

## database (certificate server)

To require a username or password to be issued when accessing a database storage location, use the **database** command in certificate server configuration mode. To return to the default value, use the **no** form of this command.

```
database username username [password password]
```

```
no database username username [password password]
```

### Syntax Description

<b>username</b> <i>username</i>	When prompted, a username will be used to access a storage location.
<b>password</b> <i>password</i>	(Optional) When prompted, a password will be used to access a storage location.

### Defaults

This command is not enabled.

### Command Modes

Certificate server configuration

### Command History

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

### Usage Guidelines

All information stored in the remote database is public: there are no private keys stored in the database location. Using a password helps to protect against a potential attacker who can change the contents of the .ser or .crl file. If the contents of the files are changed, the certificate server may shut down, refusing to either issue new certificates or respond to simple certificate enrollment protocol (SCEP) requests until the files are restored.

It is good security practice to protect all information exchanges with the database server using IP Security (IPSec). To protect your information, use a remote database to obtain the appropriate certificates and setup the necessary IPSec connections to protect all future access to the database server.

### Examples

The following example shows how to specify the username “mystorage” when accessing the complete database that is stored on an external TFTP server:

```
Router (config)# ip http server
Router (config)# crypto pki server myserver
Router (cs-server)# database level complete
Router (cs-server)# database url tftp://mytftp
Router (cs-server)# database username mystorage
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>crypto pki server</b>	Enables a Cisco IOS certificate server and enters PKI configuration mode.
	<b>database level</b>	Controls what type of data is stored in the database.
	<b>database url</b>	Specifies the location where all database entries for the certificate server will be written out.

# database archive

To set the certification authority (CA) certificate and CA key archive format—and the password—to encrypt this CA certificate and CA key archive file, use the **database archive** command in certificate server configuration mode. To disable the autoarchive feature, use the **no** form of this command.

```
database archive {pkcs12 | pem} [password password]
```

```
no database archive {pkcs12 | pem} [password password]
```

## Syntax Description

<b>pkcs12</b>	Export as a PKCS12 file. The default is PKCS12.
<b>pem</b>	Export as a privacy-enhanced mail (PEM) file.
<b>password password</b>	(Optional) Password to encrypt the CA certificate and CA key. The password must be at least eight characters. If a password is not specified, you will be prompted for the password after the <b>no shutdown</b> command has been issued for the first time. When the password is entered, it will be encrypted.

## Defaults

The archive format is PKCS (that is, the CA certificate and CA key are exported into a PKCS12 file, and you will be prompted for the password when the certificate server is turned on the first time).

## Command Modes

Certificate server configuration

## Command History

Release	Modification
12.3(11)T	This command was introduced.

## Usage Guidelines

Use this command to configure the autoarchive format for the CA certificate and CA key. The archive can later be used to restore your certificate server.

If autoarchiving is not explicitly turned off when the certificate server is first enabled (using the **no shutdown** command), the CA certificate and CA key will be archived automatically, applying the following rule:

- The CA key must be (1) manually generated and marked “exportable” or (2) automatically generated by the certificate server (it will be marked nonexportable).



### Note

It is strongly recommended that if the password is included in the configuration to suppress the prompt after the **no shutdown** command, the password should be removed from the configuration after the archiving is finished.

## Examples

The following example shows that certificate server autoarchiving has been enabled. The CA certificate and CA key format has been set to PEM, and the password has been set as cisco123.

```
Router (config)# crypto pki server myserver  
Router (cs-server)# database archive pem password cisco123
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>crypto pki server</b>	Enables a Cisco IOS certificate server.

---

# database level

To control what type of data is stored in the certificate enrollment database, use the **database level** command in certificate server configuration mode. To return to the default functionality, use the **no** form of this command.

**database level** { **minimal** | **names** | **complete** }

**no database level** { **minimal** | **names** | **complete** }

## Syntax Description

<b>minimal</b>	Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality.
<b>names</b>	The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke and particular certificate, if necessary.
<b>complete</b>	Each issued certificate is written to the database. If this keyword is used, you should enable the <b>database url</b> command; see “Usage Guidelines” for more information.

## Defaults

**minimal**

## Command Modes

Certificate server configuration

## Command History

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

## Usage Guidelines

The **database level** command is used to describe the database of certificates and certification authority (CA) states. After the user downgrades the database level, the old data stays the same and the new data is logged at the new level.

