

# 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**

<b>Syntax Description</b>	<b>no-auth</b> (Optional) Specifies that authentication is bypassed for this user.
---------------------------	--

<b>Command Default</b>	No requests are cached.
------------------------	-------------------------

<b>Command Modes</b>	Profile map configuration (config-profile-map)
----------------------	--

<b>Command History</b>	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.

<b>Usage Guidelines</b>	Use the <b>all</b> command to cache all authentication and authorization requests.
	Use the <b>all</b> command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

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

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

<b>Related Commands</b>	<b>profile</b>	Defines or modifies an individual authentication and authorization cache profile based on an exact username match.
	<b>regex</b>	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**

**off**

## 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
<b>parameter-map type urlfilter</b>	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
                    policy-name
```

## Syntax Description

Name of application policy.

## Defaults

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 (application firewall policy)

## Syntax Description

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 <b>im</b> , <b>aol</b> , <b>yahoo</b> , and <b>msn</b> keywords were introduced to support instant message traffic detection and prohibition.

## Examples

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

### HTTP-Specific Inspection Commands

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

- 
- 
- **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.

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:

## ■ application (application firewall policy)

```
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**

<b>Command</b>	<b>Description</b>
	Defines an application firewall policy and puts the router in application firewall policy 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 arap authentication` form of this command.

```

arap authentication {
    | list-name } [
    | list-name }
    
```



**Caution**

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

**Syntax Description**

	Default list created with the <code>aaa authentication</code> command.
<i>list-name</i>	Indicated list created with the <code>aaa authentication</code> command.
	(Optional) Accepts the username and password in the username field.

**Defaults**

ARAP authentication uses the default set with the `aaa authentication` 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 <code>arap authentication</code> 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` command. Entering the `arap authentication` version of `arap authentication` has the same effect as entering the command with the `arap authentication` keyword. Before issuing this command, create a list of authentication processes by using the `aaa authentication` 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
---------	-------------

---

# ase collector

*ip-address*

*ip-address*

---

## Syntax Description

---



---

## Command Default

---



---

## Command Modes

---



---

## Command History

Release	Modification

---



---

## Usage Guidelines

---



---

## Examples

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

---

## Related Commands

Command	Description
ase enable	
ase group	
ase signature extraction	
clear ase signature	
debug ase	
show ase	

---

# ase enable

ase enable

no

ase enable

no ase enable

---

## Syntax Description

---

## Command Default

---

## Command Modes

---

## Command History

Release	Modification

---

## Usage Guidelines

---

## Examples

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

---

## Related Commands

Command	Description
ase collector	
ase group	
ase signature extraction	
clear ase signature	
debug ase	
show ase	

# ase group

ase group

no

**ase group** *TIDP-group-number*

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

---

*TIDP-group-number*

---

---

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

---

---

**ase collector**

---

**ase enable**

---

**ase signature  
extraction**

---

**clear ase signature**

---

**debug ase**

---

**show ase**

---

# ase signature extraction

ase signature

```

extraction
  no
ase signature extraction
no ase signature extraction
    
```

---

## Syntax Description

---

## Command Default

---

## Command Modes

---

## Command History

Release	Modification

---

## Usage Guidelines

---

## Examples

```

ase signature extraction
    
```

---

## Related Commands

Command	Description
ase collector	
ase group	
ase enable	
clear ase signature	
debug ase	
show ase	

# 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          [          [          ]...]

no attribute number [number [number]...]
```

---

<i>number [number [number]...]</i>	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.
------------------------------------	--

---



---

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

---

Server-group configuration

---

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.

---



---

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:

-

-

-

- 

-

-

-

-

**Note**


---

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”:

