all profile map configuration through browser-proxy

all (profile map configuration)

To specify that all authentication and authorization requests be cached, use the **all**command in profile map configuration mode. To disable the caching of all requests, use the **no** form of this command.

all [**no-auth**]
no all

Syntax Description

no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No requests are cached.

Command Modes

Profile map configuration (config-profile-map)

Command History

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

Usage Guidelines

Use the **all** command to cache all authentication and authorization requests.

Use the **all** command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

Examples

The following example caches all authorization requests in the localusers cache profile group. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# all no-auth
```

Related Commands

Command	Description
profile	Defines or modifies an individual authentication and authorization cache profile based on an exact username match.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

allow-mode

To turn the default mode of the filtering algorithm on or off, use the **allow-mode**command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

allow-mode {**on** | **off**}
no allow-mode {**on** | **off**}

Syntax Description

on	Turns on the default mode of the filtering algorithm. The default is on.
off	Turns off the default mode of the filtering algorithm.

Command Default

The filtering algorithm is turned on.

Command Modes

URL parameter-map configuration

Command History

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

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **allow-mode**subcommand after you enter the **parameter-map type urlfilter** command.

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

Examples

The following example turns on the filtering algorithm:

```
parameter-map type urlfilter eng-filter-profile
 allow-mode on
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

appfw policy-name

To define an application firewall policy and put the router in application firewall policy configuration mode, use the **appfw policy-name**command in global configuration mode. To remove a policy from the router configuration, use the **no** form of this command.

appfw policy-name *policy-name*
no appfw policy-name *policy-name*

Syntax Description

policy-name	Name of application policy.

Command Default

If this command is not issued, an application firewall policy cannot be created.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command puts the router in application firewall policy (appfw-policy-*protocol)*configuration mode, which allows you to begin defining the application firewall policy that will later be applied to the Cisco IOS Firewall via the **ip inspect name** command.

What Is an Application Firewall Policy?

The application firewall uses static signatures to detect security violations. A static signature is a collection of parameters that specifies which protocol conditions must be met before an action is taken. (For example, a signature may specify that an HTTP data stream containing the POST method must reset the connection.) These protocol conditions and reactions are defined by the end user via a command-line interface (CLI) to form an application firewall policy (also known as a security policy).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
```

```
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
application	Puts the router in appfw-policy-*protocol*configuration mode and begin configuring inspection parameters for a given protocol.
ip inspect name	Defines a set of inspection rules.

appl (webvpn)

To configure an application to access a smart tunnel, use the **appl** command in WebVPN smart tunnel configuration mode. To disable an application from accessing the smart tunnel, use the **no** form of this command.

appl *display-name appl-name* **windows**
no appl *display-name appl-name* **windows**

Syntax Description

display-name	Name of the application to be displayed in the smart tunnel application access list on the web browser.
appl-name	Application name or path.
windows	Specifies the Windows platform.

Command Default

No applications have access to a smart tunnel.

Command Modes

WebVPN smart tunnel configuration mode (config-webvpn-smart-tunnel)

Command History

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

Usage Guidelines

You must configure the correct path and application name to allow the smart tunnel to provide access to applications.

Examples

The following example shows how to configure applications to access the smart tunnel:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# smart-tunnel list st1
Router(config-webvpn-smart-tunnel)# appl ie ieexplore.exe windows
Router(config-webvpn-smart-tunnel)# appl telnet telnet.exe windows
```

Related Commands

Command	Description
smart-tunnel list	Configures the smart tunnel list and enables it within a policy group.
webvpn context	Configures the SSL VPN context.

application (application firewall policy)

To put the router in appfw-policy-*protocol*configuration mode and begin configuring inspection parameters for a given protocol, use the **application**command in application firewall policy configuration mode. To remove protocol-specific rules, use the **no** form of this command.

application *protocol*
no application *protocol*

Syntax Description

protocol	Protocol-specific traffic will be inspected. One of the following protocols (keywords) can be specified: • **http** (HTTP traffic will be inspected.) • **im** {**aol** | **yahoo** | **msn**} (Traffic for the specified instant messenger application will be inspected.)

Command Default

You cannot set up protocol-specific inspection parameters.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	The **im**, **aol yahoo**, and **msn** keywords were introduced to support instant message traffic detection and prohibition.

Examples

This command puts the router in appfw-policy-*protocol*configuration mode, where "*protocol*" is dependent upon the specified protocol.

HTTP-Specific Inspection Commands

After you issue the **application http** command and enter the appfw-policy-http configuration mod e, begin configuring inspection parameters for HTTP traffic by issuing any of the following commands:

- **audit-trail**
- **content-length**
- **content-type-verification**

- **max-header-length**
- **max-uri-length**
- **port-misuse**
- **request-method**
- **strict-http**
- **timeout**
- **transfer-encoding**

Instant Messenger-Specific Inspection Commands

After you issue the **application im**command and specify an instant messenger application (AOL, Yahoo, or MSN), you can begin configuring inspection parameters for IM traffic by issuing any of the following commands:

- **alert**
- **audit trail**
- **server**
- **service**
- **timeout**

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
```

```
!
!
```

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.user1.aol.com
!
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy
interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

Related Commands

Command	Description
appfw policy-name	Defines an application firewall policy and puts the router in application firewall policy configuration mode.

application-inspect

To enable Layer 7 application protocol inspection in zone-based policy firewalls, use the **application-inspect** command in parameter-map type inspect configuration mode. To disable Layer 7 inspection, use the **no** form of this command.

application-inspect {**all** *protocol-name*}
no application-inspect {**all** *protocol-name*}

Syntax Description

all	Specifies all supported Layer 7 protocols.
protocol-name	Name of the protocol to be inspected or not. Valid values for the *protocol-name* argument are the following: • **dns**—Domain Name Server • **exec**—Remote process execution • **ftp**—File Transfer Protocol • **gtp**—GPRS Tunneling Protocol • **h323**—H.323 Protocol • **http**—HTTP • **imap**—Internet Message Access Protocol • **login**—Remote login • **msrpc**—Microsoft Remote Procedure Call • **netbios**—NETBIOS • **pop3**—Post Office Protocol Version 3 • **rtsp**—Real Time Streaming Protocol • **shell**—Shell • **sip**—Session Initiation Protocol • **skinny**—Skinny Client Control Protocol • **smtp**—Simple Mail Transfer Protocol • **sunrpc**—SUN Remote Procedure Call • **tftp**—Trivial File Transfer Protocol

Command Default

Layer 7 application protocol inspection is enabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Zone-based policy firewalls supports Layer 7 application protocol inspection along with application layer gateways (ALGs) and application inspection and controls (AICs). Layer 7 application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic that passes through a security module.

Before configuring the **application-inspect** command, you must configure either the **parameter-map type inspect** *parameter-map-name* or the **parameter-map type inspect-global** command.

Note You can only configure either the **parameter-map type inspect** *parameter-map-name* or the **parameter-map type inspect-global** command at any time. You cannot configure these command simultaneously.

Examples

The following example shows how to disable Layer 7 application protocol inspection for FTP in a user-defined parameter map:

```
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# no application-inspect ftp
```

The following example shows how to enable Layer 7 application protocol inspection for all supported protocols at a global firewall level:

```
Device(config)# parameter-map type inspect-global
Device (config-profile)# application-inspect all
```

Related Commands

Command	Description
parameter-map type inspect	Enables an inspect-type parameter map for the firewall to connect thresholds, timeouts, and other parameters that pertain to the inspect action, and enters parameter-map type inspect configuration mode.
parameter-map type inspect-global	Enables a global parameter map and enters parameter-map type inspect configuration mode.

application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode.

application redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

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

Examples

The following example shows how to enter redundancy application configuration mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)#
```

Related Commands

Command	Description
group (firewall)	Enters redundancy application group configuration mode.

arap authentication

To enable authentication, authorization, and accounting (AAA) authentication for AppleTalk Remote Access Protocol (ARAP) on a line, use the **arap authentication** command in line configuration mode. To disable authentication for an ARAP line, use the **no** form of this command.

Caution If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARAP will be disabled on this line.

arap authentication {**default***list-name*} [**one-time**]
no arap authentication {**default***list-name*}

Syntax Description

default	Default list created with the **aaa authentication arap** command.
list-name	Indicated list created with the **aaa authentication arap** command.
one-time	(Optional) Accepts the username and password in the username field.

Command Default

ARAP authentication uses the default set with **aaa authentication arap** command. If no default is set, the local user database is checked.

Command Modes

Line configuration

Command History

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

Usage Guidelines

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** keyword. Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

Examples

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARAP line 7:

```
line 7
 arap authentication MIS-access
```

Related Commands

Command	Description
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.

ase collector

Note Effective with Cisco IOS Release 12.4(24), the **ase collector** command is not available in Cisco IOS software.

To enter the destination IP address of the Automatic Signature Extraction (ASE) collector server, use the **ase collector** command in global configuration mode. To remove this IP address, use the **no** form of this command.

ase collector *ip-address*
no ase collector *ip-address*

Syntax Description

ip-address	Provides IP connectivity between the ASE sensor and ASE collector.

Command Default

No ASE collector IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to configure an ASE collector IP address:

```
Router(config)# ase collector 10.10.10.3
```

Related Commands

Command	Description
ase enable	Enables the ASE feature on a specified interface.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase enable

Note Effective with Cisco IOS Release 12.4(24), the **ase enable** command is not available in Cisco IOS software.

To enable the Automatic Signature Extraction (ASE) feature on a specified interface, use the **ase enable** command in interface configuration mode. To disable the ASE feature on a specified interface, use the **no** form of this command.

ase enable
no ase enable

Syntax Description

This command has no arguments or keywords.

Command Default

The ASE feature is disabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to enable the ASE feature on a specified interface:

```
Router(config-if)# ase enable
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase group

Note Effective with Cisco IOS Release 12.4(24), the **ase group** command is not available in Cisco IOS software.

To identify the Threat Information Distribution Protocol (TIDP) group number used for exchange between the Automatic Signature Extraction (ASE) sensor and ASE collector, use the **ase group** command in global configuration mode. To disable this group number, use the **no** form of this command.

ase group *TIDP-group-number*
no ase group *TIDP-group-number*

Syntax Description

TIDP-group-number	TIDP group number for the ASE feature. The range of group numbers is between 1 and 65535.

Command Default

No TIDP group number is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to configure a TIDP group number for the ASE feature:

```
Router(config)# ase group 10
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase signature extraction

Note Effective with Cisco IOS Release 12.4(24), the **ase signature extraction**command is not available in Cisco IOS software.

To enable the Automatic Signature Extraction (ASE) feature globally on the router, use the **ase signature extraction**command in global configuration mode. To disable the ASE feature globally on the router, use the **no** form of this command.

ase signature extraction
no ase signature extraction

Syntax Description

This command has no arguments or keywords.

Command Default

The ASE feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to enable the ASE feature globally on the router:

```
Router(config)# ase signature extraction
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Displays the ASE run-time status, which includes the TIDP group number.

asymmetric-routing

To set up an asymmetric routing link interface and to enable applications to divert packets received on the standby redundancy group to the active, use the **asymmetric-routing** command in redundancy application group configuration mode. To disable the configuration, use the **no** form of this command.

asymmetric-routing {**always-divert enable** | **interface** *type number*}
no asymmetric-routing {**always-divert enable** | **interface**}

Syntax Description

always-divert enable	Always diverts packets from the standby redundancy group (RG) to the active RG.
interface *type number*	Specifies the asymmetric routing interface that is used by the RG.