### minimum Level

The *ca-label.ser* file is always available. It contains the previously issued certificate’s serial number, which is always 1. If the .ser file is unavailable and the CA server has a self-signed certificate in the local configuration, the CA server will refuse to issue new certificates.

The file format is as follows:

```
last_serial = serial-number
```

### names Level

The *serial-number.cnm* file, which is written for each issued certificate, contains the “human readable decoded subject name” of the issued certificate and the “der encoded” values. This file can also include a certificate expiration date and the current status. (The **minimum** level files are also written out.)

The file format is as follows:

```

subjectname_der = <base64 encoded der value>
subjectname_str = <human readable decode subjectname>
expiration = <expiration date>
status = valid | revoked

```

### complete Level

The *serial-number.cer* file, which is written for each issued certificate, is the binary certificate without additional encoding. (The **minimum** and **names** level files are also written out.)

The **complete** level produces a large amount of information, so you may want to store all database entries on an external TFTP server via the **database url** command unless your router does one of the following:

- Issues only a small number of certificates
- Has a local file system that is designed to support a large number of write operations and has sufficient storage for the certificates that are being issued

### Examples

The following example shows how configure a minimum database to be stored on the local system:

```

Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server) database url nvram:
Router#(cs-server) issuer-name CN=ipsec_cs,L=Santa Cruz,C=US

```

### Related Commands

Command	Description
<b>crypto pki server</b>	Enables a Cisco IOS certificate server and enters PKI configuration mode.
<b>database url</b>	Specifies the location where all database entries for the certificate server will be written out.

# database url

To specify the location where all database entries for the certificate server will be written out, use the **database url** command in certificate server configuration mode. To return to the default location, use the **no** form of this command.

**database url** *root-url*

**no database url** *root-url*

## Syntax Description

*root-url* Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system (IFS).

## Defaults

The default location is flash.

## Command Modes

Certificate server configuration

## Command History

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

## Usage Guidelines

After you create a certificate server via the **crypto pki server** command, use the **database url** command if you want to specify a combined list of all the certificates that have been issued and the current command revocation list (CRL). The CRL is written to the certificate enrollment database as *ca-label.crl* (where *ca-label* is the name of the certificate server).



### Note

Although issuing the **database url** command is not required, it is recommended. Unless your router has a local file system that is designed for a large number of write operations and has sufficient storage for the certificates that are issued, you should issue this command.

### Cisco IOS File System

The router uses any file system that is supported by your version of Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. A user may wish to enable IFS certificate enrollment when his or her certification authority (CA) does not support Simple Certificate Enrollment Protocol (SCEP).

## Examples

The following example shows how to configure all database entries to be written out to a TFTP server:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level complete
Router#(cs-server) database url tftp://mytftp
```

### Verifying the Database URL

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
Translating "myftpserver"

% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

### Related Commands

Command	Description
<b>crypto pki server</b>	Enables a Cisco IOS certificate server and enters PKI configuration mode.
<b>database level</b>	Controls what type of data is stored in the database.

# deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime** command in server group configuration mode. To set deadtime to 0, use the **no** form of this command.

**deadtime** *minutes*

**no deadtime**

Syntax Description	<i>minutes</i>	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).
--------------------	----------------	--

**Defaults** Deadtime is set to 0.

**Command Modes** Server-group configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

**Usage Guidelines** Use this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

### When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

**Examples** The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
 server 1.1.1.1 auth-port 1645 acct-port 1646
 server 2.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
```

■ **deadtime (server-group configuration)**

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>radius-server deadtime</b>	Sets the deadtime value globally.

## default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the **default** command in ca-trustpoint configuration mode.

**default** *command-name*

<b>Syntax Description</b>	<i>command-name</i> Ca-trustpoint configuration subcommand.
---------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Ca-trustpoint configuration
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

<b>Usage Guidelines</b>	<p>Before you can configure this command, you must enable the <b>crypto ca trustpoint</b> command, which enters ca-trustpoint configuration mode.</p> <p>Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.</p>
-------------------------	---

<b>Examples</b>	<p>The following example shows how to remove the <b>crl optional</b> command from your configuration; the default of <b>crl optional</b> is off.</p> <pre>default crl optional</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

# description (identity policy)

To enter a description for an identity policy, use the **description** command in identity policy configuration mode. To remove the description, use the **no** form of this command.