```
attribute 2,4,12,217,6-10,13
attribute 64-69,218
```

**Related Commands**

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

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*]

*format-type* [*string*]

<i>format-type</i>	Type of format (see <a href="#">Table 22</a> ).
<i>string</i>	(Optional) Pattern of the data format (see <a href="#">Table 23</a> ).

Default format type is used for all services.

Server-group configuration

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

The following format types may be configured.

**Table 22** *Format Types*

	Format is type, channel, or port.
	Either interface(16), isdn(16), or async(16).
	Data format (bits): shelf(2), slot(4), port(5), or channel(5).
	Data format (bits): slot(4), module(1), port(3), vpi(8), or vci(16).
	Configurable data format (see <a href="#">Table 23</a> ).

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

**Table 23** *Characters Supported by Format-Type e*

<b>0</b>	Zero
<b>1</b>	One
<b>f</b>	DS0 shelf
<b>s</b>	DS0 slot

**Characters Supported by Format-Type e (continued)**

<b>a</b>	DS0 adapter
<b>P</b>	DS0 port
<b>i</b>	DS0 subinterface
<b>c</b>	DS0 channel
<b>F</b>	Async shelf
<b>S</b>	Async slot
<b>P</b>	Async port
<b>L</b>	Async line
<b>S</b>	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]).
<b>A</b>	PPPoX adapter
<b>P</b>	PPPoX port
<b>V</b>	PPPoX VLAN ID
<b>I</b>	PPPoX virtual path identifier (VPI)
<b>C</b>	PPPoX virtual channel indicator (VCI)
<b>U</b>	Session ID

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:

```
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
```

<b>aaa group server radius</b>	Groups different RADIUS server hosts into distinct lists and distinct methods.
<b>ip radius source-interface</b>	Forces RADIUS to use the IP addressing of a specified interface for all outgoing RADIUS packets.
<b>radius-server host</b>	Specifies a RADIUS server host.

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
```

---

*name*

---

*value*

---

**service** *service*

---

**protocol** *protocol*

---

*tag*

---

---

**no**

---

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

---

### **aaa attribute list**

---

# audit filesize

**audit filesize**  
no

**audit filesize** *size*

**no audit filesize** *size*

<b>Syntax Description</b>	Size of the audit file in KB. Valid values range from 32 KB to 128 KB. 32 KB is the default size.
---------------------------	---

<b>Defaults</b>	The audit file is 32 KB.
-----------------	--------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	
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.

<b>Usage Guidelines</b>	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.

<b>Examples</b>	The following example shows how to change the audit file size to 128 KB:
-----------------	--

```
audit filesize 128
```

---

<b>audit interval</b>	Changes the time interval that is used for calculating hashes.
<b>show audit</b>	Displays contents of the audit file.

---

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**

**no audit interval**

---

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

---

---

300 seconds (5 minutes)

---

Global configuration

---

---

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.

---

---

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.

---



---

Audit logs are enabled by default and cannot be disabled.

---

---

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

```
audit interval 120
```

---

<b>audit filesize</b>	Changes the size of the audit file.
-----------------------	-------------------------------------

<b>show audit</b>	Displays contents of the audit file.
-------------------	--------------------------------------

---

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}

---

<b>on</b>	Audit trail messages are generated.
<b>off</b>	Audit trail messages are not generated.

---

---

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

---

cfg-appfw-policy-http configuration  
cfg-appfw-policy-aim configuration  
cfg-appfw-policy-ymsgr configuration  
cfg-appfw-policy-msnmsgr configuration

---

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

---

---

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- configuration mode, where “ ” is dependent upon the specified protocol.

---

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.

---

---

**ip inspect audit-trail** Turns on audit trail messages.

---

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}**

---

<b>on</b>	Audit trail messages will be issued.
<b>off</b>	Audit trail messages will not be issued.

---

---

There are no audit trail messages.

---

Parameter-map type inspect configuration  
URL parameter-map configuration

---

12.4(6)T	This command was introduced.
----------	------------------------------

---

---

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.

---

The following example generates audit trail messages:

---

---

**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 (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 authentication` form of this command.

```
authentication { method | pre-share }
```

Syntax Description	Command	Description
	<code>rsa-sig</code>	Specifies RSA signatures as the authentication method. This method is not supported in IPv6.
	<code>rsa-encr</code>	Specifies RSA encrypted nonces as the authentication method. This method is not supported in IPv6.
	<code>pre-share</code>	Specifies preshared keys as the authentication method.

**Command Default** The RSA signatures authentication method is used.

**Command Modes** ISAKMP policy configuration

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.

**Usage Guidelines** 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 `crypto isakmp identity` 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):

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

# 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.

## Defaults

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":

```
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
		Specifies the URL of the CA server to which to send authentication requests.
		Defines an enrollment profile.
		Specifies parameters for an enrollment profile.

# 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 authentication control-direction` form of this command.