Command Default

Asymmetric routing is disabled.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Asymmetric routing occurs when packets from TCP or UDP connections flow in different directions through different routes. In asymmetric routing, packets that belong to a single connection are forwarded through one router, but return packets of the connection return through another router in the same RG. When you configure the **asymmetric routing always-divert enable** command, the packets received on the standby RG are redirected to the active RG for processing. If the **asymmetric routing always-divert enable** command is disabled, the packets received on the standby RG may be dropped.

When you configure the **asymmetric-routing interface** command, the asymmetric routing feature is enabled. After enabling the feature, configure the **asymmetric-routing always-divert enable** command to enable Network Address Translation (NAT) to divert packets that are received on the standby RG to the active RG.

Note The zone-based policy firewall does not support the **asymmetric-routing always-divert enable** command that diverts packets received on the standby RG to the active RG. The firewall forces all packet flows to be diverted to the active RG.

Examples

The following example shows how to configure asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 2
Router(config-red-app-grp)# asymmetric-routing interface gigabitethernet 0/0/0
Router(config-red-app-grp)# end
```

Related Commands

Command	Description
application redundancy	Configures application redundancy.
group	Configures a redundancy group.
redundancy	Enters redundancy configuration mode.
redundancy asymmetric-routing enable	Establishes an asymmetric flow diversion tunnel for each redundancy group.

attribute (server-group)

To add attributes to an accept or reject list, use the **attribute** command in server-group configuration mode. To remove attributes from the list, use the **no** form of this command.

attribute *number* [**number** [**number**] . . .]
no attribute *number* [**number** [**number**] . . .]

Syntax Description

number [*number* [*number* ...	Attributes to include in an accept or reject list. The value can be a single integer, such as 7, or a range of numbers, such as 56-59. At least one attribute value must be specified.

Command Default

If this command is not enabled, all attributes are sent to the network access server (NAS).

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Used in conjunction with the **radius-server attribute list** command (which defines the list name), the **attribute** command can be used to add attributes to an accept or reject list (also known as a filter). Filters are used to prevent the network access server (NAS) from receiving and processing unwanted attributes for authorization or accounting.

The **attribute** command can be used multiple times to add attributes to a filter. However, if a required attribute is specified in a reject list, the NAS will override the command and accept the attribute. Required attributes are as follows:

Note The user-password (RADIUS attribute 2) and nas-ip (RADIUS attribute 4) attributes can be filtered together successfully in the access request if they are configured to be filtered. An access request must contain either a user-password or a CHAP password or a state. Also, either a NAS IP address or NAS identifier must be present in a RADIUS accounting request.

- For authorization:
  - 2 (user-password)
  - 6 (Service-Type)
  - 7 (Framed-Protocol)
- For accounting:
  - 4 (NAS-IP-Address)
  - 40 (Acct-Status-Type)
  - 41 (Acct-Delay-Time)
  - 44 (Acct-Session-ID)

Note The user will not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose--authorization or accounting. The server will determine whether an attribute is required when it is known what the attribute is to be used for.

Examples

The following example shows how to add attributes 2, 4, 12, 217, 6-10, 13, 64-69, and 218 to the list name “standard”:

```
radius-server attribute list standard
attribute 2,4,12,217,6-10,13
attribute 64-69,218
```

Related Commands

Command	Description
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

attribute map

To attach an attribute map to a particular Lightweight Directory Access Protocol (LDAP) server, use the **attribute map**command in LDAP server configuration mode. To remove the attribute maps, use the **no** form of this command.

attribute map *map-name*
no attribute map *map-name*

Syntax Description

map-name	Attribute map name.

Command Default

No attribute maps exist for any LDAP servers.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

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

Usage Guidelines

To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example shows how to attach “attribute att_map_1” to the attribute map in LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# attribute map att_map_1
```

Related Commands

Command	Description
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

attribute nas-port format

To configure services to use specific named methods for different service types, which can be set to use their own respective RADIUS server groups, use the **attribute nas-port format** command in server-group configuration mode. To remove the override, which is to use specific named methods for different service types, use the **no** form of this command.

attribute nas-port format *format-type* [*string*]
no attribute nas-port format format-type [*string*]

Syntax Description

format-type	Type of format (see the first table below).
string	(Optional) Pattern of the data format (see the second table below).

Command Default

Default format type is used for all services.

Command Modes

Server-group configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The following format types may be configured.

Table 1: Format Types

a	Format is type, channel, or port.
b	Either interface(16), isdn(16), or async(16).
c	Data format (bits): shelf(2), slot(4), port(5), or channel(5).
d	Data format (bits): slot(4), module(1), port(3), vpi(8), or vci(16).
e	Configurable data format (see the table below).

The following characters may be used in the string pattern of the data format.

Table 2: Characters Supported by Format-Type e

0	Zero
1	One
f	DS0 shelf
s	DS0 slot

a	DS0 adapter
P	DS0 port
i	DS0 subinterface
c	DS0 channel
F	Async shelf
S	Async slot
P	Async port
L	Async line
S	PPPoX slot (includes PPP over ATM [PPPoA], PPP over Ethernet over ATM [PPPoEoA], PPP over Ethernet over Ethernet [PPPoEoE], PPP over Ethernet over VLAN [PPPoEoVLAN], and PPP over Ethernet over Queue in Queue [PPPoEoQinQ]).
A	PPPoX adapter
P	PPPoX port
V	PPPoX VLAN ID
I	PPPoX virtual path identifier (VPI)
C	PPPoX virtual channel indicator (VCI)
U	Session ID

Examples

The following example shows that a leased-line PPP client has chosen to send no RADIUS Attribute 5 while the default is set for format d:

```
interface Serial2/0
 no ip address
 encapsulation ppp
 ppp accounting SerialAccounting
 ppp authentication pap
aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1
aaa group server radius group1
 server 10.101.159.172 auth-port 1645 acct-port 1646
 attribute nas-port none
radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
ip radius source-interface	Forces RADIUS to use the IP adressing of a specified interface for all outgoing RADIUS packets.

Command	Description
radius-server host	Specifies a RADIUS server host.

attribute type

To define an attribute type that is to be added to an attribute list locally on a router, use the **attribute type**command in global configuration mode. To remove the attribute type from the list, use the **no** form of this command.

attribute type *name value* [**service** *service*] [**protocol** *protocol*] [*tag*]
no attribute type *name value* [**service** *service*] [**protocol** *protocol*] [*tag*]

Syntax Description

name	The Cisco IOS authentication, authorization, and accounting (AAA) internal name of the IETF RADIUS attribute to be added to the attribute list. For a list of supported attributes, use the CLI help option (**?**) on your platform.
value	A string, binary, or IPv4 address value. This is the RADIUS attribute that is being defined in Cisco IOS AAA format. A string added to the attribute value must be inside quotation marks. For example, if the value is “interface-config” and the string is “ip unnumbered FastEthernet0,” you would write interface-config “ip unnumbered FastEthernet0”.
service *service*	(Optional) Specifies the Access method, which is typically PPP.
protocol *protocol*	(Optional) Specifies the type of protocol, which can be ATM, IP, or virtual private dialup network (VPDN).
tag	(Optional) A means of grouping attributes that refer to the same VPDN tunnel.

Command Default

An attribute type is not added to the attribute list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(55)SE	This command was modified in Cisco IOS Release 12.2(55)SE. The following options were added for the *service* argument: **ap-lsc-join** , **ap-mic-join**, **ap-ssc-join**, **lbs-mic-join**, and **lbs-ssc-join**.

Usage Guidelines

Attributes are added to the attribute list each time a new attribute type is defined. Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation is applicable to both

RADIUS and TACACS+ AAA servers. Thus, if you are not familiar in configuring a AAA server, Cisco recommends that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “example.com.” The attribute TEST includes the attribute types interface-config “ip unnumbered FastEthernet0” and interface-config “ip vrf forwarding vrf1.”

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding vrf1" service ppp protocol lcp
!
ip vrf blue
 description vrf vrf1 template1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
subscriber authorization enable
!
subscriber profile example.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile example.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
```

Related Commands

Command	Description
aaa attribute list	Defines a AAA attribute list locally on a router.

audit filesize

To change the size of the audit file, use the **audit filesize**command in global configuration mode. To return the audit file to its default size, use the **no** form of this command.

audit filesize *size*
no audit filesize *size*

Syntax Description

size	Size of the audit file in KB. Valid values range from 32 KB to 128 KB. 32 KB is the default size.

Command Default

The audit file is 32 KB.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(27)SBC	This commnad was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also referred to as hashes), which monitor changes that have been made to your router. Because the audit file that is stored on the disk is circular, the number of messages that can be stored is dependent on the size of the selected file. Also, the size determines the number of messages that can be stored on the disk before a wrap around occurs.

You should always ensure that the audit file is secure. The audit file should be access protected so that only the audit subsystem can access it.

Note Audit logs are enabled by default and cannot be disabled.

Examples

The following example shows how to change the audit file size to 128 KB:

```
Router(config)# audit filesize 128
```

Related Commands

Command	Description
audit interval	Changes the time interval that is used for calculating hashes.

Command	Description
show audit	Displays contents of the audit file.

audit interval

To change the time interval that is used for calculating hashes, use the **audit interval**command in global configuration mode. To return to the default value, which is 5 minutes, use the **no** form of this command.

audit interval *seconds*
no audit interval *seconds*

Syntax Description

seconds	Time interval, in seconds, between hash calculations. Valid values range from 120 seconds to 3600 seconds. The default value is 300 seconds (5 minutes).

Command Default

300 seconds (5 minutes)

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27) SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Hashes are used to monitor changes in your router. A separate hash is maintained for each of the following areas:

- Running version--A hash of the information that is provided in the output of the **show version** command--running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
- Hardware configuration--A hash of platform-specific information that is generally provided in the output of the **show diag**command.
- File system--A hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
- Running configuration--A hash of the running configuration.
- Startup configuration--A hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data files.

By default, the hashes are calculated every 5 minutes to see if any changes (events) have been made to the network. The time interval prevents a large number of hashes from being generated.

Note Audit logs are enabled by default and cannot be disabled.

Examples

The following example shows how to specify hashes to be calculated every 120 seconds (2 minutes):

```
Router(config)# audit interval 120
```

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
show audit	Displays contents of the audit file.

audit-trail

To enable message logging for established or torn-down connections, use the **audit-trail**command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

audit-trail {**on** | **off**}
no audit-trail {**on** | **off**}

Syntax Description

on	Audit trail messages are generated.
off	Audit trail messages are not generated.

Command Default

If this command is not issued, the default value specified via the **ip inspect audit-trail**command will be used.

Command Modes

cfg-appfw-policy-http
configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **audit-trail** command will override the **ip inspect audit-trail** global command.

