}] [**service-policy type tag** *service-policy-name*]
no ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**}

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases
ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**} [**event timeout aaa policy identity** *id-policy-name*] [**absolute-timer** *timeout*] [**auth-cache-time** *timeout*] [**inactivity-time** *timeout*] [**list** {*list-numstd-list-numlist-name*}]
no ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**}

Syntax Description

auth-proxy-name	A name of up to 16 alphanumeric characters to be associated with an authentication proxy rule.
ftp	Specifies FTP to trigger the authentication proxy.
http	Specifies HTTP to trigger the authentication proxy.
telnet	Specifies Telnet to trigger the authentication proxy.
event timeout aaa policy identity *id-policy-name*	(Optional) Specifies the event to be associated with the policy, timeout of the based event, AAA fail policy to be applied, Identity fail policy to be applied, and Identity policy name.
absolute-timer *timeout*	(Optional) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 0 to 35791 minutes. The default value is 0 minutes.
auth-cache-time *timeout*	(Optional) Alias of inactivity timeout in minutes. Enter a value in the range 1 to 35791 minutes.
inactivity-time *min*	(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 35791 minutes. The default value is equal to the value set with the ip auth-proxy command. **Note** This option deprecates the **auth-cache-time** *timeout*option.
list {*list-num* | *std-list-num* | *list-name*	(Optional) Specifies a standard (1 to 99), extended (1 to 199), or named IP access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the access list. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.

service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	(Optional) Control plane tag service policy that is configured using the **policy-map type control tag** *policy-map-name* command. This policy map is used to apply the actions on the host when a tag is received.

Command Default

The default value is equal to the value set with the **ip auth-proxy auth-cache-time** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2	Support for named and extend access lists was introduced.
12.3(1)	The following keywords were introduced: • **ftp** • **telnet** • **inactivity-time** *timeout* • **absolute-timer** *timeout*
12.4(6)T	The **service-policy type tag** keywords and *service-policy-name*argumentwere added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **event**, **timeout**, **aaa**, **policy**, **identity**keywords and the *id-policy-name*argument were added.

Usage Guidelines

This command creates a named authentication proxy rule, and it allows you to associate that rule with an access control list (ACL), providing control over which hosts use the authentication proxy. The rule is applied to an interface on a router using the **ip auth-proxy**command.

Use the **inactivity-time** *timeout*option to override the global the authentication proxy cache timer. This option provides control over timeout values for specific authentication proxy rules. The authentication proxy cache timer monitors the length of time (in minutes) that an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity. When that period of inactivity (idle time) expires, the authentication entry and the associated dynamic access lists are deleted.

Use the **list** option to associate a set of specific IP addresses or a named ACL with the **ip auth-proxy name**command.

Use the **no** form of this command with a rule name to remove the authentication proxy rules. If no rule is specified, the **no** form of this command removes all the authentication rules on the router, and disables the proxy at all interfaces.



Note You must use the **aaa authorization auth-proxy** command with the **ip auth-proxy name**command. Together these commands set up the authorization policy to be retrieved by the firewall. Refer to the **aaa authorization auth-proxy** command for more information.

Examples

The following example shows how to create the HQ_users authentication proxy rule. Because an access list is not specified in the rule, all connection-initiating HTTP traffic is subjected to authentication.

```
ip auth-proxy name HQ_users http
```

The following example shows how to create the Mfg_users authentication proxy rule and apply it to hosts specified in ACL 10:

```
access-list 10 192.168.7.0 0.0.0.255
ip auth-proxy name Mfg_users http list 10
```

The following example shows how to set the timeout value for Mfg_users to 30 minutes:

```
access-list 15 any
ip auth-proxy name Mfg_users http inactivity-timer 30 list 15
```

The following example shows how to disable the Mfg_users rule:

```
no ip auth-proxy name Mfg_users
```

