

eap



Note

This command is removed effective with Cisco IOS Release 12.4(6)T.

To specify Extensible Authentication Protocol- (EAP-) specific parameters, use the **eap** command in identity profile configuration mode. To disable the parameters that were set, use the **no** form of this command.

```
eap {username name | password password}
```

```
no eap {username name | password password}
```

Syntax Description

username <i>name</i>	Username that will be sent to Request-Id packets.
password <i>password</i>	Password that should be used when replying to an Message Digest 5 (MD5) challenge.

Defaults

EAP parameters are not set.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(6)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if your router is configured as a supplicant. This command provides the means for configuring the identity and the EAP MD5 password that will be used by 802.1X to authenticate.

Examples

The following example shows that the EAP username “user1” has been configured:

```
Router (config)# identity profile dot1x
Router (config-identity-prof)# eap username user1
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the **enable** command in either user EXEC, privileged EXEC, or diagnostic mode.

```
enable [privilege-level] [view [view-name]]
```

Syntax Description	
<i>privilege-level</i>	(Optional) Privilege level at which to log in.
view	(Optional) Enters into root view, which enables users to configure CLI views. Note This keyword is required if you want to configure a CLI view.
<i>view-name</i>	(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.

Defaults Privilege-level 15 (privileged EXEC)

Command Modes User EXEC (>)
Privileged EXEC (#)
Diagnostic Mode (diag)

Command History	Release	Modification
	10.0	This command was introduced.
	12.3(7)T	The view keyword and <i>view-name</i> argument were added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SRB	The view keyword and <i>view-name</i> argument were integrated into Cisco IOS Release 12.2(33)SRB.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(22)SB.
	Cisco IOS XE Release 2.1	This command became available on the ASR 1000 Series Routers, and became available in diagnostic mode for the first time.

Usage Guidelines By default, using the **enable** command without the *privilege-level* argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the **enable view** command (without the *view-name* argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The *view-name* argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the **enable** command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first

Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip         IP information
  parser     Display parser information
  version    System hardware and software status
```

```
Router# show ip ?

access-lists      List IP access lists
accounting        The active IP accounting database
aliases           IP alias table
arp               IP ARP table
as-path-access-list List AS path access lists
bgp               BGP information
cache             IP fast-switching route cache
casa              display casa information
cef               Cisco Express Forwarding
community-list    List community-list
dfp               DFP information
dhcp              Show items in the DHCP database
drp               Director response protocol
dvmrp             DVMRP information
eigrp             IP-EIGRP show commands
extcommunity-list List extended-community list
flow              NetFlow switching
helper-address     helper-address table
http              HTTP information
igmp              IGMP information
irdp              ICMP Router Discovery Protocol
.
.
```

The following example shows how to use the **enable view** command to switch from the root view to the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view

Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all

Views Present in System:
View Name:  first
View Name:  second
! Switch to the CLI view "first."
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view "first."
Router# show parser view

Current view is 'first'
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement, use the **no** form of this command.

```
enable password [level level] {password | [encryption-type] encrypted-password}
```

```
no enable password [level level]
```

Syntax Description

<i>level level</i>	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
<i>password</i>	Password users type to enter enable mode.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default is level 15.

Command Modes

Global configuration

Command History

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

Usage Guidelines



Caution

If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.

**Caution**

If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-v**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter *abc?123* at the password prompt.

Examples

The following example enables the password “pswd2” for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password “\$1\$i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the enable password command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

```
enable secret [level level] {password | [encryption-type] encrypted-password}
```

```
no enable secret [level level]
```

Syntax Description

level <i>level</i>	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or in the no form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the no form of the command.
<i>password</i>	Password for users to enter enable mode. This password should be different from the password created with the enable password command.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available for this command is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default level is 15.

Command Modes

Global configuration

Command History

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

Usage Guidelines



Caution

If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a non-reversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you paste into this command an encrypted password that you copied from a router configuration file.