Before you can issue the **audit-trail**command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol*configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example, which shows how to define the HTTP application firewall policy "mypolicy," enables audit trail messages for the given policy. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  audit trail on
  strict-http action allow alarm
```

```
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect audit-trail	Turns on audit trail messages.

audit-trail (zone)

To turn audit trail messages on or off, use the **audit-trail** command in parameter-map type inspect configuration mode or URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

audit trail {**on** | **off**}
no audit trail {**on** | **off**}

Syntax Description

on	Audit trail messages will be issued.
off	Audit trail messages will not be issued.

Command Default

There are no audit trail messages.

Command Modes

Parameter-map type inspect configuration
URL parameter-map configuration

Command History

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

Usage Guidelines

You can use the **audit-trail** subcommand when you are creating a parameter map. For each inspected protocol, you can set the audit trail to **on** or **off**.

When you are configuring an inspect type parameter map, you can enter the **audit-trail**subcommand after you enter the **parameter-map type inspect** command.

When you are creating or modifying a URL parameter map, you can enter the **audit-trail**subcommand after you enter the **parameter-map type urlfilter** command.

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

Examples

The following example generates audit trail messages:

```
parameter-map type inspect insp-params
 audit-trail on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication**command in redundancy application protocol configuration mode. To disable the authentication settings in the redundancy group, use the **no** form of this command.

authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}
no authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

Syntax Description

text *string*	Uses clear text authentication.
md5 key-string	Uses MD5 key authentication. The *key* argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted.
0	(Optional) Specifies that the text following immediately is not encrypted.
7	(Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm.
md5 key-chain *key-chain-name*	Uses MD5 key-chain authentication.

Command Default

The key is not encrypted.

Command Modes

Redundancy application protocol configuration (config-red-app-prtcl)

Command History

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

Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# authentication text name1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

Command	Description
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange (IKE) policy, use the **authentication** command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the **no** form of this command.

authentication {**rsa-sig** | **rsa-encr** | **pre-share** | **ecdsa-sig**}
no authentication

Syntax Description

rsa-sig	Specifies RSA signatures as the authentication method. This method is not supported in IPv6.
rsa-encr	Specifies RSA encrypted nonces as the authentication method. This method is not supported in IPv6.
pre-share	Specifies preshared keys as the authentication method.
ecdsa-sig	Specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method.

Command Default

The RSA signatures authentication method is used.

Command Modes

ISAKMP policy configuration (config-isakmp)

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)T	This command was modified. The **ecdsa-sig** keyword was added.

Usage Guidelines

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

Use this command to specify the authentication method to be used in an IKE policy.

If you specify RSA signatures, you must configure your peer routers to obtain certificates from a certification authority (CA).

If you specify RSA encrypted nonces, you must ensure that each peer has the other peer's RSA public keys. (See the **crypto key pubkey-chain rsa**, **addressed-key**, **named-key**, **address**, and commands.)

If you specify preshared keys, you must also separately configure these preshared keys. (See the **crypto isakmp identity** and **crypto isakmp key** commands.)

Examples

The following example configures an IKE policy with preshared keys as the authentication method (all other parameters are set to the defaults):

```
Router(config)#
 crypto isakmp policy 15
Router
(config-isakmp)#
 authentication pre-share
Router
(config-isakmp)#
 exit
```

Related Commands

Command	Description
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy.
crypto key generate rsa (IKE)	Generates RSA key pairs.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

authentication (IKEv2 profile)

To specify the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile, use the **authentication** command in IKEv2 profile configuration mode. To delete the authentication method, use the **no** form of this command.

authentication {**local** {**rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig** | **eap** | [**gtc** | **md5** | **mschapv2** | {**username** *username*} | {**password** *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig**}}
no authentication {**local** {**rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig** | **eap** | [**gtc** | **md5** | **mschapv2** | {**username** *username*} | {**password** *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share**[**key** *password*] | **ecdsa-sig**}}

Syntax Description

local	Specifies the local authentication method.
rsa-sig	Specifies Rivest, Shamir, and Adelman (RSA) signature as the authentication method.
pre-share	Specifies preshared key as the authentication method.
key	Specifies a preshared key.
password	Specifies a password for preshared key. This argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.
ecdsa-sig	Specifies Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method.
eap	Specifies Extensible Authentication Protocol (EAP) as the authentication method.
gtc	(Optional) Specifies Extensible Authentication Protocol (EAP) as the authentication method using Generic Token Card (GTC) for verifying the credentials.
md5	(Optional) Specifies Extensible Authentication Protocol (EAP) as the authentication method using Message Digest 5 (MD5) for verifying the credentials.
mschapv2	(Optional) Specifies Extensible Authentication Protocol (EAP) as the authentication method using Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2) for verifying the credentials.
username *username*	Specifies the EAP user name.
password	Specifies the EAP password.
remote	Specifies the remote authentication method.
query-identity	(Optional) Queries EAP identity from the peer.

timeout *seconds*	(Optional) Specifies the duration, in seconds, to wait for the next IKE_AUTH request after sending the first IKE_AUTH response. The range is from 45 to 180, and the default is 90.

Command Default

The default local and remote authentication method is not configured.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **ecdsa-sig** keyword was added.
15.1(3)T	This command was modified. The **eap** and **query-identity** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(3)T	This command was modified. The **eap** keyword was added for the local authentication method and the **timeout** *seconds* keyword-argument pair was added for the remote EAP authentication method.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.3(3)M	This command was modified. The following keywords and arguments were added: • *password* • **gtc** • **md5** • **mschapv2** • **username** *username* • **username**

Usage Guidelines

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

Use this command to specify the local and remote authentication methods in an IKEv2 profile. You can configure only one local authentication method and multiple remote authentication methods. Multiple remote authentication methods are allowed because the profile caters to multiple peers, and the authentication method that a peer uses is not known. However, each remote authentication method must be specified in a separate command.

If the RSA signature is configured as the local or remote authentication method, you must specify the PKI trustpoints to obtain the signing and verification certificates using the **pki trustpoint** command.

If a preshared key is configured as the local or remote authentication method, you must separately configure the preshared keys and the keyring using the **keyring** command to specify the local and remote keys.

If the **query-identity** keyword is specified, the EAP identity request is sent when the remote peer indicates the intent to use EAP authentication by omitting the Auth payload in the IKE-AUTH request and the local policy allows EAP authentication for the remote peer. The remote EAP identity is used in the following scenarios:

- The EAP identity is used to switch to another IKEv2 profile.
- The remote EAP identity is passed to the RADIUS EAP server as the username for the peer to be authenticated for external EAP.
- The remote EAP identity is used to derive a name for requests using a name mangler.

The **timeout** *seconds* keyword-argument pair is used with the remote EAP authentication method and specifies the duration to obtain EAP credentials on the EAP client.

Extensible Authentication Protocol (EAP) as the local authentication method is supported only on the IKEv2 initiator and EAP as the remote authentication is supported only on the IKEv2 responder. If EAP is specified as the local authentication method, the remote authentication method must be certificate based. If the **authentication remote eap query-identity** command is not configured on the FlexVPN server, the client cannot have an IPv4 or IPv6 address as the local identity because the IP address cannot be used as the username for the EAP authentication method.

Examples

The following example shows how to specify an authentication method in an IKEv2 profile:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# match identity remote address 192.168.1.1
Device(config-ikev2-profile)# authentication local rsa-sig
Device(config-ikev2-profile)# authentication remote eap query-identity
Device(config-ikev2-profile)# authentication remote rsa-sig
Device(config-ikev2-profile)# identity local email user1@example.com
Device(config-ikev2-profile)# keyring keyring-1
Device(config-ikev2-profile)# pki trustpoint tp-remote verify
```

In the above example, the profile profile1 specifies preshare as the local authentication method and rsa-sig and EAP query identity as the remote authentication methods that use keyring keyring-1 and the trustpoint tp-remote.

The following example shows how to configure an IKEv2 profile for two peers using different authentication methods:

```
Device(config)# crypto ikev2 profile profile2
Device(config-ikev2-profile)# match identity local email user1@example.com
Device(config-ikev2-profile)# match identity remote email user2@example.com
Device(config-ikev2-profile)# authentication local eap
Device(config-ikev2-profile)# authentication remote rsa-sig
```

The above profile caters to two peers, user1@example.com authenticated with EAP and user2@example.com authenticated with preshare.

The following example shows how to configure the EAP as the local authentication method on the IKEv2 initiator:

```
Device(config)# crypto ikev2 profile prof-flex
Device(config-ikev2-profile)# match identity remote address 0.0.0.0
```

```
Device(config-ikev2-profile)# match certificate cmap-1
Device(config-ikev2-profile)# authentication remote rsa-sig
Device(config-ikev2-profile)# authentication local eap
Device(config-ikev2-profile)# keyring local key
Device(config-ikev2-profile)# pki trustpoint ca-server
```

The following example shows how to configure EAP as the remote authentication method on the IKEv2 responder:

```
Device(config)# crypto ikev2 profile prof-flex
Device(config-ikev2-profile)# match identity remote address 0.0.0.0
Device(config-ikev2-profile)# identity local dn
Device(config-ikev2-profile)# authentication remote eap query-identity
Device(config-ikev2-profile)# authentication local rsa-sig
Device(config-ikev2-profile)# keyring local key
Device(config-ikev2-profile)# pki trustpoint ca-server
Device(config-ikev2-profile)# aaa authentication eap rad
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.
keyring	Specifies the keyring used with a preshared key authentication method.
pki trustpoint	Specifies the PKI trustpoints used with the RSA signature authentication method.
show crypto ikev2 profile	Displays the IKEv2 profile.

authentication bind-first

To configure the sequence of the search and bind operations of an authentication request in the Lightweight Directory Access Protocol (LDAP) server, use the **authentication bind-first** command in LDAP server configuration mode. To remove the search and bind configuration, use the **no** form of this command.

authentication bind-first [**no-authorization**]
no authentication bind-first [**no-authorization**]

Syntax Description

no-authorization	(Optional) Specifies that no authorization is required for authentication requests.

Command Default

The search operation is performed first, and the bind operation is performed later.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.2(1)T	This command was modified. The **no-authorization**keyword was added.

Usage Guidelines

In an LDAP deployment, the search operation is performed first, and the bind operation is performed later. The search operation is performed first because if the password attribute is returned as part of the search operation, then the password verification can be done locally on the LDAP client and there is no need for the bind operation. If the password attribute is not returned, a bind operation can be performed. Another advantage of performing the search operation first and the bind operation later is that the distinguished name (DN) received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with the base DN.

Use the **no-authorization**keyword to specify whether authorization is required for authentication requests. The **no-authorization** keyword should be used when you do not want to download the user profile from the server.

Examples

The following example shows how to configure the search and bind operations for an authentication request that does not require authorization:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication bind-first no-authorization
```

The following example shows how to configure the search and bind operations for an authentication request:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication bind-first
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

authentication command

To specify the HTTP command that is sent to the certification authority (CA) for authentication, use the **authentication command**in ca-profile-enroll configuration mode.

authentication command *http-command*

Syntax Description

http-command	Defines the HTTP command. **Note** The *http-command* argument is not the HTTP URL.