**description** *line-of-description*

**no description** *line-of-description*

Syntax Description	<i>line-of-description</i>	Description of the identity policy.
--------------------	----------------------------	-------------------------------------

Defaults	A description is not entered for the identity policy.
----------	---

Command Modes	Identity policy configuration
---------------	-------------------------------

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

Examples	The following example shows that a default identity policy and its description (“bluemoon”) have been specified:
----------	--

```
Router (config)# identity policy bluemoon
Router (config-identity-policy)# description policyABC
```

Related Commands	Command	Description
	description (identity profile)	Enters a description for an identity profile.

# description (identity profile)

To enter a description for an identity profile, use the **description** command in identity profile configuration mode. To remove the description of the identity profile, use the **no** form of this command.

**description** *line-of-description*

**no description** *line-of-description*

## Syntax Description

<i>line-of-description</i>	Description of the identity profile.
----------------------------	--------------------------------------

## Defaults

A description is not entered for the identity profile.

## Command Modes

Identity profile configuration

## Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	This command was previously configured in dot1x configuration mode.

## Usage Guidelines

The **identity profile** command and one of its keywords (**default**, **dot1x**, or **eapoudp**) must be entered in global configuration mode before the **description** command can be used.

## Examples

The following example shows that a default identity profile and its description (“ourdefaultpolicy”) have been specified:

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

## Related Commands

Command	Description
<b>description (identity policy)</b>	Enters a description for an identity policy.
<b>identity profile</b>	Creates an identity profile and enters identity profile configuration mode.

# description (isakmp peer)

To add the description of an Internet Key Exchange (IKE) peer, use the **description** command in ISAKMP peer configuration mode. To delete the description, use the **no** form of this command.

**description** *line-of-description*

**no description** *line-of-description*

Syntax Description	<i>line-of-description</i>	Description given to an IKE peer.
--------------------	----------------------------	-----------------------------------

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

Command Modes	ISAKMP peer configuration
---------------	---------------------------

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

Usage Guidelines	IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.
------------------	--

Examples	The following example shows that the description “connection from site A” has been added for an IKE peer:
----------	---

```
Router# crypto isakmp peer address 10.2.2.9
Router (config-isakmp-peer)# description connection from site A
```

Related Commands	Command	Description
	<b>clear crypto session</b>	Deletes crypto sessions (IPSec and IKE SAs).
	<b>show crypto isakmp peer</b>	Displays peer descriptions.
	<b>show crypto session</b>	Displays status information for active crypto sessions in a router.

# device (identity profile)

To statically authorize or reject individual devices, use the **device** command in identity profile configuration mode. To disable the authorization or rejection, use the **no** form of this command.

```
device {authorize {ip address ip-address {policy policy-name} | mac-address mac-address | type
{cisco | ip | phone}} | not-authorize}
```

```
no device {authorize {ip address ip-address {policy policy-name} | mac-address mac-address |
type {cisco | ip | phone}} | not-authorize}
```

## Syntax Description

<b>authorize</b>	Configures an authorized device.
<b>ip address</b>	Specifies a device by its IP address.
<i>ip-address</i>	The IP address.
<b>policy</b>	Applies an associated policy with the device.
<i>policy-name</i>	Name of the policy.
<b>mac-address</b>	Specifies a device by its MAC address.
<i>mac-address</i>	The MAC address.
<b>type</b>	Specifies a device by its type.
<b>cisco</b>	Specifies a Cisco device.
<b>ip</b>	Specifies an IP device.
<b>phone</b>	Specifies a Cisco IP phone.
<b>not-authorize</b>	Configures an unauthorized device.

## Defaults

A device is not statically authorized or rejected.

## Command Modes

Identity profile configuration

## Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The <b>unauthorize</b> keyword was changed to <b>not authorize</b> . The <i>cisco-device</i> argument was deleted. The <b>ip address</b> keyword and <i>ip-address</i> argument were added. The <b>ip</b> and <b>phone</b> keywords were added.

## Usage Guidelines

The **identity profile** command and **default**, **dot1x**, or **eapoudp** keywords must be entered in global configuration mode before the **device** command can be used.