The following example shows how to disable the authentication proxy at all interfaces and remove all the rules from the router configuration:

```
no ip auth-proxy xyz ftp
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.
ip auth-proxy (global)	Sets the authentication proxy idle timeout value (that is, the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).
ip auth-proxy (interface)	Applies an authentication proxy rule at a firewall interface.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy watch-list

To enable and configure an authentication proxy watch list in the interface configuration command mode, use the **ip auth-proxy watch-list** command. To disable the watch-list functionality, remove an IP address from the watch list. Or, to return to the default setting, use the **no** form of this command.

ip auth-proxy watch-list {**add-item** *ip-addr* | **enable** | **expiry-time** *minutes*}
no ip auth-proxy watch-list [**add-item** *ip-addr* | **expiry-time**]

Syntax Description

add-item *ip-addr*	Adds an IP address to the watch list.
enable	Enables a watch list.
expiry-time *minutes*	Specifies the duration of time that an entry is in the watch list; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- *minutes* is **30** minutes.
- The watch-list functionality is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The valid values for minutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or 2147483647 in decimal). Setting the *minutes* to 0 (zero) places the entries in the list permanently.

This command is supported on the firewall interfaces only.

Use the **no** form of this command to do the following:

- **no ip auth-proxy watch-list** --Disables the watch-list functionality .
- no **ip auth-proxy watch-list add-item** *ip-addr*--Removes the IP address from the watch list.
- **no ip auth-proxy watch-list expiry-time** --Returns to the default setting.

A watch list consists of IP addresses that have opened TCP connections to port 80 and have not sent any data. No new connections are accepted from this type of IP address (to port 80) and the packet is dropped.

An entry remains in the watch list for the time that is specified by **expiry-time** *minutes*.

When you disable a watch list, no new entries are put into the watch list, but the sessions are put in SERVICE_DENIED state. The timer deletes sessions after 2 minutes.

Examples

This example shows how to enable an authentication proxy watch list:

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

This example shows how to disable an authentication proxy watch list:

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

This example shows how to add an IP address to a watch list:

```
Router(config-if)# ip auth-proxy watch-list add-item 10.0.0.2
Router(config-if)#
```

This example shows how to set the duration of time that an entry is in a watch list:

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip device tracking probe

To enable the tracking of device probes, use the **ip device tracking probe** command in configuration mode. To disable device probes, use the **no** form of this command.

ip device tracking probe {**count** *count* | **delay** *delay* | **interval** *interval*}

Syntax Description

count *count*	Specifies the number of IP tracking probes from 1 to 5.
delay *delay*	Specifies the delay time of IP tracking probes from 1 to 120 seconds.
interval *interval*	Specifies the time between IP tracking probes from 30 to 300 minutes.

Command Default

Device probe tracking is disabled.

Command Modes

Config mode (config #)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.

Examples

The following example shows how to set the probe count to 5:

```
Router(config)# ip device tracking probe count 5
```

The following example shows how to set the delay time to 60:

```
Router(config)# ip device tracking probe delay 60
```

The following example shows how to set the interval time to 35:

```
Router(config)# ip device tracking probe interval 35
```

Related Commands

Command	Description
show ip device tracking	Displays information about entries in the IP device tracking table.

ip dhcp client broadcast-flag (interface)

To configure a DHCP client to set or clear the broadcast flag, use the **ip dhcp client broadcast-flag** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client broadcast-flag {**clear** | **set**}
no ip dhcp client broadcast-flag

Syntax Description

clear	Clears the broadcast flag.
set	Sets the broadcast flag.

Command Default

The broadcast flag is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

For a DHCP server to work on a Dynamic Multipoint VPN (DMVPN) network, the DHCP client available on the spoke must unicast the DHCP messages from the server to the client. By default, the DHCP client on the spoke broadcasts the DHCP messages. The broadcast flag is set during broadcast. Hence, the DHCP client on the spoke must have an option to clear the DHCP broadcast flag. You can use the **ip dhcp client broadcast-flag** command to configure the DHCP client to set or clear the broadcast flag.

Examples

The following example shows how to configure a DHCP client to clear the broadcast flag:

```
Router(config)# tunnel 1
Router(config-if)# ip dhcp client broadcast-flag clear
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from the DHCP.
ip dhcp support tunnel unicast	Configures a spoke-to-hub tunnel to unicast the DHCP replies over the DMVPN network.

ip dhcp support tunnel unicast

To configure a spoke-to-hub tunnel to unicast DHCP replies over a Dynamic Multipoint VPN (DMVPN) network, use the **ip dhcp support tunnel unicast** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support tunnel unicast
no ip dhcp support tunnel unicast

Syntax Description

This command has no arguments or keywords.

Command Default

A spoke-to-hub tunnel broadcasts the replies over the DMVPN network.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. The DHCP relay agent must unicast the DHCP messages for a DHCP server to be functional in the DMVPN environment. Hence for the DHCP to be functional in DMVPN environment, you must configure the DHCP relay agent to unicast the DHCP messages.