```
{ | }
```

## Syntax Description

Enables bidirectional control on the port.

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 command in global configuration mode. To remove a previously configured recovery delay, use the form of this command.

*milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	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.
---------------------------	---------------------	---

<b>Command Default</b>	The default delay is 1000 milliseconds.
------------------------	---

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SXI	This command was introduced.

<b>Examples</b>	<p>The following example shows how to configure the critical recovery delay period to 1500 milliseconds:</p> <pre>Switch(config)# authentication critical recovery delay 1500</pre>
-----------------	---

# 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 authentication event fail` form of this command.

```
authentication event fail [ retry-count ] { vlan-id | next-method }
```

**no authentication event fail**

Syntax Description	retry	(Optional) Specifies how many times the authentication method is tried after an initial failure.
	<b>action</b>	
	<b>authorize vlan</b>	
	<b>next-method</b>	
	<b>authentication order</b>	

**Command Default** Authentication is attempted two times after the initial failed attempt.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification

**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
	<b>authentication event no-response action</b>	
	<b>authentication order</b>	

# authentication event no-response action

authentication event no-response action  
no

authentication event no-response action authorize vlan

no authentication event no-response

---

## Syntax Description

authorize vlan

---



---

## Command Default

---

## Command Modes

---

## Command History

Release	Modification

---



---

## Usage Guidelines

authentication event no-response action

---

## Examples

```
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	

---

# authentication event server alive action reinitialize

authentication event server

```

alive action reinitialize
no

authentication event server alive action reinitialize

no authentication event server alive action reinitialize

```

---

## Syntax Description

---

## Command Default

---

## Command Modes

---

## Command History

Release	Modification

---

## Usage Guidelines

authentication event server alive action reinitialize

---

## Examples

```

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
<b>authentication event server dead action authorize</b>	

# authentication event server dead action authorize

```
authentication event server dead action authorize
no
```

```
authentication event server dead action authorize vlan
```

```
no authentication event server dead action authorize
```

---

## Syntax Description

vlan

---



---

## Command Default

---

## Command Modes

---

## Command History

Release	Modification

---



---

## Usage Guidelines

authentication event server dead action authorize

---

## Examples

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

---

## Related Commands

Command	Description
authentication event server alive action reinitialize	

---

# authentication fallback

**authentication fallback**  
**no**

**authentication fallback** *fallback-profile*

**no authentication fallback**

---

**Syntax Description**

*fallback-profile*

---

---

**Command Default**

---

**Command Modes**

---

**Command History**

---

---

---

**Usage Guidelines**

**authentication fallback**  
**fallback profile**

---

**Examples**

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

---

---

---

```
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
```

*list-name*

*list-name*

---

*list-name*

---

---

```
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
```

---

---

---

---



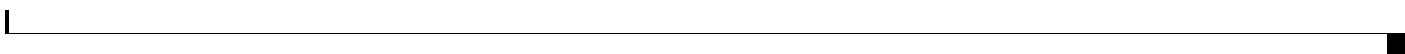
---

---

---

---





---

---

---

---

---

---

---

---

*session-type*

---

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

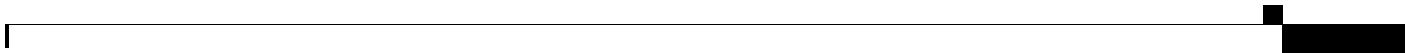
```
Router(config-if)# no authentication open  
Router(config-if)#
```

---

---

---

---