Command Default

No default behavior or values

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use the **authentication command** to send the HTTP request to the CA server for certificate authentication. Before enabling this command, you must use the **authentication url** command.

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure certificate authentication via HTTP for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication url	Specifies the URL of the CA server to which to send authentication requests.
crypto ca profile enrollment	Defines an enrollment profile.

Command	Description
parameter	Specifies parameters for an enrollment profile.

authentication command bounce-port ignore

To configure the router to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the **authentication command bounce-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

authentication command bounce-port ignore
no authentication command bounce-port ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The router accepts a RADIUS CoA bounce port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

A RADIUS CoA bounce port command sent from a RADIUS server can cause a link flap on an authentication port, which triggers Dynamic Host Configuration Protocol (DHCP) renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The **authentication command bounce-port ignore** command configures the router to ignore the RADIUS CoA bounce port command to prevent a link flap from occuring on any hosts that are connected to an authentication port.

Examples

This example shows how to configure the router to ignore a RADIUS CoA bounce port command:

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

Related Commands

Command	Description
authentication command disable-port ignore	Configures the router to ignore a RADIUS server CoA **disable port** command.

authentication command disable-port ignore

To allow the router to ignore a RADIUS server Change of Authorization (CoA) disable port command, use the **authentication command disable-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

authentication command disable-port ignore
no authentication command disable-port ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The router accepts a RADIUS CoA disable port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the **authentication command disable-port ignore** command to configure the router to ignore the RADIUS server CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

Examples

This example shows how to configure the router to ignore a CoA **disable port** command:

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

Related Commands

Command	Description
authentication command bounce-port ignore	Configures the router to ignore a RADIUS server CoA bounce port command.

authentication compare

To replace a bind request with a compare request for an authentication, use the **authentication compare** command in LDAP server configuration mode. To disable the comparison of bind operations for the authentication requests, use the **no** form of this command.

authentication compare
no authentication compare

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication request is performed with bind request.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

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

Examples

The following example shows how to replace a bind request with a compare request for an authentication:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication compare
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

authentication control-direction

To set the direction of authentication control on a port, use the **authentication control-direction**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication control-direction {**both** | **in**}
no authentication control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The IEEE 802.1x standard is implemented to block traffic between the nonauthenticated clients and network resources. This means that nonauthenticated clients cannot communicate with any device on the network except the authenticator. The reverse is true, except for one circumstance--when the port has been configured as a unidirectional controlled port.

Unidirectional State

The IEEE 802.1x standard defines a unidirectional controlled port, which enables a device on the network to "wake up" a client so that it continues to be reauthenticated. When you use the **authentication control-direction in** command to configure the port as unidirectional, the port changes to the spanning-tree forwarding state, thus allowing a device on the network to wake the client, and force it to reauthenticate.

Bidirectional State

When you use the **authentication control-direction both** command to configure a port as bidirectional, access to the port is controlled in both directions. In this state, the port does not receive or send packets.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# authentication control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# authentication control-direction both
```

authentication critical recovery delay

To configure the Auth Manager critical recovery delay, use the **authentication critical recovery delay**command in global configuration mode. To remove a previously configured recovery delay, us the **no** form of this command.

authentication critical recovery delay *milliseconds*
no authentication critical recovery delay

Syntax Description

milliseconds	The period of time, in milliseconds, that the Auth Manager waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000.

Command Default

The default delay is 1000 milliseconds.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example shows how to configure the critical recovery delay period to 1500 milliseconds:

```
Switch(config)# authentication critical recovery delay 1500
```

authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id* | **next-method**}
no authentication event fail

Syntax Description

retry *retry-count*	(Optional) Specifies how many times the authentication method is tried after an initial failure.
action	Specifies the action to be taken after an authentication failure as a result of incorrect user credentials.
authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.
next-method	Specifies that the next authentication method be invoked after a failed authentication attempt. The order of authentication methods is specified by the **authentication order** command.

Command Default

Authentication is attempted two times after the initial failed attempt.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Only the dot1x authentication method can signal this type of authentication failure.

Examples

The following example specifies that after three failed authentication attempts the port is assigned to a restricted VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event fail retry 3 action authorize vlan 40

Switch(config-if)# end
```

Related Commands

Command	Description
authentication event no-response action	Specifies the action to be taken when authentication fails due to a nonresponsive host.

Command	Description
authentication order	Specifies the order in which authentication methods are attempted.

authentication event no-response action

To specify how the Auth Manager handles authentication failures as a result of a nonresponsive host, use the **authentication event no-response action** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event no-response action authorize vlan *vlan-id*
no authentication event no-response

Syntax Description

authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command Default

Authentication fails.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **authentication event no-response action** command to specify how to handle authentication failures as a result of a nonresponsive host.

Examples

The following example specifies that when authentication fails as a result of a non-responsive host, the port is assigned to a VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event no-response action authorize vlan 40

Switch(config-if)# end
```

Related Commands

Command	Description
authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials

authentication event server alive action reinitialize

To reinitialize an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting (AAA) server becomes available, use the **authentication event server alive action reinitialize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server alive action reinitialize
no authentication event server alive action reinitialize

Syntax Description

This command has no arguments or keywords.

Command Default

The session is not reinitialized .

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **authentication event server alive action reinitialize** command to reinitialize authorized sessions when a previously unreachable AAA server becomes available.

Examples

The following example specifies that authorized sessions are reinitialized when a previously unreachable AAA server becomes available:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server dead action authorize	Specifies how to handle authorized sessions when the AAA server is unreachable.

authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server dead action authorize vlan *vlan-id*
no authentication event server dead action authorize

Syntax Description

vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command Default

No session is authorized.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **authentication event server dead action authorize** command to authorize sessions even when the AAA server is unavailable.

Examples

The following example specifies that when the AAA server becomes unreachable, the port is assigned to a VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server dead action authorize vlan 40

Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server alive action reinitialize	Reinitializes an authorized session when a previously unreachable AAA server becomes available.

authentication fallback

To enable a web authentication fallback method, use the **authentication fallback** command in interface configuration mode. To disable web authentication fallback, use the **no** form of this command.

authentication fallback *fallback-profile*
no authentication fallback

Syntax Description

fallback-profile	The name of the fallback profile for web authentication.

Command Default

Web authentication fallback is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication fallback** command to specify the fallback profile for web authentication. Use the **fallback profile** command to specify the details of the profile.

Examples

The following example shows how to specify a fallback profile on a port:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet1/0/3
Router(config-if)# authentication fallback profile1
Router(config-if)# end
```

Related Commands

Command	Description
fallback profile	Specifies the profile for web authentication.

authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]
no authentication host-mode

Syntax Description

single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.
multi-auth	Specifies that multiple clients can be authenticated on the port at any given time.
multi-domain	Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time.
multi-host	Specifies that after the first client is authenticated all subsequent clients are allowed access.
open	(Optional) Specifies that the port is open; that is, there are no access restrictions.

Command Default

Access to a port is not allowed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Before you use this command, you must use the **authentication port-control** command with the keyword **auto**.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

Examples

:The following example shows how to enable authentication in **multi-host** mode:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# authentication port-control auto

Switch(config-if)# authentication host-mode multi-host
```

Related Commands

Command	Description
authentication port-control	Displays information about interfaces.

authentication list (tti-registrar)

To authenticate the introducer in an Secure Device Provisioning (SDP) transaction, use the **authentication list**command in tti-registrar configuration mode. To disable the authentication, use the **no** form of this command.

authentication list *list-name*
no authentication list *list-name*

Syntax Description

list-name	Name of the list.

Command Default

An introducer is not authenticated.

Command Modes

tti-registrar configuration

Command History

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

Usage Guidelines

This command is used in SDP transactions. When the command is configured, the RADIUS or TACACS+ AAA server checks for a valid account by looking at the username and password.

The authentication list and the authorization list will usually both point to the same AAA list, but it is possible that the lists can be on different databases. This latter scenario is not recommended.

Examples

The following example shows that an authentication list named “authen-tac” has been configured. In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an SDP operation.
debug crypto wui	Displays information about an SDP operation.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.

Command	Description
template username	Establishes a template username and password to access the configuration template on the file system.

authentication open

To enable open access on this port, use the **authentication open** command in interface configuration mode. To disable open access on this port, use the **no** form of this command.

authentication open
no authentication open

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings by entering the **show authentication** privileged EXEC command.

This command overrides the **authentication host-mode** *session-type* **open** global configuration mode command for the port only.

Examples

The following example shows how to enable open access to a port:

```
Router(config-if)# authentication open
Router(config-if)#
```

The following example shows how to enable open access to a port:

```
Router(config-if)# no authentication open
Router(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

authentication order {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
no authentication order

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication(MAB).
webauth	Specifies web-based authentication.

Command Default

The default authentication order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication order** command to specify explicitly which authentication methods are run and the order in which they are run. Each method may be entered only once in the list and no method can be listed after **webauth**.

Examples

The following example sets the authentication order for a port:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x
Router(config-if)# end
Router#
```

Related Commands

Command	Description
authentication priority	Specifies the priority of authentication methods on a port.

authentication periodic

To enable automatic reauthentication on a port, use the **authentication periodic** command in interface configuration or template configuration mode. To disable, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication periodic** command replaces the **dot1x reauthentication** command.

authentication periodic
no authentication periodic

Syntax Description

This command has no arguments or keywords.

Command Default

Reauthentication is disabled.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

Use the **authentication periodic** command to enable automatic reauthentication on a port. To configure the interval between reauthentication attempts, use the **authentication timer reauthenticate** command.

Examples

The following example shows how to enable reauthentication and sets the interval to 1800 seconds:

```
Device(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface fastethernet0/2
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate 1800
```

The following example shows how to enable reauthentication and sets the interval to 1800 seconds for an interface template:

```
Device# configure terminal
Device(config)# template user-template1
```

```
Device(config-template)# authentication periodic
Device(config-template)# end
```

Related Commands

Command	Description
authentication timer reauthenticate	Specifies the period of time between attempts to reauthenticate an authorized port.

authentication port-control

To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1x port-control** command.

authentication port-control {**auto** | **force-authorized** | **force-unauthorized**}
no authentication port-control

Syntax Description

auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

Ports are authorized without authentication exchanges.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

To verify port-control settings, use the **show interfaces** command and check the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

With CSCtr06196, use the **dot1x pae authenticator** command in interface configuration mode to set the Port Access Entity (PAE) type.

Examples

The following example shows how to specify that the authorization status of the client be determined by the authentication process:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface ethernet0/2
Device(config-if)# authentication port-control auto
```

Related Commands

Command	Description
show interfaces	Configures the authorization state of a controlled port.

authentication priority

To specify the priority of authentication methods on a port, use the **authentication priority**command in interface configuration mode. To return to the default, use the **no** form of this command.

authentication priority {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
no authentication priority

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication.
webauth	Specifies web-based authentication.

Command Default

The default priority order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The **authentication order** command specifies the order in which authentication methods are attempted. This order is the default priority. To override the default priority and allow higher priority methods to interrupt a running authentication method, use the **authentication priority** command.