**Caution**

If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

**Note**

After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If **service password-encryption** is set, the encrypted form of the password you create here is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
- Must not have a number as the first character
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-v**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter **abc?123** at the password prompt.

Examples

The following example specifies the enable secret password of “greentree”:

```
enable secret greentree
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: greentree
```

The following example enables the encrypted password “\$1\$FaD0\$Xyti5Rkls3LoyxzS8”, which has been copied from a router configuration file, for privilege level 2 using encryption type 5:

```
enable password level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable password	Sets a local password to control access to various privilege levels.

enabled (IPS)

To change the enabled status of a given signature or signature category, use the **enabled** command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

enabled {true | false}

no enabled

Syntax Description

true	Enables a specified signature or all signatures within a specified category.
false	Disables a specified signature or all signatures within a specified category.

Command Default

All commands are enabled.

Command Modes

Signature-definition-status configuration (config-sigdef-status)
IPS-category-action configuration (config-ips-category-action)

Command History

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

Usage Guidelines

Use the **enabled** command to change the status of a signature or signature category to active (true) or inactive (false).

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sig)# signature 9000 0
Router(config-sig-sig)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Changes the enabled or retired status of a given signature or signature category.

encryption (IKE policy)

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

```
encryption { des | 3des | aes | aes 192 | aes 256 }
```

```
no encryption
```

Syntax Description	des	56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
	3des	168-bit DES (3DES) as the encryption algorithm.
	aes	128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
	aes 192	192-bit AES as the encryption algorithm.
	aes 256	256-bit AES as the encryption algorithm.

Command History The 56-bit DES-CBC encryption algorithm

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.0(2)T	The 3des option was added.
	12.2(13)T	The following keywords were added: aes , aes 192 , and aes 256 .
	12.4(4)T	IPv6 support was added.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
 encryption 3des
 exit
```

The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured
        encryption method for ISAKMP policy 1
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

engine (IPS)

To enter signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature, use the **engine** command in signature-definition-action configuration mode.

engine

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Signature-definition-action configuration (config-sigdef-action)

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

Usage Guidelines If you wish to change router actions for a specific signature, you must issue the engine command to enter the appropriate configuration mode, which allows you to issue the **event-action** command and specify any supported action.

Examples The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)# ^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands	Command	Description
	event-action	Changes router actions for a signature or signature category.
	signature	Specifies a signature for which the CLI user tunings will be changed.

enrollment

To specify the enrollment parameters of your certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [**mode**] [**retry** *minutes*] [**retry** *number*] **url** *url*

no enrollment [**mode**] [**retry** *minutes*] [**retry** *number*] **url** *url*

Syntax Description

mode	(Optional) Specifies registration authority (RA) mode if your CA system provides a RA.
retry <i>minutes</i>	(Optional) Specifies the wait period between certificate request retries. The default is 1 minute between retries.
retry <i>number</i>	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.)
url <i>url</i>	Specifies the URL of the CA where your router should send certificate requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, <i>url</i> must be in the form http://CA_name, where CA_name is the CA's host Domain Name System (DNS) name or IP address. If you are using TFTP for enrollment, <i>url</i> must be in the form tftp://certserver/file_specification. (The file_specification is optional. See the "Usage Guidelines" for additional information.)

Defaults

RA mode is turned off until you enable the **mode** keyword.
The router will send the CA another certificate request every 1 minute unless otherwise specified.
There is no limit to the number of retries unless you specify a number via **retry** *number*.
Your router does not know the CA URL until you specify it via **url** *url*.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(13)T	The url <i>url</i> option was enhanced to support TFTP enrollment.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry minutes** option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries is exceeded. By default, the router will keep sending requests forever, unless you can change this parameter to a finite number using the **retry number** option.

Use the **url url** option to specify or change the URL of the CA. You can specify enrollment via SCEP (an HTTP URL) or TFTP (a TFTP URL).

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the `file_specification` is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url url** option does not include a file specification, the router’s FQDN will be used.)