---

**Examples**

The following configuration example defines an identity profile for Extensible Authentication Protocol over UDP (EAPoUDP) to statically authorize host 192.168.1.3 with “greentree” as the associated identity policy:

```
Router(config)# identity profile eapoudp  
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy greentree
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>identity profile eapoudp</b>	Creates an identity profile.

---

# dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of this command.

**dialer aaa** [**password** *string* | **suffix** *string*]

**no dialer aaa** [**password** *string* | **suffix** *string*]

## Syntax Description

<b>password</b> <i>string</i>	(Optional) Defines a nondefault password for authentication. The password string can be a maximum of 128 characters.
<b>suffix</b> <i>string</i>	(Optional) Defines a suffix for authentication. The suffix string can be a maximum of 64 characters.

## Defaults

This feature is not enabled by default.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The <b>password</b> and <b>suffix</b> keywords were added.

## Usage Guidelines

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be “cisco.”



### Note

Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

## Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 1.1.1.1. The username in the access-request message is “1.1.1.1@ciscoDoD” and the password is “cisco.”

```
interface dialer1
dialer aaa
dialer aaa suffix @ciscoDoD password cisco
```

## Related Commands

Command	Description
<b>accept dialout</b>	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.

---

<b>dialer congestion-threshold</b>	Specifies congestion threshold in connected links.
<b>dialer vpdn</b>	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.

---

# disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** command in privileged EXEC mode.

```
disconnect ssh [vty] session-id
```

Syntax Description	vtv	(Optional) Virtual terminal for remote console access.
	<i>session-id</i>	The <i>session-id</i> is the number of connection displayed in the <b>show ip ssh</b> command output.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.

**Usage Guidelines** The **clear line vty n** command, where *n* is the connection number displayed in the **show ip ssh** command output, may be used instead of the **disconnect ssh** command.

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

**Examples** The following example terminates SSH connection number 1:

```
disconnect ssh 1
```

Related Commands	Command	Description
	<b>clear line vty</b>	Returns a terminal line to idle state using the privileged EXEC command.

# dn

To associate the identity of a router with the distinguished name (DN) in the certificate of the router, use the **dn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

```
dn name=string [, name=string]
```

```
no dn name=string [, name=string]
```

## Syntax Description

<i>name=string</i>	Identity used to restrict access to peers with specific certificates. Optionally, you can associate more than one identity.
--------------------	---

## Command Default

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

## Command Modes

Crypto identity configuration

## Command History

Release	Modification
12.2(4)T	This command was introduced.

## Usage Guidelines

Use the **dn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the DN that the peer used to authenticate itself.



### Note

The *name* defined in the **crypto identity** command must match the *string* defined in the **dn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

An encrypting peer matches this list if it contains the attributes listed in any one line defined within the *name=string*.

**Examples**

The following example shows how to configure an IPsec crypto map that can be used only by peers that have been authenticated by the DN and if the certificate belongs to “green”:

```
crypto map map-to-green 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-green
!
crypto identity to-green
  dn ou=green
```

**Related Commands**

Command	Description
<b>crypto identity</b>	Configures the identity of the router with a given list of DNs in the certificate of the router.
<b>fqdn</b>	Associates the identity of the router with the hostname that the peer used to authenticate itself.

## dnis (authentication)

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

**no dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

Syntax Description		
<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.	
<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.	
<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.	
<b>password</b> <i>string</i>	(Optional) Password to use in the Access-Request packet. The default is cisco.	

### Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

### Command Modes

AAA preauthentication configuration

### Command History

Release	Modification
12.1(2)T	This command was introduced.

### Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

### Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
group radius
dnis password Ascend-DNIS
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa preauth</b>	Enters AAA preauthentication mode.
<b>group (authentication)</b>	Selects the security server to use for AAA preauthentication.
<b>isdn guard-timer</b>	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

## dnis (RADIUS)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

```
dnis [if-avail | required] [accept-stop] [password password]
```

```
no dnis [if-avail | required] [accept-stop] [password password]
```

### Syntax Description

<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements such as <b>clid</b> or <b>ctype</b> from being tried once preauthentication has succeeded for a call element.
<b>password</b> <i>password</i>	(Optional) Defines the password for the preauthentication element.

### Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

### Command Modes

AAA preauthentication configuration

### Command History

Release	Modification
12.1(2)T	This command was introduced.

### Usage Guidelines

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

### Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
group radius
dnis required
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clid</b>	Preauthenticates calls on the basis of the CLID number.
<b>ctype</b>	Preauthenticates calls on the basis of the call type.
<b>dnis bypass (AAA preauthentication configuration)</b>	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
<b>group (RADIUS)</b>	Specifies the AAA RADIUS server group to use for preauthentication.

# dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dial Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** command in AAA preauthentication configuration mode. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