Examples

The following example shows the commands used to configure the authentication order and the authentication priority on a port:

```
Router# configure terminal
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x webauth
Router(config-if)# authentication priority dot1x mab
Router(config-if)# end
Router#
```

Related Commands

Command	Description
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.

authentication terminal

To manually cut-and-paste certificate authentication requests, use the **authentication terminal**command in ca-profile-enroll configuration mode. To delete a current authentication request, use the **no** form of this command.

authentication terminal
no authentication terminal

Syntax Description

This command has no arguments or keywords.

Command Default

An authentication request is not specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests when a network connection between the router and certification authority (CA) is not available. After this command is enabled, the authentication request is printed on the console terminal so that it can be manually copied (cut) by the user.

Examples

The following example shows how to specify manual certificate authentication and certificate enrollment via HTTP:

```
crypto ca profile enrollment E
 authentication terminal
 enrollment terminal
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity**command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

authentication timer inactivity {*seconds* | **server**}
no authentication timer inactivity

Syntax Description

seconds	The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535.
server	Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server.

Command Default

The inactivity timer is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

In order to prevent reauthentication of inactive sessions, use the **authentication timer inactivity**command to set the inactivity timer to an interval shorter than the reauthentication interval set with the **authentication timer reauthenticate** command.

Examples

The following example sets the inactivity interval on a port to 900 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer inactivity 900

Switch(config-if)# end
```

Related Commands

Command	Description
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration or template configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

authentication timer reauthenticate {*seconds* | **server**}
no authentication timer reauthenticate

Syntax Description

seconds	The number of seconds between reauthentication attempts. The range is from 1 to 65535. The default is 3600.
server	Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server.

Command Default

The automatic reauthentication interval is set to 3600 seconds.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

Use the **authentication timer reauthenticate** command to set the automatic reauthentication interval of an authorized port. If you use the **authentication timer inactivity** command to configure an inactivity interval, configure the reauthentication interval to be longer than the inactivity interval.

Examples

The following example shows how to set the reauthentication interval on a port to 1800 seconds:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface GigabitEthernet6/0
Device(config-if)# authentication timer reauthenticate 1800
Device(config-if)# end
```

The following example shows how to set the reauthentication interval on a port to 1500 seconds for an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# authentication timer reauthenticate 1500
Device(config-template)# end
```

Related Commands

Command	Description
authentication periodic	Enables automatic reauthentication.
authentication timer inactivity	Specifies the interval after which the Auth Manager ends an inactive session.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer restart

To specify the period of time after which the Auth Manager attempts to authenticate an unauthorized port, use the **authentication timer restart** command in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

authentication timer restart
seconds
no authentication timer restart

Syntax Description

seconds	The number of seconds between attempts to authenticate an unauthorized port. The range is 1 to 65535. The default is 60.

Command Default

No attempt is made to authenticate unauthorized ports.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication timer restart** command to specify the interval between attempts to authenticate an unauthorized port. The default interval is 60 seconds.

Examples

The following example sets the authentication timer interval to 120 seconds:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet6/0

Router(config-if)# authentication timer restart 120

Router(config-if)# end
```

Related Commands

Command	Description
authentication timer inactivity	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.

authentication trustpoint

To specify the trustpoint used to authenticate the Secure Device Provisioning (SDP) petitioner device's existing certificate, use the **authentication trustpoint**command in tti-registrar configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

authentication trustpoint {*trustpoint-label* | **use-any**}
no authentication trustpoint {*trustpoint-label* | **use-any**}

Syntax Description

trustpoint-label	Name of trustpoint.
use-any	Use any configured trustpoint.

Command Default

If this command is not specified, the petitioner-signing certificate is not verified.

Command Modes

tti-registrar configuration

Command History

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

Usage Guidelines

Issue the **authentication trustpoint** command in tti-registrar configuration mode to validate the signing certificate that the petitioner used.

Examples

The following example shows how to specify the trustpoint mytrust for the petitioner-signing certificate:

```
crypto provisioning registrar
 authentication trustpoint mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.

Command	Description
trustpoint signing	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar for signing the SDP data including the certificate.

authentication violation

To specify the action to be taken when a security violation occurs on a port, use the **authentication violation**command in interface configuration mode. To return to the default action, use the **no** form of this command.

authentication violation {**restrict** | **shutdown**}
no authentication violation

Syntax Description

restrict	Specifies that the port restrict traffic with the domain from which the security violation occurs.
shutdown	Specifies that the port shuts down upon a security violation.

Command Default

Ports are shut down when a security violation occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

Examples

The following example configures the GigabitEthernet interface to restrict traffic when a security violation occurs:

```
Switch(config)# interface GigabitEthernet6/2

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict

Switch(config-if)# end
```

authentication url

To specify the URL of the certification authority (CA) server to which to send authentication requests, use the **authentication url** command in ca-profile-enroll configuration mode. To delete the authentication URL from your enrollment profile, use the **no** form of this command.

authentication url *url*
no authentication url *url*

Syntax Description

url	URL of the CA server to which your router should send authentication requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the url argument must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA. If you are using TFTP for enrollment, the url argument must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Command Default

Your router does not recognize the CA URL until you declare one using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

If you do not specify the **authentication command** after you enable the **authentication url** command, the **authentication url** command functions the same as the **enrollment url** *url* command in trustpoint configuration mode. That is, the **authentication url** command will then be used only for certificate enrollment--not authentication.

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to configure an enrollment profile for direct HTTP enrollment with a CA server. In this example, the authentication command is also present.

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
```

```
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

The following example shows how to configure the enrollment profile named "E" to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment	Specifies the enrollment parameters of your CA.

authorization

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line configuration mode. To disable authorization, use the no form of this command.

authorization {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default***list-name*]
no authorization {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default***list-name*]

Syntax Description

arap	Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol.
commands	Enables authorization on the selected lines for all commands at the specified privilege level.
level	Specific command level to be authorized. Valid entries are 0 through 15.
exec	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines.
reverse-access	Enables authorization to determine if the user is allowed reverse access privileges.
default	(Optional) The name of the default method list, created with the **aaa authorization**command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Command Default

Authorization is not enabled.

Command Modes

Line configuration

Command History

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

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command authorization (for level 15) using the method list named charlie on line 10:

```
line 10
 authorization commands 15 charlie
```

Related Commands

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

authorization (server-group)

To filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization, use the **authorization**command in server-group configuration mode. To remove the filter on the authorization request or reply, use the **no** form of the command.

authorization [**request** | **reply**] [**accept** | **reject**] *list-name*
no authorization [**request** | **reply**] [**accept** | **reject**] *list-name*

Syntax Description

request	(Optional) Defines filters for outgoing authorization Access Requests.
reply	(Optional) Defines filters for incoming authorization Accept or Reject packets and for outgoing accounting requests.
accept	(Optional) Indicates that the required attributes and the attributes specified in the *list-name* argument will be accepted. All other attributes will be rejected.
reject	(Optional) Indicates that the attributes specified in the list-name will be rejected . All other attributes will be accepted.
list-name	Defines the given name for the accept or reject list.

Command Default

If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.
12.3(3)B	The **request** and **reply** keywords were added.
12.3(7)T	The **request** and **reply** keywords were integrated into Cisco IOS Release 12.3(7)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS authorization allows users to configure the network access server (NAS) to restrict the use of specific attributes, thereby preventing the NAS from processing unwanted attributes.

Only one filter may be used for RADIUS authorization per server group.

Note The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute (server-group configuration)**command to add to an accept or reject list.

Examples

The following example shows how to configure accept list "min-author" in an Access-Accept packet from the RADIUS server:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
 server 10.1.1.1
 authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
 attribute 6-7
```

The following example shows that the attribute "all-attr" will be rejected in all outbound authorization Access Request messages:

```
aaa group server radius ras
 server 192.168.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
radius-server attribute list	Defines an accept or reject list name.

authorization (tti-registrar)

To enable authentication, authorization, and accounting (AAA) authorization for an introducer or a certificate, use the **authorization**command in tti-registrar configuration mode. To disable authorization, use the **no** form of this command.

{**authorization login** | **certificate** | **login certificate**}
{**no authorization login** | **certificate** | **login certificate**}

Syntax Description

login	Use the username of the introducer for AAA authorization.
certificate	Use the certificate of the petitioner for AAA authorization.
login certificate	Use the username of the introducer and the certificate of the petitioner for AAA authorization.

Command Default

If an authorization list is configured, then authorization is enabled by default.

Command Modes

tti-registrar configuration

Command History

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

Usage Guidelines

This command controls the authorization of the introduction. Authorization can be based on the following:

- The login of the petitioner (username and password) to the registrar
- The current certificate of the petitioner
- Both the login of the introducer and the current certificate of the petitioner

If you issue the **authorization login** command, the introducer logs in with a username and password such as ttiuser and mypassword, which are used against the configured authorization list to contact the AAA server and determine the appropriate authorization.

If you issue the **authorization certificate** command, the certificate of the petitioner is used to build an AAA username, which is used to obtain authorization information.

If you issue the **authorization login certificate** command, authorization for the introducer combines with authorization for the petitioner's current certificate. This means that two AAA authorization lookups occur. In the first lookup, the introducer username is used to retrieve any AAA attributes associated with the introducer. The second lookup is done using the configured certificate name field. If an AAA attribute appears in both lookups, the second one prevails.

Examples

The following example shows how to specify authorization for both the introducer and the current certificate of the petitioner:

```
crypto provisioning registrar
 authorization login certificate
```

Related Commands

Command	Description
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction.

authorization address ipv4

To specify a list of addresses for a Group Domain of Interpretation (GDOI) group, use the **authorization address ipv4** command in GDOI local server configuration mode. To remove an address from the group, use the **no** form of this command.

authorization address ipv4 {*access-list-name* | *access-list-number*}
no authorization address ipv4 {*access-list-name* | *access-list number*}

Syntax Description

access-list-name	A hostname or distinguished name (DN).
access-list number	Standard IP access list number. Value: 1 through 99

Command Default

A list of addresses is not specified.

Command Modes

GDOI local server configuration

Command History

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

Usage Guidelines

If the identity of the Internet Key Exchange (IKE) authentication matches an entry in the access control list, the address is authorized.

Examples

The following example shows that access list number 99 has been specified to be part of a GDOI group:

```
authorization address ipv4 99
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

authorization identity

To specify an authorization identity for a Group Domain of Interpretation (GDOI) group based on a distinguished name (DN) or Fully Qualified Domain Name (FQDN), use the **authorization identity** command in GDOI local server configuration mode. To delete a GDOI group authorization identity, use the **no** form of this command.

authorization identity *name*
no authorization identity *name*

Syntax Description

name	The name of the authorization identity, which can be a DN or FQDN.

Command Default

An authorization identity for a GDOI group is not defined.

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

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

Usage Guidelines

Cisco Group Encrypted Transport Virtual Private Network (GET VPN) supports GDOI group member (GM) authorization using the authorization identity command when using Public Key Infrastructure (PKI) authentication between the GM and a key server (KS).

An authorization identity for a GDOI group is used to restrict registration of group members within a GDOI group. In order to successfully register with the KS, the DN or FQDN of the group members should match the configured identity string in this command. Use the authorization identity command to configure an authorization identity for a GDOI group.

Examples

The following example specifies an authorization identity using a DN called GETVPN_FILTER for the GETVPN GDOI group:

```
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# server local
Router(gdoi-local-server)# authorization identity GETVPN_FILTER
Router(gdoi-local-server)# exit
Router(config-gdoi-group)# exit
Router(config)# crypto indentity GETVPN_FILTER
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto identity	Configures the identity of a router with a given list of DNs in the certificate of the router.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

authorization list (global)

To specify the authentication, authorization, and accounting (AAA) authorization list, use the **authorization list** command in global configuration mode. To disable the authorization list, use the **no** form of this command.

authorization list *list-name*
no authorization list *list-name*

Syntax Description

list-name	Name of the AAA authorization list.