**Note**

The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all `ca-identity` and `trusted-root` configuration mode commands). If you enter a `ca-identity` or `trusted-root` subcommand, the configuration mode and command will be written back as `ca-trustpoint`.

Examples

The following example shows how to declare a CA named “ka” and specify the URL of the CA as “http://example:80”:

```
crypto ca trustpoint ka
enrollment url http://example:80
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the CA’s certificate).
crypto ca trustpoint	Declares the CA that your router should use.

enrollment command

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

enrollment command

Syntax Description This command has no arguments or keywords.

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 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 the enrollment profile name “E” for certificate enrollment:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

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

Related Commands	Command	Description
	crypto ca profile enrollment	Defines an enrollment profile.
	parameter	Specifies parameters for an enrollment profile.

enrollment credential

To specify an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server, use the **enrollment credential** command in ca-profile-enroll configuration mode.

enrollment credential *label*

Syntax Description	<i>label</i>	Name of the certification authority (CA) trustpoint of another vendor.
---------------------------	--------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Ca-profile-enroll configuration
----------------------	---------------------------------

Command History	Release	Modification
	12.3(11)T	This command was introduced.
	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.(33)SRA.

Usage Guidelines	To configure a router that is already enrolled with a CA of another vendor that is to be enrolled with a Cisco IOS certificate server, you must configure a certificate enrollment profile (via the crypto pki profile enrollment command). Thereafter, you should issue the enrollment credential command, which specifies the trustpoint of another vendor that has to be enrolled with a Cisco IOS certificate server.
-------------------------	---

Examples	The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:
-----------------	---

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  ip-address FastEthernet2/0
  revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
  enrollment profile cs1
  revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
! enrollment credential command) that "msca-root" is being initially enrolled with the
! Cisco IOS CA.
crypto pki profile enrollment cs1
  enrollment url http://cs:80
  enrollment credential msca-root!
```

```

! Configure the certificate server, and issue and the grant auto trustpoint command to
! instruct the certificate server to accept enrollment request only from clients who are
! already enrolled with trustpoint "msca-root."
crypto pki server cs
  database level minimum
  database url nvram:
  issuer-name CN=cs
  grant auto trustpoint msca-root
!
crypto pki trustpoint cs
  revocation-check crl
rsa-keypair cs
!
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  revocation-check crl

```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name port-num*

Syntax Description

<i>host-name</i>	Defines the proxy server used to get the CA.
<i>port-num</i>	Specifies the port number used to access the CA.

Defaults

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
enrollment url http://kahului
enrollment http-proxy bomborra 8080
crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment mode ra

The **enrollment mode ra** command is replaced by the **enrollment command** command. See the **enrollment command** command for more information.

enrollment profile

To specify that an enrollment profile can be used for certificate authentication and enrollment, use the **enrollment profile** command in ca-trustpoint configuration mode. To delete an enrollment profile from your configuration, use the **no** form of this command.

enrollment profile *label*

no enrollment profile *label*

Syntax Description

<i>label</i>	Creates a name for the enrollment profile.
--------------	--

Defaults

Your router does not recognize any enrollment profiles until you declare one using this command.

Command Modes

Ca-trustpoint 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

Before you can enable this command, you must enter the **crypto ca trustpoint** command.

The **enrollment profile** command enables your router to accept an enrollment profile, which can be configured via the **crypto ca profile enrollment** command. The enrollment profile, which consists of two templates, can be used to specify different URLs or methods for certificate authentication and enrollment.

Examples

The following example shows how to declare the enrollment profile named "E":

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

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

Related Commands	Command	Description
	crypto ca profile enrollment	Defines an enrollment profile.
	crypto ca trustpoint	Declares the CA that your router should use.

enrollment retry count

The **enrollment retry count** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry period

The **enrollment retry period** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment selfsigned

To specify self-signed enrollment for a trustpoint, use the **enrollment selfsigned** command in ca-trustpoint configuration mode. To delete self-signed enrollment from a trustpoint, use the **no** form of this command.

enrollment selfsigned

no enrollment selfsigned

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior or values.