```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# authentication order mab dot1x
Switch(config-if)# end
Switch#
```

---

---

---

---

---

---

---

---

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

---

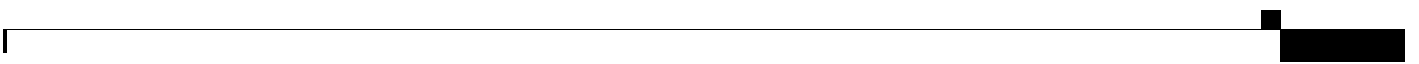
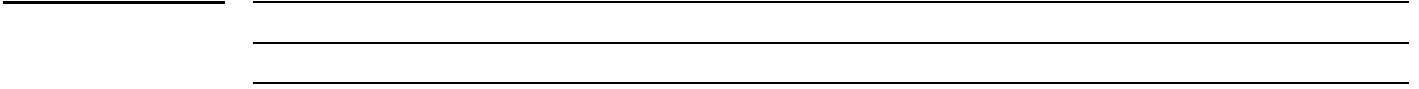
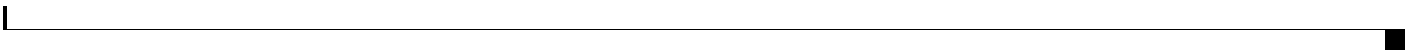
---

---

---

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interface ethernet0/2
Switch(config-if)# authentication port-control auto
```



```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# authentication order mab dot1x webauth
Switch(config-if)# authentication priority dot1x mab
Switch(config-if)# end
Switch#
```

| \_\_\_\_\_ ■

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

| \_\_\_\_\_ ■

---

---

---

---

---

---

---

---

---

---

```
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
```

---

---

---

---

---

---

---

---

---

---







*trustpoint-label* |

*trustpoint-label* |

---

*trustpoint-label*

---

---

---

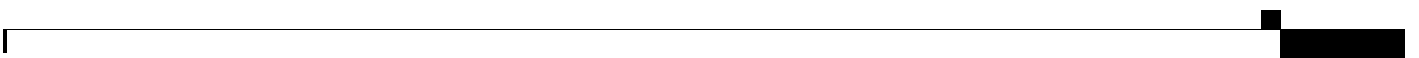
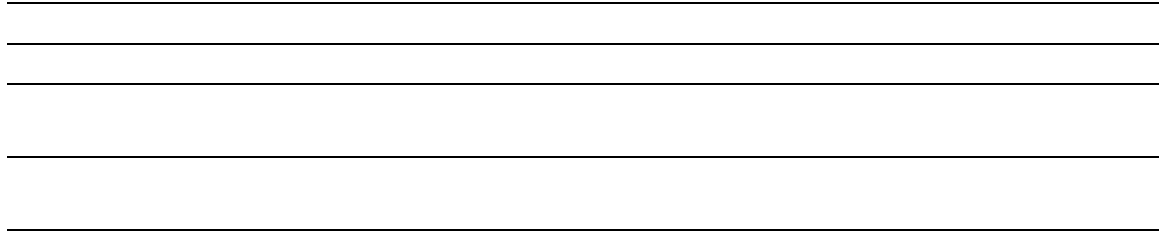
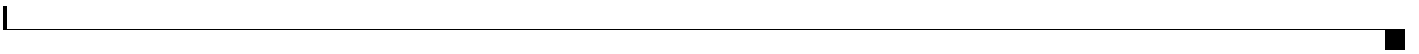
---

---

crypto provisioning registrar  
authentication trustpoint mytrust

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

---





*url*

*url*

---

*url*

*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.)

---

12.2(13)ZH

This command was introduced.

---

12.3(4)T

This command was integrated into Cisco IOS Release 12.3(4)T.

---

*url*

---

```
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
```

---

---

Specifies the HTTP command that is sent to the CA for authentication.

---

Defines an enrollment profile.

---

Specifies the enrollment parameters of your CA.

---

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

```

aaa authorization { exec | exec-shell | exec-shell | exec-shell } [ level | list-name ]
no aaa authorization { exec | exec-shell | exec-shell | exec-shell } [ level | list-name ]

```

	Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol.
	Enables authorization on the selected lines for all commands at the specified privilege level.
<i>level</i>	Specific command level to be authorized. Valid entries are 0 through 15.
	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines.
	Enables authorization to determine if the user is allowed reverse access privileges.
	(Optional) The name of the default method list, created with the <code>aaa authorization</code> command.
<i>list-name</i>	(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 <code>aaa authorization</code> command.

Authorization is not enabled.

Line configuration

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.

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 `aaa 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.

---

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

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

---

---

Sets parameters that restrict user access to a network.

---

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

```
no authorization [request | reply] [accept | reject]
```

**no authorization** [request | reply] [accept | reject]

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

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

Server-group configuration

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 <b>request</b> and <b>reply</b> keywords were added.
12.3(7)T	The <b>request</b> and <b>reply</b> 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.