Command Default

An authorization list is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **authorization list** command to specify a AAA authorization list. For components that do not support specifying the application label, a default label of "any" from the AAA server will provide authorization. Likewise, a label of "none" from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent to a label of "none," but "none" is included for completeness and clarity.)

Examples

The following example shows that the AAA authorization list "maxaa" is specified:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization username	Specifies the parameters for the different certificate fields that are used to build the AAA username.

authorization list (tti-registrar)

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner in an Secure Device Provisioning (SDP) operation, use the **authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

authorization list *list-name*
no authorization list *list-name*

Syntax Description

list-name	Name of the list.

Command Default

There is no authorization list on the AAA server.

Command Modes

tti-registrar configuration

Command History

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

Usage Guidelines

This command is used in SDP operations. When the command is used, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```

Note The existence of a valid AAA username record is enough to pass the authentication check. The "cisco-avpair=tti" information is necessary only for the authorization check.

If a subject name was received in the authorization response, the TTI registrar stores it in the enrollment database, and that "subjectname" overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered "tti:iosconfig" values are expanded into the TTI Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.

Note The template configuration location may include a variable "$n," which is expanded to the name with which the user is logged in.

Examples

The following example shows that the authorization list name is "author-rad." In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an SDP operation.
debug crypto wui	Displays information about an SDP operation.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.
template username	Establishes a template username and password to access the configuration template on the file system.

authorization username

To specify the parameters for the different certificate fields that are used to build the authentication, authorization and accounting (AAA) username, use the **authorization username** command in global configuration mode. To disable the parameters, use the **no** form of this command.

authorization username {**subjectname** *subjectname*}
no authorization username {**subjectname** *subjectname*}

Syntax Description

subjectname	AAA username that is generated from the certificate subject name.
subjectname	Builds the username. The f**ollowing are**options that may be used as the AAA username: • **all** --Entire distinguished name (subject name) of the certificate. • **commonname** --Certificate common name. • **country** --Certificate country. • **email** --Certificate email. • **ipaddress** --Certificate ipaddress. • **locality** --Certificate locality. • **organization** --Certificate organization. • **organizationalunit** --Certificate organizational unit. • **postalcode** --Certificate postal code. • **serialnumber** --Certificate serial number. • **state** --Certificate state field. • **streetaddress** --Certificate street address. • **title** --Certificate title. • **unstructuredname** --Certificate unstructured name.

Command Default

Parameters for the certificate fields are not specified.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(11)T	The **all** option for the *subjectname argument*was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Examples

The following example shows that the serialnumber option is to be used as the authorization username:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

authorization username (tti-registrar)

To specify the parameters for the different certificate fields that are used to build the authentication, authorization, and accounting (AAA) username, use the **authorization username** command in tti-registrar configuration mode. To disable the parameters, use the **no** form of this command.

authorization username {**subjectname** *subjectname*}
no authorization username {**subjectname** *subjectname*}

Syntax Description

subjectname	AAA username that is generated from the certificate subject name.
subjectname	Builds the username. The f**ollowing**options can be used as the AAA username: • **all** --Entire distinguished name (subject name) of the certificate • **commonname** --Certificate common name • **country** --Certificate country • **email** --Certificate e-mail • **ipaddress** --Certificate IP address • **locality** --Certificate locality • **organization** --Certificate organization • **organizationalunit** --Certificate organizational unit • **postalcode** --Certificate postal code • **serialnumber** --Certificate serial number • **state** --Certificate state field • **streetaddress** --Certificate street address • **title** --Certificate title • **unstructuredname** --Certificate unstructured name

Command Default

Parameters for the certificate fields are not specified.

Command Modes

tti-registrar configuration

Command History

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

Examples

The following example shows that the **serialnumber** option is used as the authorization username:

```
aaa authorization network maxaaa group tacac+
```

```
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

authorize accept identity

To configure an identity policy profile, use the **authorize accept identity**command in parameter-map-type consent configuration mode. To remove an identity policy profile, use the **no** form of this command with the configured policy name.

authorize accept identity *identity-policy-name*
no authorize accept identity *identity-policy-name*

Syntax Description

identity-policy-name	Name of an identify profile.

Command Default

An identity policy does not exist.

Command Modes

Parameter-map-type consent (config-profile)

Command History

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

Usage Guidelines

If an identity policy is not configured, the interface policy will be used.

Examples

The following example shows how to configure accept policies within the consent-specific parameter maps:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

auth-type {**authorize** | **not-authorize**} **policy** *policy-name*
no auth-type {**authorize** | **not-authorize**} **policy** *policy-name*

Syntax Description

authorize	Policy is specified for all authorized devices.
not-authorize	Policy is specified for all unauthorized devices.
policy *policy-name*	Specifies the name of the identity policy to apply for the associated authentication result.

Command Default

A policy is not set for authorized or unauthorized devices.

Command Modes

Identity profile configuration

Command History

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

Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit
Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit
Router (config)# identity profile dot1x

Router (config-identity-prof)# auth-type authorize policy grant
```

Related Commands

Command	Description
identity policy	Creates an identity policy.
identity profile dot1x	Creates an 802.1x identity profile.

auth-type (ISG)

To specify the type of authorization Intelligent Services Gateway (ISG) will use for RADIUS clients, use the **auth-type**command in dynamic authorization local server configuration mode. To return to the default authorization type, use the **no** form of this command.

auth-type {**all** | **any** | **session-key**}
no auth-type

Syntax Description

all	All attributes must match for authorization to be successful. This is the default.
any	Any attribute must match for authorization to be successful.
session-key	The session-key attribute must match for authorization to be successful. **Note** The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid.

Command Default

All attributes must match for authorization to be successful.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

An ISG can be configured to allow external policy servers to dynamically send policies to the ISG. This functionality is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer to peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server. Use the **auth-type**command to specify the type of authorization ISG will use for RADIUS clients.

Examples

The following example configures the ISG authorization type:

```
aaa server radius dynamic-author
 client 10.0.0.1
 auth-type any
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures an ISG as a AAA server to facilitate interaction with an external policy server.

auto-enroll

To enable certificate autoenrollment, use the **auto-enroll** command in ca-trustpoint configuration mode. To disable certificate autoenrollment, use the **no** form of this command.

auto-enroll [*percent*] [**regenerate**]
no auto-enroll [*percent*] [**regenerate**]

Syntax Description

percent	(Optional) The renewal percentage parameter, causing the router to request a new certificate after the specified percent lifetime of the current certificate is reached. If the percent lifetime is not specified, the request for a new certificate is made when the old certificate expires. The specified percent value must not be less than 10 . If a client certificate is issued for less than the configured validity period due to the impending expiration of the certification authority (CA) certificate, the rollover certificate will be issued for the balance of that period. A minimum of 10 percent of the configured validity period, with an absolute minimum of 3 minutes is required, to allow rollover enough time to function.
regenerate	(Optional) Generates a new key for the certificate even if the named key already exists.

Command Default

Certificate autoenrollment is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(7)T	The *percent* argument was added to support key rollover.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the auto-enroll command to automatically request a router certificate from the CA that is using the parameters in the configuration. This command will generate a new Rivest, Shamir, and Adelman (RSA) key only if a new key does not exist with the requested label.

A trustpoint that is configured for certificate autoenrollment will attempt to reenroll when the router certificate expires.

Use the **regenerate** keyword to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded

and the new key pair is renamed with the name of the original key pair. Some CAs require a new key for reenrollment to work.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Note If you are using a Secure Shell (SSH) service, you should set up specific RSA key pairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructure share the same default RSA key pair, a temporary disruption of SSH service could occur. The RSA key pair could become invalid or change because of the CA system, in which case you would not be able to log in using SSH. You could receive the following error message: "key changed, possible security problem.")

Examples

The following example shows how to configure the router to autoenroll with the CA named "trustme1" on startup. In this example, the **regenerate** keyword is issued, so a new key will be generated for the certificate. The renewal percentage is configured as 90; so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires.

```
crypto ca trustpoint trustme1
 enrollment url http://trustme1.example.com/
 subject-name OU=Spiral Dept., O=example1.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
 password revokeme
 rsakeypair trustme1 2048
 exit
crypto ca authenticate trustme1
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca trustpoint	Declares the CA that your router should use.

auto-rollover

To enable the automated certificate authority (CA) certificate rollover functionality, use the **auto-rollover**command in certificate server mode. To disable the automated rollover functionality, use the **no** form of this command.

auto-rollover [*time-period*]
no auto-rollover

Syntax Description

time-period	(Optional) Indicates when the shadow CA certificate should be generated in absolute time (not a percentage). Default is 30 calendar days before the expiration of the active private key infrastructure (PKI) root certificate.

Command Default

Automated CA rollover is not enabled.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

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

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

CAs, like their clients, have certificates with expiration dates that have to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring it must generate a new certificate and possibly a new key pair. This process, called rollover, allows for continuous operation of the network while clients and the certificate server are switching from an expiring CA certificate to a new CA certificate.

The command **auto-rollover** initiates the automatic CA certificate rollover process.