Command Modes

ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you can use the **enrollment selfsigned** command, you must enable the **crypto pki trustpoint** command, which defines the trustpoint and enters ca-trustpoint configuration mode.

If you do not use this command, you should specify another enrollment method for the router by using an enrollment command such as **enrollment url** or **enrollment terminal**.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local:

```
crypto pki trustpoint local
 enrollment selfsigned
```

Related Commands

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

enrollment terminal (ca-profile-enroll)

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

enrollment terminal

no enrollment terminal

Syntax Description This command has no arguments or keywords.

Defaults A certificate enrollment request is not specified.

Command Modes Ca-profile-enroll configuration

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

Usage Guidelines A user may manually cut-and-paste certificate authentication requests and certificates when a network connection between the router and certification authority (CA) is unavailable. After this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.



Note

Although most routers accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

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

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

Related Commands	Command	Description
	crypto ca profile enrollment	Defines an enrollment profile.

enrollment terminal (ca-trustpoint)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal [pem]

no enrollment terminal [pem]

Syntax Description

pem (Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

No default behavior or values

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(4)T	The pem keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

A user may want to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal.

The pem Keyword

Use the **pem** keyword to issue certificate requests (via the **crypto ca enroll** command) or receive issued certificates (via the **crypto ca import certificate** command) in PEM-formatted files through the console terminal. If the CA server does not support simple certificate enrollment protocol (SCEP), the certificate request can be presented to the CA server manually.



Note

When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the **crypto ca authenticate** command.

Examples

The following example shows how to manually specify certificate enrollment via cut-and-paste. In this example, the CA trustpoint is “MS.”

```
crypto ca trustpoint MS
  enrollment terminal
  crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca enroll	Obtains the certificates of your router from the certification authority.
crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment url (ca-identity)

The **enrollment url (ca-identity)** command is replaced by the **enrollment url (ca-trustpoint)** command. See the **enrollment url (ca-trustpoint)** command for more information.

enrollment url (ca-profile-enroll)

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

enrollment url *url*

no enrollment url *url*

Syntax Description

<i>url</i>	URL of the CA server to which your router should send certificate requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the <i>url</i> 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 <i>url</i> 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.)
------------	--

Defaults

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name “E”:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial

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

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

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment url (ca-trustpoint)

To specify the enrollment parameters of a certification authority (CA), use the **enrollment url** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

no enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

Syntax Description

mode	(Optional) Specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
retry period <i>minutes</i>	(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 to 60 minutes.)
retry count <i>number</i>	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 to 100 retries.)
url <i>url</i>	Specifies the URL of the file system where your router should send certificate requests. For enrollment method options, see Table 41 .
pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

Your router does not know the CA URL until you specify it using the **url** *url* keyword and argument.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3T	This command was introduced as the enrollment url (ca-identity) command.
12.2(8)T	This command replaced the enrollment url (ca-identity) command. The mode , retry period <i>minutes</i> , and retry count <i>number</i> keywords and arguments were added.
12.2(13)T	The url <i>url</i> option was enhanced to support TFTP enrollment.
12.3(4)T	The pem keyword was added, and the url <i>url</i> option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified period of time (the retry period), the router will send another certificate request. By default, the router will send a maximum of ten requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified via the **retry count** *number* option) is exceeded.

Use the **pem** keyword to issue certificate requests (using the **crypto pki enroll** command) or receive issued certificates (using the **crypto pki import certificate** command) in PEM-formatted files.

**Note**

When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained using the **crypto ca authenticate** command.

Use the **url** *url* option to specify or change the URL of the CA. [Table 41](#) lists the available enrollment methods.

Table 41 Certificate Enrollment Methods

Enrollment Method	Description
bootflash	Enroll via bootflash: file system
cns	Enroll via Cisco Networking Services (CNS): file system
flash	Enroll via flash: file system
ftp	Enroll via FTP: file system
null	Enroll via null: file system
nvrाम	Enroll via NVRAM: file system
rcp	Enroll via remote copy protocol (rcp): file system
scp	Enroll via secure copy protocol (scp): file system
SCEP ¹	Enroll via Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL)
system	Enroll via system: file system
TFTP ²	Enroll via TFTP: file system

1. If you are using SCEP for enrollment, the URL 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.
2. If you are using TFTP for enrollment, the URL must be in the form `tftp://certserver/file_specification`. (The `file_specification` is optional. See the section “TFTP Certificate Enrollment” for additional information.)

TFTP Certificate Enrollment

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the `file_specification` is included in the URL, the router will append an extension onto the file specification. When the **crypto pki authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the FQDN of the router will be used.)

**Note**

The **crypto pki trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all **ca-identity** and **trusted-root** configuration mode commands). If you enter a **ca-identity** or **trusted-root** command, the configuration mode and command will be written back as **pki-trustpoint**.

Examples

The following example shows how to declare a CA named “trustpoint” and specify the URL of the CA as “http://example:80”:

```
crypto pki trustpoint trustpoint
  enrollment url http://example:80
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.

eou allow

To allow additional Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) options, use the **eou allow** command in global configuration mode. To disable the options that have been set, use the **no** form of this command.

```
eou allow { clientless | ip-station-id }
```

```
no eou allow { clientless | ip-station-id }
```

Syntax Description

clientless	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
ip-station-id	Allows an IP address in the station-id field.

Defaults

No additional EAPoUDP options are allowed.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **eou allow** command used with the **clientless** keyword requires that a user group be configured on the Cisco Access Control Server (ACS) using the same username and password that are specified using the **eou clientless** command.

Examples

The following example shows that clientless hosts are allowed:

```
Router (config)# eou allow clientless
```

Related Commands

Command	Description
eou clientless	Sets user group credentials for clientless hosts.

eou clientless

To set user group credentials for clientless hosts, use the **eou clientless** command in global configuration mode. To remove the user group credentials, use the **no** form of this command.

```
eou clientless {password password | username username}
```

```
no eou clientless {password | username}
```

Syntax Description

password <i>password</i>	Sets a password.
username <i>username</i>	Sets a username.

Defaults

Username and password values are clientless.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For this command to be effective, the **eou allow** command must also be enabled.

Examples

The following example shows that a clientless host with the username “user1” has been configured:

```
Router (config)# eou clientless username user1
```

The following example shows that a clientless host with the password “user123” has been configured:

```
Router (config)# eou clientless password user123
```

Related Commands

Command	Description
eou allow	Allows additional EAPoUDP options.

eou default

To set global Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) parameters to the default values, use the **eou default** command in global or interface configuration mode.

eou default

Syntax Description This command has no arguments or keywords.

Defaults The EAPoUDP parameters are set to their default values.

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

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 You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Using this command, you can reset existing values to their default values.

Examples The following configuration example shows that EAPoUDP parameters have been set to their default values:

```
Router (config)# eou default
```

eou initialize

To manually initialize Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) state machines, use the **eou initialize** command in global configuration mode. This command has no **no** form.

```
eou initialize { all | authentication { clientless | eap | static } | interface interface-name | ip
ip-address | mac mac-address | posturetoken string }
```

Syntax Description		
all		Initiates reauthentication of all EAPoUDP clients. This keyword is the default.
authentication		Specifies the authentication type.
clientless		Clientless authentication type.
eap		EAP authentication type.
static		Static authentication type.
interface		Specifies a specific interface.
<i>interface-name</i>		
ip	<i>ip-address</i>	Specifies a specific IP address.
mac	<i>mac-address</i>	Specifies a specific MAC address.
posturetoken	<i>string</i>	Specifies a specific posture token.

Command Default None

Command Modes Global configuration (config)

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

Usage Guidelines If this command is used, existing EAPoUDP state machines will be reset.