Use the **ip dhcp support tunnel unicast** command to configure the DHCP relay agent to unicast the DHCP protocol messages from the server (hub) to the client (spoke). The relay agent uses the nonbroadcast multiaccess (NBMA) address to create temporary routes in Next Hop Resolution Protocol (NHRP) to help unicast the DHCPOFFER and DHCPACK messages to the spoke.

Examples

The following example shows how to configure a spoke-to-hub tunnel to unicast the replies over a DMVPN network:

```
Router(config)# ip dhcp support tunnel unicast
```

Related Commands

Command	Description
ip address dhcp	Configures an IP address on an interface acquired through DHCP.
ip dhcp client broadcast-flag	Configures the DHCP client to set or clear the broadcast flag.

ip-extension

To specify that IP extensions are included in a certificate request either for enrollment or generation of a certificate authority (CA) certificate for the Cisco IOS CA, use the **ip-extension** command in ca-trustpoint configuration mode. To remove a previously specified IP extension, use the **no** form of this command.

ip-extension [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*}
no ip-extension [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*}

Syntax Description

multicast	(Optional) Specifies that only multicast traffic, a subsequent address family identifier (SAFI), will be included in certificate requests. **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
unicast	(Optional) Specifies that only unicast traffic, a SAFI, will be included in certificate requests. **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
inherit	Specifies that IP addresses will be inherited from an issuer certificate. The issuer's certificate is first checked to find a certificate containing the address range or prefix. If no match is found, the certificate from the next issuer in the chain is checked, and so forth, up the certificate chain, recursively, until a match is located.
ipv4	(Optional) Specifies that only IPv4 addresses are inherited. **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.
ipv6	(Optional) Specifies that only IPv6 addresses are inherited. **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.
prefix *ipaddress*	Specifies the IP address prefix or a single IP address for either an IPv4 or IPv6 address. The IP address formats are: • A.B.C.D IPv4 address • A.B.C.D/nn IPv4 prefix • X:X:X:X::X IPv6 address • X:X:X:X::X/<0-128> IPv6 prefix

range	Specifies that there is a range of IP addresses.
min-ipaddress	The beginning IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Begninning IPv4 address in the range • X:X:X:X::X Beginning IPv6 address in the range
max-ipaddress	The ending IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Ending IPv4 address in the range • X:X:X:X::X Ending IPv6 address in the range

Command Default

No IP extensions will be included in a certificate request.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The **ip-extension** command may be used to specify IP extensions for a public key infrastructure (PKI) server or client and may be issued one or more times, including multiple issuances with the **inherit**, **prefix**, and **range**keywords. For the inherit option, if the address family is not specified, both IPv4 and IPv6 addresses will be inherited. When the IPv4 or IPv6 address family is not specified for prefix or range, the address family will be determined from the address format.

Note It is recommended that you validate each **ip-extension** command line against your existing IP-extension configuration according to RFC 3779, verifying that IP address ranges do not overlap. The issue's certificate may not be available to validate the issuer's certificate for subsets of addresses.

Examples

The following example shows how to specify that multiple IP extensions are included in the server certificate request:

```
Router(ca-trustpoint)# ip-extension multicast prefix 10.64.0.0/11
! Only multicast traffic with the IPv4 prefix 10.64.0.0/11 will be included in certificate
 requests.
```

Router(ca-trustpoint)# **ip-extension prefix 2001:100:1::/48**

! Multicast and unicast traffic with the IPv6 prefix 2001:100:1::/48 will be included in certificate requests.

Router(ca-trustpoint)# **ip-extension inherit**

! Multicast and unicast traffic with IPv4 and IPv6 addresses will be inherited from the issuer's certificate.

Router(ca-trustpoint)# **ip-extension inherit ipv6**

! Multicast and unicast traffic with IPv6 addresses only will be inherited from the issuer's certificate.

Router(ca-trustpoint)# **ip-extension unicast range 209.165.200.225 143.255.55.255**

```
! Unicast traffic within the specified IPv4 address range will be included in the certificate
 request.
Router(ca-trustpoint)# ip-extension range 2001:1:1::1 2001:1:2:ffff:ffff:ffff:ffff:ffff
! Multicast and unicast traffic within the specified IPv6 address range will be included
in the certificate request.
```