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.



---

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.

---

---

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
```

---

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

---

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}

---

<b>login</b>	Use the username of the introducer for AAA authorization.
<b>certificate</b>	Use the certificate of the petitioner for AAA authorization.
<b>login certificate</b>	Use the username of the introducer and the certificate of the petitioner for AAA authorization.

---

---

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

---

tti-registrar configuration

---

12.3(14)T	This command was introduced.
-----------	------------------------------

---

---

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.

---

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
```

---

<b>authorization list (tfti-registrar)</b>	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 {
```

```
no authorization address ipv4 {
```

## Syntax Description

A hostname or distinguished name (DN).

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
<b>crypto gdoi group</b>	Identifies a GDOI group and enters GDOI group configuration mode.
<b>server local</b>	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**

**no authorization list**

## Syntax Description

Name of the AAA authorization list.

## Defaults

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
<b>authorization username</b>	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**

**no authorization list**

### Syntax Description

Name of the list.

### Defaults

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="ttdi:subjectname=<<DN subjectname>>"
  cisco-avpair="ttdi:iosconfig#<<value>>"
  cisco-avpair="ttdi:iosconfig#<<value>>"
  cisco-avpair="ttdi: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)#
Router(tti-registrar)#
Router(tti-registrar)#
Router(tti-registrar)#
Router(tti-registrar)#
Router(tti-registrar)#
Router(tti-registrar)#
```

**Related Commands**

Command	Description
<b>authentication list (tti-registrar)</b>	Authenticates the introducer in an SDP operation.
<b>debug crypto wui</b>	Displays information about an SDP operation.
<b>template config</b>	Specifies a remote URL for a Cisco IOS CLI configuration template.
<b>template username</b>	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

<b>subjectname</b>	AAA username that is generated from the certificate subject name.
<i>subjectname</i>	Builds the username. The following are options that may be used as the AAA username: <ul style="list-style-type: none"> <li>• <b>all</b>—Entire distinguished name (subject name) of the certificate.</li> <li>• <b>commonname</b>—Certificate common name.</li> <li>• <b>country</b>—Certificate country.</li> <li>• <b>email</b>—Certificate email.</li> <li>• <b>ipaddress</b>—Certificate ipaddress.</li> <li>• <b>locality</b>—Certificate locality.</li> <li>• <b>organization</b>—Certificate organization.</li> <li>• <b>organizationalunit</b>—Certificate organizational unit.</li> <li>• <b>postalcode</b>—Certificate postal code.</li> <li>• <b>serialnumber</b>—Certificate serial number.</li> <li>• <b>state</b>—Certificate state field.</li> <li>• <b>streetaddress</b>—Certificate street address.</li> <li>• <b>title</b>—Certificate title.</li> <li>• <b>unstructuredname</b>—Certificate unstructured name.</li> </ul>

## Defaults

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 <b>all</b> option for the <i>subjectname</i> 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**

<b>Command</b>	<b>Description</b>
<b>authorization list</b>	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

<b>subjectname</b>	AAA username that is generated from the certificate subject name.
<i>subjectname</i>	Builds the username. The following options can be used as the AAA username: <ul style="list-style-type: none"> <li>• <b>all</b>—Entire distinguished name (subject name) of the certificate</li> <li>• <b>commonname</b>—Certificate common name</li> <li>• <b>country</b>—Certificate country</li> <li>• <b>email</b>—Certificate e-mail</li> <li>• <b>ipaddress</b>—Certificate IP address</li> <li>• <b>locality</b>—Certificate locality</li> <li>• <b>organization</b>—Certificate organization</li> <li>• <b>organizationalunit</b>—Certificate organizational unit</li> <li>• <b>postalcode</b>—Certificate postal code</li> <li>• <b>serialnumber</b>—Certificate serial number</li> <li>• <b>state</b>—Certificate state field</li> <li>• <b>streetaddress</b>—Certificate street address</li> <li>• <b>title</b>—Certificate title</li> <li>• <b>unstructuredname</b>—Certificate unstructured name</li> </ul>