```
dnis bypass {dnis-group-name}
```

```
no dnis bypass {dnis-group-name}
```

## Syntax Description

<i>dnis-group-name</i>	Name of the defined DNIS group.
------------------------	---------------------------------

## Defaults

No DNIS numbers are bypassed for preauthentication.

## Command Modes

AAA preauthentication configuration

## Command History

Release	Modification
12.1(2)T	This command was introduced.

## Usage Guidelines

Before using this command, you must first create a DNIS group with the **dialer dnis group** command.

## Examples

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
 group radius
 dnis required
 dnis bypass hawaii
```

```
dialer dnis group hawaii
 number 12345
 number 12346
```

## Related Commands

Command	Description
<b>dialer dnis group</b>	Creates a DNIS group.
<b>dnis (RADIUS)</b>	Preauthenticates calls on the basis of the DNIS number.

# dns

To specify the primary and secondary Domain Name Service (DNS) servers, use the **dns** command in (Internet Security Association Key Management Protocol) ISAKMP group configuration mode. To remove this command from your configuration, use the **no** form of this command.

```
dns primary-server secondary-server
```

```
no dns primary-server secondary-server
```

## Syntax Description

<i>primary-server</i>	Name of the primary DNS server.
<i>secondary-server</i>	Name of the secondary DNS server.

## Defaults

A DNS server is not specified.

## Command Modes

ISAKMP group configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.

## Usage Guidelines

Use the **dns** command to specify the primary and secondary DNS servers for the group.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that needs to be defined or changed, before enabling the **dns** command.

## Examples

The following example shows how to define a primary and secondary DNS server for the default group name:

```
crypto isakmp client configuration group default
key cisco
dns 2.2.2.2 2.3.2.3
pool dog
acl 199
```

## Related Commands

Command	Description
<b>acl</b>	Configures split tunneling.
<b>crypto isakmp client configuration group</b>	Specifies the policy profile of the group that will be defined.
<b>domain (isakmp-group)</b>	Specifies the DNS domain to which a group belongs.

# dnsix-dmdp retries

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no** form of this command.

**dnsix-dmdp retries** *count*

**no dnsix-dmdp retries** *count*

<b>Syntax Description</b>	<i>count</i>	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.
---------------------------	--------------	--

**Defaults** Retransmits messages up to 4 times, or until acknowledged.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Examples** The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>dnsix-nat authorized-redirection</b>
	<b>dnsix-nat primary</b>	Specifies the IP address of the host to which DNSIX audit messages are sent.
	<b>dnsix-nat secondary</b>	Specifies an alternate IP address for the host to which DNSIX audit messages are sent.
	<b>dnsix-nat source</b>	Starts the audit-writing module and defines audit trail source address.
	<b>dnsix-nat transmit-count</b>	Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.

# dnsix-nat authorized-redirection

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** command in global configuration mode. To delete an address, use the **no** form of this command.

**dnsix-nat authorized-redirection** *ip-address*

**no dnsix-nat authorized-redirection** *ip-address*

---

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the host from which redirection requests are permitted.
---------------------------	-------------------	---

---

---

<b>Defaults</b>	An empty list of addresses.
-----------------	-----------------------------

---

---

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

---

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

---

---

<b>Usage Guidelines</b>	Use multiple <b>dnsix-nat authorized-redirection</b> commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.
-------------------------	---

---

---

<b>Examples</b>	The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:
-----------------	--

```
dnsix-nat authorization-redirection 192.168.1.1
```

## dnsix-nat primary

To specify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

**dnsix-nat primary** *ip-address*

**no dnsix-nat primary** *ip-address*

### Syntax Description

<i>ip-address</i>	IP address for the primary collection center.
-------------------	---

### Defaults

Messages are not sent.

### Command Modes

Global configuration

### Command History

Release	Modification
10.0	This command was introduced.

### Usage Guidelines

An IP address must be configured before audit messages can be sent.