Examples

The following example shows how to configure automated CA certificate rollover.

```
Router(config)# crypto pki server mycs
Router(cs-server)# auto-rollover 25
Router(cs-server)# no shut
%Some server settings cannot be changed after CA certificate generation.
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
```

```
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
Router(cs-server)#
```

With auto rollover enabled, the show crypto pki server command displays the current configuration of the certificate server.

```
Router# show crypto pki server
Certificate Server mycs:
    Status:enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name:CN=mycs
    CA cert fingerprint:70AFECA9 211CDDCC 6AA9D7FF 3ADB03AE
    Granting mode is:manual
    Last certificate issued serial number:0x1
    CA certificate expiration timer:00:49:26 PDT Jun 20 2008
    CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
    Current storage dir:nvram:
    Database Level:Minimum - no cert data written to storage
    Auto-Rollover configured, overlap period 25 days
    Autorollover timer:00:49:26 PDT May 26 2008....
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.

Command	Description
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

auto-update client

To configure automatic update parameters for an Easy VPN remote device, use the **auto-update client** command in global configuration mode. To disable the parameters, use the **no** form of this command.

auto-update client *type-of-system* **url** *url* **rev** *review-version*
no auto-update client *type-of-system* **url** *url* **rev** *review-version*

Syntax Description

type-of-system	Free-format string (see the table below).
url *url*	URL from which the Easy VPN device obtains the automatic update.
rev *review-version*	The version number is a comma-delimited string of acceptable versions.

Command Default

Automatic updates cannot occur.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The URL is a generic way to specify the protocol, username, password, address of the server, directory, and filename. The format of a URL is as follows: protocol://username:password@server address:port/directory/filename.

The automatic update on the remote device is triggered only if the current version of the software is earlier than the one specified in the revision string. Otherwise, the automatic update is ignored.

The table below lists possible free-format strings to be used for the type-of-system argument.

Table 3: Possible Free-format Strings

Free-Format String	Operating System
Win	Microsoft Windows
Win95	Microsoft Windows 95
Win98	Microsoft Windows 98
WinNt	Microsoft Windows NT
Win2000	Microsoft Windows 2000

Free-Format String	Operating System
Linux	Linux
Mac	Macintosh
VPN3002	Cisco VPN 3002 Hardware Client

Examples

The following example shows update parameters have been set for a Windows 2000 operating system, a URL of http:www.ourcompanysite.com/newclient, and versions 3.0.1(Rel) and 3.1(Rel):

```
crypto isakmp client configuration group {group-name
}
 auto-update client Win2000 url http:www.ourcompanysite.com/newclient rev 3.0.1(Rel),
3.1(Rel)
```

automate-tester (config-ldap-server)

To enable automated testing on the Lightweight Directory Access Protocol (LDAP) server, use the **automate-tester** command in LDAP server configuration mode. To disable automated testing, use the **no** form of this command.

automate-tester username *user* **probe-on**
no automate-tester username *user* **probe-on**

Syntax Description

username *user*	Specifies the automatic test username.
probe-on	Verifies the status of the server by sending a packet.

Command Default

Automated testing is disabled by default.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.4(2)T	This command was introduced.

Usage Guidelines

The **aaa new-model** command must be configured before issuing the **automate-tester** command.

Use the **automate-tester** command when clients (for example, dot1x) expect the state of the server (DEAD or ALIVE) before any request is sent to the AAA server.

Example

The following example shows how to enable automatic testing on the LDAP server:

```
Device> enable
Device# configure terminal
Device(config)# username user1 password 0 pwd1
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# deadtime 1
Device(config-ldap-server)# automate-tester username user1 probe-on
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ldap server	Specifies the name for the LDAP server configuration and enters LDAP server configuration mode.

automate-tester (config-radius-server)

To enable the automated testing feature for the RADIUS server, use the **automate-tester** command in RADIUS server configuration mode. To remove the automated testing feature, use the **no** form of this command.

automate-tester username *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*]
no automate-tester username *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*]

Syntax Description

username *user*	Specifies the automatic test user ID username.
ignore-auth-port	(Optional) Disables testing on the User Datagram Protocol (UDP) port for the RADIUS authentication server.
ignore-acct-port	(Optional) Disables testing on the UDP port for the RADIUS accounting server.
idle-time *minutes*	(Optional) Specifies the time, in minutes, for which the server remains idle before it is quarantined and test packets are sent out. The default value is 60.

Command Default

The automated testing feature is disabled for the RADIUS server accounting and authentication UDP ports.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **aaa new-model** command must be configured before issuing this command.

Use the **automate-tester** command to enable automatic testing on the RADIUS server accounting and authentication UDP ports for RADIUS server load balancing.

Examples

The following example shows how to enable automatic testing on the RADIUS server with the authorization and accounting ports specified with an idle time of 2 hours:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812
Device(config-radius-server)# automate-tester username user1 idle-time 120
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
address ipv6	Configures the IPv6 address for the RADIUS server accounting and authentication parameters.

Command	Description
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

auto secure

To secure the management and forwarding planes of the router, use the **auto secure** command in privileged EXEC mode.

auto secure [**management** | **forwarding**] [**no-interact** | **full**] [**ntp** | **login** | **ssh** | **firewall** | **tcp-intercept**]

Syntax Description

management	(Optional) Only the management plane will be secured.
forwarding	(Optional) Only the forwarding plane will be secured.
no-interact	(Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter.
full	(Optional) The user will be prompted for all interactive questions. This is the default.
ntp	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command line-interface (CLI).
login	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
ssh	(Optional) Specifies the configuration of the Secure Shell (SSH) feature in the AutoSecure CLI.
firewall	(Optional) Specifies the configuration of the firewall feature in the AutoSecure CLI.
tcp-intercept	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

Command Default

Autosecure is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)T.
12.3(4)T	The following keywords were added in Cisco IOS Release 12.3(4)T: **full**, **ntp**, **login**, **ssh**, **firewall**, and **tcp-intercept**
12.3(8)T	Support for the roll-back functionality and system logging messages were added to Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **auto secure** command allows a user to disable common IP services that can be exploited for network attacks by using a single CLI. This command eliminates the complexity of securing a router both by automating the configuration of security features and by disabling certain features that are enabled by default and that could be exploited for security holes.

Caution If you are using Security Device Manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

This command takes you through a semi-interactive session (also known as the AutoSecure dialogue) in which to secure the management and forwarding planes. This command gives you the option to secure just the management or forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

Caution If your device is managed by a network management (NM) application, securing the management plane could turn off vital services and disrupt the NM application support.

This command also allows you to go through all noninteractive configuration portions of the dialogue before the interactive portions. The noninteractive portions of the dialogue can be enabled by selecting the optional **no-interact**keyword.

Roll-back and System Logging Message Support

In Cisco IOS Release 12.3(8)T, support for roll-back of the AutoSecure configuration is introduced. Roll-back enables a router to revert back to its preautosecure configuration state if the AutoSecure configuration fails.

System Logging Messages capture any changes or tampering of the AutoSecure configuration that were applied on the running configuration.

Note Prior to Cisco IOS Release 12.3(8)T, roll-back of the AutoSecure configuration is unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Examples

The following example shows how to enable AutoSecure to secure only the management plane:

```
Router# auto secure management
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on your system, including the Cisco web browser user interface.
show auto secure config	Displays AutoSecure configurations.

backoff exponential

To configure the router for exponential backoff retransmit of accounting requests per RADIUS server or server group, enter the **backoff exponential** command in server-group RADIUS configuration mode or RADIUS server configuration mode. To disable this functionality, use the **no** form of this command.

backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]
no backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

Syntax Description

max-delay *minutes*	(Optional) Number of retransmissions done in exponential max-delay mode. The max-delay mode indicates that the router starts retransmitting with a minimum time that keeps doubling with each retransmit failure until the maximum configured delay time is reached. The valid range for the *minutes* argument is 1 through 120; if the *minutes* value is not specified, the default value of 60 will be used.
backoff-retry *retransmits*	(Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. The valid range for the *retransmits* argument is 1 through 50; if the *retransmits* value is not specified, the default value of 5 will be used.

Command Default

This command is disabled.

Command Modes

Server-group RADIUS configuration (config-sg-radius)

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.2(2)T	This command was modified. The RADIUS server configuration (config-radius-server) mode was added to this command.

Usage Guidelines

Before enabling the **backoff exponential** command, you must configure one of the following commands:

- The **aaa group server radius** command allows you to specify a server group and enter server-group RADIUS configuration mode.
- The **radius server** command allows you to enter the RADIUS server configuration mode.

The **backoff exponential** command allows you to configure an exponential backoff retransmission per RADIUS server or server group. That is, after the normally configured retransmission retries have been used, the router will keep on trying with an interval that doubles on each retransmit failure until a configured maximum interval is reached. This functionality allows you to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

Examples

The following example shows how to configure an exponential backoff retransmission in the server-group RADIUS configuration (config-sg-radius) mode:

```
Device(config)# aaa group server radius cat
Device(config-sg-radius)# backoff exponential max-delay 90 backoff-retry 10
```

The following example shows how to configure an exponential backoff retransmission in the RADIUS server configuration (config-radius-server) mode:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2 acct-port 1813 auth-port 1812
Device(config-radius-server)# backoff exponential max-delay 60 backoff-retry 32
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.
radius-server backoff exponential	Configures the router for exponential backoff retransmit of accounting requests.

backup-gateway

To configure a server to "push down" a list of backup gateways to the client, use the **backup-gateway** command in global configuration mode or IKEv2 authorization policy configuration mode. To remove a backup gateway, use the **no** form of this command.

backup-gateway {*ip-addresshostname*}
no backup-gateway {*ip-addresshostname*}

Syntax Description

ip-address	IP address of the gateway.
hostname	Host name of the gateway.

Command Default

A list of backup gateways is not configured.

Command Modes

Global configuration (config)

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

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Before using the **backup-gateway** command, you must first configure the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command.

When using this command with the **crypto ikev2 authorization policy** command to configure a backup gateway, you can configure up to ten backup gateway commands. FlexVPN server pushes the configured backup gateways to the client via Cisco Unity attribute MODECFG_BACKUPSERVERS.

An example of an attribute-value (AV) pair for the backup gateway attribute is as follows:

```
ipsec:ipsec-backup-gateway=10.1.1.1
```

Examples

The following example shows that gateway 10.1.1.1 has been configured as a backup gateway:

```
crypto isakmp client configuration group group1
 backup-gateway 10.1.1.1
```

The following output example shows that five backup gateways have been configured:

```
crypto isakmp client configuration group sdm
 key 6 RMZPPMRQMSdiZNJg`EBbCWTKSTi\d[
 pool POOL1
 acl 150
```

```
 backup-gateway 172.16.12.12
 backup-gateway 172.16.12.13
 backup-gateway 172.16.12.14
 backup-gateway 172.16.12.130
 backup-gateway 172.16.12.131
 max-users 250
 max-logins 2
```

The following example shows how to configure five backup gateways.

```
crypto ikev2 authorization policy policy1
 backup-gateway gw1
 backup-gateway gw2
 backup-gateway gw3
 backup-gateway 1.1.1.1
 backup-gateway 1.1.1.2
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

backup group

To add a peer to a backup group, use the **backup group** in the IKEv2 FlexVPN client profile configuration mode. To declare a peer as part of no group, use the **no** form of this command.

backup group {*group-number* | **default**}
no backup group

Syntax Description

group-number	Backup group number.
default	The default group.

Command Default

The clients belong to the backup group 0 and are not nvgened.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

If two peers are in the same backup group, they will try to connect to each of their peer in the same order as described in the backup gateway list. The only difference is that they will refrain from connecting to the same peer at the same moment.

If the peers are not present in the same backup group, they live an independent life and connect to their peers in the order described in backup gateway list but will not look at each other and may end up connecting to the same peer if the configuration authorizes it.

Note Any changes to this command terminates the active session.

Examples

The following example shows how to configure the **backup group** command:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# backup group default
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

banner

To configure an extended authentication (Xauth) banner string under a group policy definition, use the **banne**r command in global configuration mode. To disable the banner, use the **no** form of this command.

banner c *banner-text* **c**
no c *banner-text* **c**

Syntax Description

c	Delimiting character that must precede and follow the banner text. The delimiting character may be a character of your choice, such as "c" or "@."
banner-text	Text string of the banner. Maximum number of characters = 1024.