### Defaults

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
```

## ■ authorization username (tli-registrar)

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>authorization list</b>	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.

**authorize accept identity** *identity-policy-name*

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

## Syntax Description

*identity-policy-name* Name of 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

<b>authorize</b>	Policy is specified for all authorized devices.
<b>not-authorize</b>	Policy is specified for all unauthorized devices.
<b>policy</b> <i>policy-name</i>	Specifies the name of the identity policy to apply for the associated authentication result.

## Defaults

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)#
Router (config-ext-nacl)#
Router (config-ext-nacl)#

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

Router (config)#
Router (config-identity-prof)#
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>identity policy</b>	Creates an identity policy.
<b>identity profile dot1x</b>	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** {all | any | session-key }

## Syntax Description

<b>all</b>	All attributes must match for authorization to be successful. This is the default.
<b>any</b>	Any attribute must match for authorization to be successful.
<b>session-key</b>	The session-key attribute must match for authorization to be successful. <b>Note</b> 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

## 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
<b>aaa server radius dynamic-author</b>	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

<i>percent</i>	(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.
<b>regenerate</b>	(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 <i>percent</i> 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
<b>crypto ca authenticate</b>	Retrieves the CA certificate and authenticates it.
<b>crypto ca trustpoint</b>	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**

<b>Syntax Description</b>	<i>time-period</i>	(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.
---------------------------	--------------------	--

**Defaults** Automated CA rollover is not enabled.

**Command Modes** Certificate server configuration

Command History	Release	Modification
	12.4(2)T	This command was introduced.

**Usage Guidelines** 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)#
Router(cs-server)#
Router(cs-server)#

%Some server settings cannot be changed after CA certificate generation.
% Generating 1024 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#
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
<b>crypto pki server</b>	Enables a Cisco IOS certificate server and enters certificate configuration mode.
<b>show crypto pki server</b>	Displays current state and configuration of the certificate server.

# 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	
<b>management</b>	(Optional) Only the management plane will be secured.
<b>forwarding</b>	(Optional) Only the forwarding plane will be secured.
<b>no-interact</b>	(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.
<b>full</b>	(Optional) The user will be prompted for all interactive questions. This is the default.
<b>ntp</b>	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command line-interface (CLI).
<b>login</b>	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
<b>ssh</b>	(Optional) Specifies the configuration of the Secure Shell (SSH) feature in the AutoSecure CLI.
<b>firewall</b>	(Optional) Specifies the configuration of the firewall feature in the AutoSecure CLI.
<b>tcp-intercept</b>	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

## Defaults

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: <b>full</b> , <b>ntp</b> , <b>login</b> , <b>ssh</b> , <b>firewall</b> , and <b>tcp-intercept</b> .
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#
```

**Related Commands**

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

# 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

<i>type-of-system</i>	Free-format string (see <a href="#">Table 24</a> ).
<b>url</b> <i>url</i>	URL from which the Easy VPN device obtains the automatic update.
<b>rev</b> <i>review-version</i>	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.

[Table 24](#) lists possible free-format strings to be used for the type-of-system argument.

**Table 24** 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
Linux	Linux

**Table 24**      **Possible Free-format Strings**

Free-Format String	Operating System
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)
```

# backoff exponential

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

```
backoff exponential [ minutes ] [ retransmits ]
no backoff exponential [ minutes ] [ retransmits ]
```

## Syntax Description

<i>minutes</i>	(Optional) Number of retransmissions done in exponential max-delay mode. Valid range for the <i>minutes</i> argument is 1 through 120; if <i>minutes</i> is not specified, the default value (60 minutes) will be used.
<i>retransmits</i>	(Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. Valid range for the <i>retransmits</i> argument is 1 through 50; if <i>retransmits</i> is not specified, the default value (5 retransmits) will be used.

## Command Default

This command is not enabled.

## Command Modes

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

## 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.

## Usage Guidelines

Before enabling this command, you must configure the `server-group radius` command, which allows you to specify a server group and enter server-group RADIUS configuration mode.

The `backoff exponential` command allows you to configure an exponential backoff retransmission per RADIUS 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:

```
aaa group server radius cat
 backoff exponential max-delay 90 backoff-retry 10
```

## ■ backoff exponential

**Related Commands**

<b>Command</b>	<b>Description</b>
	Groups different RADIUS server hosts into distinct lists and distinct methods.
	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. To remove a backup gateway, use the `no backup-gateway` form of this command.

