icmp idle-timeout through ip http ezvpn

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).

Command	Description
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.

ip access-group

To apply an IP access list 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, use the **no** form of this command.

ip access-group {*access-list-name*| *access-list-number*} {**in**| **out**}

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

Syntax Description

access-list-name	Name of the existing IP access list 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
Cisco IOS XE 3SE	This command introduced.

Usage Guidelines

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

Applying Access Lists to Interfaces

Access lists 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, the networking device also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list 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, the networking device also checks the destination access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable inbound access lists 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).

Examples

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

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

Related Commands

Command	Description
deny	Sets conditions in a named IP access list that will deny packets.
ip access-list	Defines an IP access list by name or number.
permit	Sets conditions in a named IP access list that will permit packets.
show ip access-list	Displays the contents of IP access lists.

ip access-list

To define an IP 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 to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list {{**standard** | **extended**} {*access-list-name* | *access-list-number*} | **helper egress check** | **log-update threshold** *threshold* | **logging** {**hash-generation** | **interval** *milliseconds*} | **role-based** *access-list-name*}

no ip access-list {{**standard** | **extended**} {*access-list-name* | *access-list-number*} | **helper egress check** | **log-update threshold** | **logging** {**hash-generation** | **interval**} | **role-based** *access-list-name*}

Syntax Description

standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list.
access-list-name	Name of the IP access list. 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 is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to configure a named or numbered IP access list. This command places the device 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.

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 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:

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

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

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

Related Commands

Command	Description
deny	Sets conditions in a named IP access list that will deny packets.
ip access-group	Applies an ACL to an interface or a service policy map.
permit	Sets conditions in a named IP access list that will permit packets.
show ip access-list	Displays the contents of IP access lists.

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 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* [**event timeout aaa policy identity** *identity-policy-name*]

no ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

Syntax Description

admission-name	Authentication or admission rule name.
event timeout aaa policy identity	Specifies an authentication policy to be applied when the AAA server is unreachable.
identity-policy-name	Authentication or admission rule name to be applied when the AAA server is unreachable.

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.

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 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.
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.

Command	Description
show ip admission configuration	Displays the configuration of web-based authentication ip admission.

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.