Command Default

If a banner is not configured, a banner will not be displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Examples

The following example shows that the banner "The quick brown fox jumped over the lazy dog" has been specified:

```
crypto isakmp client configuration group EZVPN
 banner @ The quick brown fox jumped over the lazy dog @
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

banner (parameter-map webauth)

To display a banner on the web-authentication login web page, use the **banner** command in parameter map webauth configuration mode. To disable the banner display, use the **no** form of this command.

banner [**file** *location*:*filename* | **text** *banner-text*]
no banner [**file** *location*:*filename* | **text** *banner-text*]

Syntax Description

file *location*:*filename*	(Optional) Specifies a file that contains the banner to display on the web authentication login page.
text *banner-text*	(Optional) Specifies a text string to use as the banner. You must enter a delimiting character before and after the banner text. The delimiting character can be any character of your choice, such as "c" or "@."

Command Default

No banner displays on the web-authentication login web page.

Command Modes

Parameter map webauth configuration (config-params-parameter-map)

Command History

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

Usage Guidelines

The **banner** command allows you to configure one of three possible scenarios:

- The **banner** command without any keyword or argument—Displays the default banner using the name of the device: "Cisco Systems, <device's hostname> Authentication."
- The **banner** command with the **file** *filename* keyword-argument pair—Displays the banner from the custom HTML file you supply. The custom HTML file must be stored in the disk or flash of the device.
- The **banner** command with the **text** *banner-text* keyword-argument pair—Displays the text that you supply. The text must include any required HTML tags.

Note If the **banner** command is not enabled, nothing displays on the login page except text boxes for entering the username and password.

Examples

The following example shows that a file in flash named webauth_banner.html is specified for the banner:

```
parameter-map type webauth MAP_1
 type webauth
 banner file flash:webauth_banner.html
```

The following example shows how to configure the message "login page banner" by using "c" as the delimiting character, and it shows the resulting configuration output.

```
Device(config-params-parameter-map)# banner text c login page banner c
```

```
parameter-map type webauth MAP_2
 type webauth
 banner text ^c login page banner ^c
```

Note The caret symbol (^) displays in the configuration output before the delimiting character that you entered even though you do not enter it.

Related Commands

Command	Description
consent email	Requests a user's e-mail address on the web-authentication login web page.
redirect (parameter-map webauth)	Redirects users to a particular URL during web-based authentication.
show ip admission status banner	Displays information about configured banners for web authentication.

banner (WebVPN)

To configure a banner to be displayed after a successful login, use the **banner** command in webvpn group policy configuration mode or IKEv2 authorization policy configuration mode. To remove the banner, use the **no** form of this command.

banner *string*
no banner

Syntax Description

string	Text string that contains 7-bit ASCII values and HTML tags and escape sequences. The text banner must be in quotation marks if it contains spaces.

Command Default

A banner is not configured.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

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

Command History

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

Usage Guidelines

Before using this command, you must first configure the **crypto ikev2 authorization policy** command.

When using this command with the **crypto ikev2 authorization policy** command, the format of the banner text shoule be 'c banner-text c', where 'c' is a delimiting character. Any character can be used as a delimiting character. The banner text can have spaces, special characters and can span multiple lines. FlexVPN server pushes the banner to the client via Cisco Unity attribute MODECFG_BANNER.

Examples

The following example configures “Login Successful” to be displayed after login:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner “Login Successful”
Router(config-webvpn-group)#
```

This example shows how to display banner text that has spaces, spans multiple lines and is delimited by character 'z'

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-author-policy)# banner z
Enter TEXT message. End with the character 'z'.
This is banner text
z
Router# show run | beg policy2
crypto ikev2 authorization policy policy2
banner ^C
This
is
banner text
```

```
^C
!
Router# sh cry ikev2 authorization policy policy2
IKEv2 Authorization Policy : policy2
Banner :
This
is
banner text
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

base-dn

To configure a base distinguished name (DN) that you want to use to perform search operations in the Lightweight Directory Access Protocol (LDAP) server directory tree, use the **base-dn** command in LDAP server configuration mode. To delete a configured base DN for the LDAP server, use the **no** form of this command.

base-dn *string*
no base-dn *string*

Syntax Description

string	Distinguished name of the search base.

Command Default

No distinguished names are created.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

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

Usage Guidelines

This command is valid only for LDAP servers. A base DN can take a form such as dc=example,dc=domain, where the base DN uses the Domain Name Server (DNS) domain name as its basis and is split into the domain components.

Examples

The following example shows how to configure the base DN for an LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"
```

Related Commands

Command	Description
ipv4 (l**dap)**	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap)**	Configures the transport protocol for establishing a connection with the LDAP server.

bidirectional

To enable incoming and outgoing IP traffic to be exported across a monitored interface, use the **bidirectional** command in router IP traffic export (RITE) configuration mode. To return to the default functionality, use the **no** form of this command.

bidirectional
no bidirectional

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not enabled, only incoming traffic is exported.

Command Modes

RITE configuration

Command History

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

Usage Guidelines

By default, only incoming IP traffic is exported. If you choose to export outgoing IP traffic, you must issue both the **bidirectional** command, which enables outgoing traffic to be exported, and the **outgoing** command, which specifies how the outgoing traffic will be filtered.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples

The following example shows how to export both incoming and outgoing IP traffic on the FastEthernet interface:

```
Router(config)# ip traffic-export profile johndoe
Router(config-rite)# interface FastEthernet1/0.1
Router(config-rite)# bidirectional

Router(config-rite)# incoming access-list 101

Router(config-rite)# outgoing access-list 101

Router(config-rite)# mac-address 6666.6666.3333
```

Related Commands

Command	Description
interface (RITE)	Specifies the outgoing interface for exporting traffic.

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

binary file

To specify the binary file location on the registrar and the destination binary file location on the petitioner, use the **binary file** command in tti-registrar configuration mode.

binary file *sourceURL destinationURL*

Syntax Description

sourceURL	Specifies the source URL on the registrar for the binary file using one of the keywords in .
destinationURL	Specifies the destination URL on the petitioner for binary file using one of the keywords in .

Command Default

None

Command Modes

tti-registrar configuration (tti-registrar)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **binary file** command to specify the location where a binary file will be retrieved from and copied to during the Trusted Transitive Introduction (TTI) exchange. There may be up to nine binary files transferred, each with a different source and destination location. A destination URL could also be a token on the petitioner, such as usbtoken0:

The binary files are retrieved from the registrar and copied to the petitioner. Source URLs for the binary file location are expanded on the registrar. Destination URLs are expanded on the petitioner. Binary files are not processed through the binary expansion functions.

Table 4: Source and Destination URL Keywords

Keyword	Description
archive:	Retrieves from the archive location.
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
disk0:	Retrieves from disk0.
disk1:	Retrieves from disk1.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server.

Keyword	Description
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tar:	Retrieves from a compressed file in tar format.
tftp:	Retrieves from a TFTP network server.
tmpsys:	Retrieves from a temporary system location.
unix:	Retrieves from the UNIX system location.
usbtoken:	Retrieves from the USB token.

Examples

The following example shows how to specify on the registrar where the source binary files are located and where the binary files will be copied to on the petitioner:

```
crypto provisioning registrar
  pki-server cs1
  binary file http://myserver/file1 usbtoken0://file1
  binary file http://myserver/file2 flash://file2
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a secure device provisioning (SDP) registrar and enter tti-registrar configuration mode.
template file	Specifies the source template file location on the registrar and the destination template file location on the petitioner.

bind authenticate

To authenticate the client to a Lightweight Directory Access Protocol (LDAP) server, use the **bind authenticate** command in LDAP server configuration mode. To disable authenticated bind and to allow anonymous bind, use the **no** form of this command.

bind authenticate root-dn *username* **password** [**0** *string* | **6** *string* | **7** *string*] *string*
no bind authenticate root-dn *username* **password** [**0** *string* | **6** *string* | **7** *string*] *string*

Syntax Description

root-dn	Specifies the bind distinguished name (DN) for an authenticated user.
username	Root user of the LDAP server.
password	Specifies the LDAP server password.
0	(Optional) Specifies the unencrypted (cleartext) shared key.
6	(Optional) Specifies the advanced encryption scheme (AES) encrypted key. **Note** Type 6 AES encrypted passwords are configured using the **password encryption aes** command.
7	(Optional) Specifies the hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

Anonymous bind is performed. Anonymous bind refers to a simple bind operation with no DN and password.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.4(1)T	This command was modified. The **6** keyword was added.

Examples

The following example shows how to authenticate the “user1” user to the LDAP server using the password “123”:

```
Device> enable
Device# configure terminal
Device(config)# ldap server server1
Device(config-ldap-server)# bind authenticate root-dn
cn=user1,cn=users,dc=nac-blr2,dc=example,dc=com password 123
```

Related Commands

Command	Description
ipv4 (**ldap**)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
password encryption aes	Enables a type 6 encrypted preshared key.
transport port (ldap)	Configures the transport protocol for establishing a connection with the LDAP server.

block count

To lock out group members for a length of time after a set number of incorrect passwords are entered, use the **block count**command in local RADIUS server group configuration mode. To remove the user block after invalid login attempts, use the **no** form of this command.

block count *count* **time** {**seconds** | **infinite**}
no block count *count* **time** {**seconds** | **infinite**}

Syntax Description

count	Number of failed passwords that triggers a lockout. Range is from 1 to 4294967295.
time	Specifies the time to block the account.
seconds	Number of seconds that the lockout should last. Range is from 1 to 4294967295.
infinite	Specifies the lockout is indefinite.

Command Default

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

If the **infinite keyword**is entered, an administrator must manually unblock the locked username.

Examples

The following command locks out group members for 120 seconds after three incorrect passwords are entered:

```
Router(config-radsrv-group)#
block count 3 time 120
```

Related Commands

Command	Description
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

browser-attribute import

To import user-defined browser attributes into a webvpn context, use the **browser-attribute import**command in webvpn context configuration mode. To remove a browser attribute, use the **no** form of this command.

browser-attribute import *device* **:** *file*
no browser-attribute import *device* **:** *file*

Syntax Description

device **:** *file*	• *device* **:** --Storage device on the system. • *file* --Name of file to be imported. The file name should include the directory location.

Command Default

Default values of the attributes are used.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(22)T	This command was introduced. Attributes that are currently supported are primary color, secondary color, text color, secondary text color, login-message, browser title, and title color.

Usage Guidelines

This command will override any other browser attributes that have already been configured using command-line interface (CLI).

Examples

The following example shows that the file "test-attr.xml" is to be imported from flash:

```
Router (config)# webvpn context sslvpn
 Router (config-webvpn-context)# browser-attribute import flash:test-attr.xml
```

Related Commands

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

browser-proxy

To apply browser-proxy parameter settings to a group, use the **browser-proxy** command in ISAKMP group configuration mode. To disable the parameter settings, use the **no** form of this command.

browser-proxy *browser-proxy-map-name*
no browser-proxy *browser-proxy-map-name*

Syntax Description

browser-proxy-map-name	Name of the browser proxy.

Command Default

Browser-proxy settings are not applied to a group.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Ensure that you define the browser proxy name before you define the crypto Internet Security Association and Key Management Protocol (ISAKMP) client configuration group name. The two names have to be the same.

Examples

The following example shows that browser proxy map “EZVPN” has been applied to the group “EZVPN”:

```
crypto isakmp client configuration group EZVPN
 browser-proxy EZVPN
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.