Examples The following example shows that all EAPoUDP state machines have been reauthenticated:

```
Router (config)# eou initialize all
```

Related Commands	Command	Description
	eou revalidate	Revalidates an EAPoUDP association.

eou logging

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) system logging events, use the **eou logging** command in global configuration mode. To remove EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description This command has no arguments or keywords.

Defaults Logging is disabled.

Command Modes Global configuration (config)

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

Examples The following example shows that EAPoUDP logging has been enabled:

```
Router (config)# eou logging
```

The following is sample EAPoUDP logging output:

```
Apr 9 10:04:09.824: %EOU-6-SESSION: IP=10.0.0.1| HOST=DETECTED| Interface=FastEthernet0/0
*Apr 9 10:04:09.900: %EOU-6-CTA: IP=10.0.0.1| CiscoTrustAgent=DETECTED
*Apr 9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| TOKEN=Healthy
*Apr 9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| ACLNAME=#ACSACL#-IP-HealthyACL-40921e54
*Apr 9 10:06:19.576: %EOU-6-POSTURE: IP=10.0.0.1| HOST=AUTHORIZED|
Interface=FastEthernet0/0.420
*Apr 9 10:06:19.580: %EOU-6-AUTHTYPE: IP=10.0.0.1| AuthType=EAP
*Apr 9 10:06:04.424: %EOU-6-SESSION: IP=192.168.2.1| HOST=REMOVED|
Interface=FastEthernet0/0.420
```

eou max-retry

To set the number of maximum retry attempts for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou max-retry** command in global or interface configuration mode. To remove the number of retries that were entered, use the **no** form of this command.

eou max-retry *number-of-retries*

no eou max-retry *number-of-retries*

Syntax Description

<i>number-of-retries</i>	Number of maximum retries that may be attempted. The value ranges from 1 through 10. The default is 3.
--------------------------	--

Defaults

The default number of retries is 3.

Command Modes

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

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4	The value range was changed from 1 through 3 to 1 through 10.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the maximum number of retries for an EAPoUDP session has been set for 2:

```
Router (config)# eou max-retry 2
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values or EAPoUDP session cache entries.

eou port

To set the UDP port for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou port** command in global configuration mode. This command has no **no** form.

eou port *port-number*

Syntax Description

<i>port-number</i>	Number of the port. The value ranges from 1 through 65535. The default value is 27186.
--------------------	--

Defaults

The default *port-number* value is 27186.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Ensure that the port you set does not conflict with other UDP applications.

Examples

The following example shows that the port for an EAPoUDP session has been set to 200:

```
Router (config)# eou port 200
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP.

eou rate-limit

To set the number of simultaneous posture validations for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou rate-limit** command in global configuration mode. This command has no **no** form.

eou rate-limit *number-of-validations*

Syntax Description

<i>number-of-validations</i>	Number of clients that can be simultaneously validated. The value ranges from 1 through 200. The default value is 20.
------------------------------	---

Defaults

No default behaviors or values

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you set the rate limit to 0 (zero), rate limiting will be turned off.

If the rate limit is set to 100 and there are 101 clients, validation will not occur until one drops off.

To return to the default value, use the **eou default** command.

Examples

The following example shows that the number of posture validations has been set to 100:

```
Router (config)# eou rate-limit 100
```

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
show eou	Displays information about EAPoUDP.

eou revalidate

To revalidate an Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) association, use the **eou revalidate** command in privileged EXEC mode. To disable the revalidation, use the **no** form of this command.

```
eou revalidate {all | authentication {clientless | eap | static} | interface interface-name | ip
ip-address | mac mac-address | posturetoken string}
```

```
no eou revalidate {all | authentication {clientless | eap | static} | interface interface-name | ip
ip-address | mac mac-address | posturetoken string}
```

Syntax Description

all	Enables revalidation of all EAPoUDP clients. This keyword option is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface <i>interface-name</i>	Name of the interface. (See Table 42 for the types of interface that may be shown.)
ip <i>ip-address</i>	IP address of the client.
mac <i>mac-address</i>	The 48-bit hardware address of the client.
posturetoken <i>string</i>	Name of the posture token.