```
{ip-address | hostname}
```

```
{ip-address | hostname}
```

## Syntax Description

<i>ip-address</i>	IP address of the gateway.
<i>hostname</i>	Host name of the gateway.

## Defaults

A list of backup gateways is not configured.

## Command Modes

Global configuration (config)

## 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 `isakmp client configuration group` command.

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

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



### Note

- If you have to configure more than one backup gateway, you have to add a command line for each.
- You can configure a maximum of 10 backup gateways.

## 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 RMZPPMRQMSdiZNUg`EBbCWTkSTi\d[
```

## ■ backup-gateway

```
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
```

---

**Related Commands**

---

**Command**

---

**Description**

---

Specifies to which group a policy profile will be defined.

---

# banner

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

```
banner {banner-text}
```

```
{banner-text}
```

## Syntax Description

	Delimiting character that must precede and follow the banner text. The delimiting character may be a character of your choice, such as “c” or “@.”
<i>banner-text</i>	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
<code>group-policy</code>	Specifies to which group a policy profile will be defined.

## banner (WebVPN)

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

*string*

<b>Syntax Description</b>	<i>string</i>	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 displayed after a successful login.

**Command Modes** Webvpn group policy configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(6)T	

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

```
Router(config)#
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner "Login Successful"
Router(config-webvpn-group)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<code>group-policy</code>	Enters webvpn group policy configuration mode to configure a policy group.
	<code>context</code>	Enters webvpn context configuration mode to configure the SSL VPN context.

# 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 bidirectional` form of this command.

## Syntax Description

This command has no arguments or keywords.

## Defaults

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 `access-list` 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**

<b>Command</b>	<b>Description</b>
<b>interface (RITE)</b>	Specifies the outgoing interface for exporting traffic.
<b>ip traffic-export profile</b>	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
<b>outgoing</b>	Configures filtering for outgoing export traffic.

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*

<i>sourceURL</i>	Specifies the source URL on the registrar for the binary file using one of the keywords in <a href="#">Table 24</a> .
<i>destinationURL</i>	Specifies the destination URL on the petitioner for binary file using one of the keywords in <a href="#">Table 24</a> .

None

tti-registrar configuration (tti-registrar)

12.4(15)T	This command was introduced.
-----------	------------------------------

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 usbtokn0:

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 25** *Source and Destination URL Keywords*

<b>Keyword</b>	<b>Description</b>
<b>archive:</b>	Retrieves from the archive location.
<b>cns:</b>	Retrieves from the Cisco Networking Services (CNS) configuration engine.
<b>disk0:</b>	Retrieves from disk0.
<b>disk1:</b>	Retrieves from disk1.
<b>flash:</b>	Retrieves from flash memory.
<b>ftp:</b>	Retrieves from the FTP network server.
<b>http:</b>	Retrieves from a HTTP server.
<b>https:</b>	Retrieves from a Secure HTTP (HTTPS) server.
<b>null:</b>	Retrieves from the file system.
<b>nvrn:</b>	Retrieves from the NVRAM of the router.

**Table 25** *Source and Destination URL Keywords*

<b>Keyword</b>	<b>Description</b>
<b>rcp:</b>	Retrieves from a remote copy (rcp) protocol network server.
<b>scp:</b>	Retrieves from a network server that supports Secure Shell (SSH).
<b>system:</b>	Retrieves from system memory, which includes the running configuration.
<b>tar:</b>	Retrieves from a compressed file in tar format.
<b>tftp:</b>	Retrieves from a TFTP network server.
<b>tmpsys:</b>	Retrieves from a temporary system location.
<b>unix:</b>	Retrieves from the UNIX system location.
<b>usbtoken:</b>	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**

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

# 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

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

## Defaults

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) #
```

## Related Commands

Command	Description
<b>clear radius local-server</b>	Clears the statistics display or unblocks a user.
<b>debug radius local-server</b>	Displays the debug information for the local server.
<b>group</b>	Enters user group configuration mode and configures shared setting for a user group.
<b>nas</b>	Adds an access point or router to the list of devices that use the local authentication server.

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

<i>browser-proxy-map-name</i>	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
<b>crypto isakmp client configuration group</b>	Specifies to which group a policy profile will be defined.