The following is sample output from the **show crypto pki certificates verbose** command. The output displays X.509 certificate IP address extension information where the IPv4 multicast prefix has been set to 10.64.0.0/11, and the IPv4 unicast range has been set to 209.165.201.1 209.165.201.30.

```
CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number (hex): 01
   Certificate Usage: Signature
   Issuer:
     cn=srtr1
   Subject:
     cn=srtr1
   Validity Date:
     start date: 21:50:11 PST Sep 29 2008
     end   date: 21:50:11 PST Sep 29 2011
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (1024 bit)
   Signature Algorithm: MD5 with RSA Encryption
   Fingerprint MD5: 30C1C9B6 BC17815F DF6095CD EDE2A5F3
   Fingerprint SHA1: A67C451E 49E94E87 8EB0F71D 5BE642CF C68901EF
   X509v3 extensions:
     X509v3 Key Usage: 86000000
       Digital Signature
       Key Cert Sign
       CRL Signature
     X509v3 Subject Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
     X509v3 Basic Constraints:
         CA: TRUE
     X509v3 Authority Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
     Authority Info Access:
     X509v3 IP Extension:
         IPv4 (Unicast):
           209.165.202.129-209.165.202.158
         IPv4 (Multicast):
```

```
        10.64.0.0/11
Associated Trustpoints: srtr1
```

Related Commands

Command	Description
show crypto pki certificates	Displays information about the CA certificate.
show crypto pki trustpoints	Displays information about trustpoints that are configured on the router.

ip http ezvpn

To enable the Cisco Easy VPN remote web server interface, use the **ip http ezvpn** command in global configuration mode. To disable the Cisco Easy VPN remote web server interface, use the **no** form of this command.

Cisco uBR905 and Cisco BR925 cable access routers
ip http ezvpn
no ip http ezvpn

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco Easy VPN Remote web server interface is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)YJ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables the Cisco Easy VPN Remote web server, an onboard web server that allows users to connect an IPSec Easy VPN tunnel and to provide the required authentication information. The Cisco Easy VPN Remote web server allows the user to perform these functions without having to use the Cisco command-line interface (CLI).

Before using this command, you must first enable the Cisco web server that is onboard the cable access router by entering the **ip http server** command. Then use the **ip http ezvpn** command to enable the Cisco Easy VPN remote web server. You can then access the web server by entering the IP address for the Ethernet interface of the router in your web browser.



Note The Cisco Easy VPN Remote web interface does not work with the cable monitor web interface in Cisco IOS Release 12.2(8)YJ. To access the cable monitor web interface, you must first disable the Cisco Easy VPN remote web interface with the **no ip http ezvpn** command, and then enable the cable monitor with the **ip http cable-monitor** command.

Examples

The following example shows how to enable the Cisco Easy VPN remote web server interface:

```
Router# configure terminal
```

```
Router(config)# ip http server
Router(config)# ip http ezvpn
Router(config)# exit
Router# copy running-config startup-config
```

Related Commands

Command	Description
ip http cable-monitor	Enables and disables the Cable Monitor Web Server feature.
ip http port	Configures the TCP port number for the HTTP web server of the router.
ip http server	Enables and disables the HTTP web server of the router.

ipv6 access-list match-local-traffic

To enable IPv6 Access Control List (ACL) matching for locally generated traffic, use the **ipv6 access-list match-local-traffic** command.

ipv6 access-list match-local-traffic

Syntax Description

This command has no arguments or keywords.

Command Default

Locally generated IPv6 traffic is not filtered by outgoing interface ACLs.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10.7S	This command was introduced.
Cisco IOS XE Release 16.1.1	This command was integrated into Cisco IOS XE Release 16.1.1

Usage Guidelines

By default, an IPv6 Access Control List (ACL) attached to a routed interface in the outgoing direction applies only to transit IPv6 traffic leaving the device. Traffic originating from the device bypasses outgoing ACLs on egress interfaces by default and leaves without being filtered.

To enable outgoing ACLs on routed interfaces to also filter IPv6 traffic originating from the device, use the **ipv6 access-list match-local-traffic** global configuration command. This command causes locally generated IPv6 traffic to be filtered by the outgoing ACL on the egress interface. If no outgoing ACL is applied to the egress interface, locally generated traffic leaving through the interface will not be filtered.

Note The **ipv6 access-list match-local-traffic** command applies globally to all IPv6 traffic originated by the device leaving through any of its routed interfaces. On any routed interface, any attached outgoing IPv6 ACL will apply to all locally generated traffic leaving through that interface.

Examples

The following example shows how to force locally originated IPv6 traffic to be filtered by outgoing IPv6 ACLs on egress interfaces:

```
Router# configure terminal
Router(config)# ipv6 access-list match-local-traffic
```