Command Default

None

Command Modes

Privileged EXEC (#)

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

If you use this command, existing EAPoUDP sessions will be revalidated.

[Table 42](#) lists the interface types that may be used with the **interface** keyword.

Table 42 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface

Table 42 Description of Interface Types (continued)

Interface Type	Description
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all EAPoUDP clients are to be revalidated:

```
Router# eou revalidate all
```

Related Commands

Command	Description
eou initialize	Manually initializes EAPoUDP state machines.

eou timeout

To set the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) timeout values, use the **eou timeout** command in global or interface configuration mode. To remove the value that was set, use the **no** form of this command.

```
eou timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status query seconds}
```

```
no timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status query seconds}
```

Syntax Description

aaa seconds	Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.
hold-period seconds	Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.
retransmit seconds	Retransmit period, in seconds. The value range is from 1 through 60. Default=3.
revalidation seconds	Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.
status query seconds	Status query period after revalidation, in seconds. The value range is from 30 through 1800. Default=300.

Defaults

No default behavior or values

Command Modes

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

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

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the status query period after revalidation is set to 30:

```
Router (config)# eou timeout status query 30
```

Related Commands

Command	Description
<code>show eou</code>	Displays information about EAPoUDP global values.

error-msg

To display a specific error message when a user logs on to a Secure Sockets Layer Virtual Private Network (SSL VPN) gateway, use the **error-msg** command in webvpn acl configuration mode. To remove the error message, use the **no** form of this command.

error-msg *message-string*

no error-msg *message-string*

Syntax Description

message-string Error message to be displayed.

Command Default

No special error message is displayed.

Command Modes

Webvpn acl configuration

Command History

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

Usage Guidelines

If the **error-url** command is configured, the user is redirected to the error URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated information page showing the message that was configured using the **error-msg** command.

Examples

This example shows that the following error message will be displayed when the user logs on to the SSL VPN gateway:

```
webvpn context context1
acl acl1
error-msg "If you have any questions, please contact <a
href+mailto:employee1@example.com>Employee1</a>."
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level and enters webvpn acl configuration mode.
error-url	Defines a URL as an ACL violation page using a SSL VPN gateway.
webvpn context	Configures a SSL VPN context and enters webvpn context configuration mode.

error-url

To define a URL as an access control list (ACL) violation page using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the **error-url** command in webvpn acl configuration mode. To remove the ACL violation page, use the **no** form of this command.

error-url *access-deney-page-url*

no error-url *access-deney-page-url*

Syntax Description

access-deney-page-url URL to which a user is directed for an ACL violation.

Command Default

If this command is not configured, the gateway redirects the ACL violation page to a predefined URL.

Command Modes

Webvpn acl configuration

Command History

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

Usage Guidelines

If the **error-url** command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated error page.

Examples

The following example shows that the URL “http://www.example.com” has been defined as the ACL violation page:

```
webvpn context context1
acl acl1
error-url "http://www.example.com"
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.
error-msg	Displays a specific error message when a user logs on to a SSL VPN gateway.
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

evaluate

To nest a reflexive access list within an access list, use the **evaluate** command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the **no** form of this command.

evaluate *name*

no evaluate *name*

Syntax Description

name The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the **permit** (reflexive) command.

Defaults

Reflexive access lists are not evaluated.

Command Modes

Access-list configuration

Command History

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

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the **permit** (reflexive) command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry “points” to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

Examples

The following example shows reflexive filtering at an external interface. This example defines an extended named IP access list *inboundfilters*, and applies it to inbound traffic at the interface. The access list definition permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic, denies all Internet Control Message Protocol traffic, and causes all Transmission Control Protocol traffic to be evaluated against the reflexive access list *tcptraffic*.

If the reflexive access list *tcptraffic* has an entry that matches an inbound packet, the packet will be permitted into the network. *tcptraffic* only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
  description Access to the Internet via this interface
  ip access-group inboundfilters in
!
ip access-list extended inboundfilters
  permit 190 any any
  permit eigrp any any
  deny icmp any any
  evaluate tcptraffic
```

Related Commands

Command	Description
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

event-action

To change router actions for a signature or signature category, use the **event-action** command in signature-definition-action-engine or IPS-category-action configuration mode. To revert to the default router action values, use the **no** form of this command.

event-action *action*

no event-action

Syntax Description

action

Router actions for a specified signature or signature category. The *action* argument can be any of the following options:

- **deny-attacker-inline**
- **deny-connection-inline**
- **deny-packet-inline**
- **produce-alert**
- **reset-tcp-connection**

Note Event actions for an individual signature must be entered on a single line. However, event actions associated with a category can be entered separately or on a single line.

Command Default

Default values for the signature or signature category will be used.

Command Modes

Signature-definition-action-engine configuration (config-sigdef-action-engine)
IPS-category-action configuration (config-ips-category-action)

Command History

Release

Modification

12.4(11)T

This command was introduced.

Usage Guidelines

Signature-Based Changes

After signature-based changes are complete, Cisco IOS Intrusion Prevention System (IPS) prompts the user to confirm whether or not the changes are acceptable. Confirming the changes instructs Cisco IOS IPS to compile the changes for the signature and modify memory structures to reflect the change. Also, Cisco IOS IPS will save the changes to the location specified via the **ip ips config location** command (for example, flash:ips5/*.xml).

You can issue the **show ip ips signatures** command to verify the event-action configuration. (The **show running-config** command does not show individual signature tuning information.)

Signature Category-Based Changes

After signature category-based changes are complete, the category tuning information is saved in the command-line interface (CLI) configuration.

Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)# ^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

The following example shows how to tune event-action parameters for the signature category “adware/spyware.” All the tuning information will be applied to all signatures that belong to the adware/spyware signature category.

```
Router(config)# ip ips signature category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes:[confirm]y
```

Related Commands

Command	Description
engine	Enters the signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.
ip ips config location	Specifies the location in which the router will save signature information.
signature	Specifies a signature for which the CLI user tunings will be changed.
show ip ips	Displays IPS information such as configured sessions and signatures.

exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server, use the **exclusive-domain** command in URL parameter-map configuration mode. To disable this capability, use the **no** form of this command.

exclusive-domain {deny | permit} *domain-name*

no exclusive-domain {deny | permit} *domain-name*

Syntax Description

deny	Removes the specified domain name from the exclusive domain list. Blocks all traffic destined for the specified domain name.
permit	Adds the specified domain name to the exclusive domain list. Permits all traffic destined for the specified domain name.
<i>domain-name</i>	Domain name that is added or removed from the exclusive domain name list; for example, www.example.com.

Command Default

Disabled.

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 **exclusive-domain** subcommand after you enter the **parameter-map type urlfilter** command. For detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

The **exclusive-domain** command allows you to specify a list of domain names (exclusive domains) so that the Cisco IOS firewall does not create a lookup request for the traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending lookup requests to the web server for traffic that is destined for a host that is completely allowed to all users. You can enter the complete domain name or a partial domain name.

Complete Domain Name

If you add a complete domain name, such as www.example.com, to the exclusive domain list, all traffic whose URLs are destined for this domain (such as www.example.com/news and www.example.com/index) is excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Partial Domain Name

If you add only a partial domain name to the exclusive domain list, such as example.com, all URLs whose domain names end with this partial domain name (such as www.example.com/products and www.example.com/eng) are excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Examples

The following example adds cisco.com to the exclusive domain list:

```
parameter-map type urlfilter ul
exclusive-domain permit example.com
```

Related Commands

Command	Description
ip urlfilter exclusive-domain	Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.