### Examples

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.1.1.1
```

# dnsix-nat secondary

To specify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

**dnsix-nat secondary** *ip-address*

**no dnsix-nat secondary** *ip-address*

---

**Syntax Description**

<i>ip-address</i>	IP address for the secondary collection center.
-------------------	---

---

---

**Defaults**

No alternate IP address is known.

---

**Command Modes**

Global configuration

---

**Command History**

Release	Modification
10.0	This command was introduced.

---

---

**Usage Guidelines**

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

---

**Examples**

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

# dnsix-nat source

To start the audit-writing module and to define the audit trail source address, use the **dnsix-nat source** command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

**dnsix-nat source** *ip-address*

**no dnsix-nat source** *ip-address*

Syntax Description	<i>ip-address</i>	Source IP address for DNSIX audit messages.
--------------------	-------------------	---

Defaults	Disabled
----------	----------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	You must issue the <b>dnsix-nat source</b> command before any of the other <b>dnsix-nat</b> commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.
------------------	---

Examples	The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:
----------	---

```
dnsix-nat source 192.168.2.5
interface ethernet 0
 ip address 192.168.2.5 255.255.255.0
```

# dnsix-nat transmit-count

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command in global configuration mode. To revert to the default audit message count, use the **no** form of this command.

**dnsix-nat transmit-count** *count*

**no dnsix-nat transmit-count** *count*

---

**Syntax Description**

<i>count</i>	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.
--------------	---

---

---

**Defaults**

One message is sent at a time.

---

**Command Modes**

Global configuration

---

**Command History**

Release	Modification
10.0	This command was introduced.

---

---

**Usage Guidelines**

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

---

**Examples**

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

# domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the **domain** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

**domain** *name*

**no domain** *name*

## Syntax Description

<i>name</i>	Name of the DNS domain.
-------------	-------------------------

## Defaults

A DNS domain is not specified.

## Command Modes

ISAKMP group configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.

## Usage Guidelines

Use the **domain** command to specify group domain membership.

You must enable the **crypto isakmp configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **domain** command.

## Examples

The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  domain cisco.com
```

## Related Commands

Command	Description
<b>acl</b>	Configures split tunneling.
<b>crypto isakmp client configuration group</b>	Specifies the DNS domain to which a group belongs.
<b>crypto isakmp keepalive</b>	Specifies the primary and secondary DNS servers.

# dot1x default

To reset the global 802.1X parameters to their default values, use the **dot1x default** command in global configuration mode.

## dot1x default

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command has no default setting.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
	12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

**Usage Guidelines** Use the **show dot1x** privileged EXEC command to verify your current 802.1X settings.

**Examples** The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

Related Commands	Command	Description
	<b>dot1x max-req</b>	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
	<b>dot1x re-authentication (EtherSwitch)</b>	Enables periodic reauthentication of the client for the Ethernet switch network module.
	<b>dot1x timeout (EtherSwitch)</b>	Sets retry timeouts for the Ethernet switch network module.
	<b>show dot1x (EtherSwitch)</b>	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

# dot1x initialize

To initialize an interface, use the **dot1x initialize** command in privileged EXEC mode. This command does not have a **no** form.

**dot1x initialize** [**interface** *interface-name*]

## Syntax Description

<b>interface</b>	(Optional) Specifies an interface to be initialized. If this keyword is not entered, all interfaces are initialized.
<i>interface-name</i>	

## Defaults

An interface is not initialized.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Examples

The following example shows that Ethernet 0 is to be initialized:

```
Router# dot1x initialize interface ethernet 0
```

# dot1x max-req

To set the maximum number of times that a router or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req** command in interface configuration or global configuration mode. To disable the number of times that were set, use the **no** form of this command.

**dot1x max-req** *number-of-retries*

**no dot1x max-req** *number-of-retries*

Syntax Description	<i>number-of-retries</i>	Maximum number of retries. The value is from 1 through 10. The default value is 2.
--------------------	--------------------------	--

**Defaults** The default number of retries is 2.

**Command Modes** Interface configuration (router)  
Global configuration (EtherSwitch)

Command History	Release	Modification
	12.1(6)EA2	This command was introduced for the Cisco Ethernet Switch Module.
	12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
	12.3(2)XA	This command was introduced on the following Cisco routers: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

**Usage Guidelines** You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Examples** The following example shows that the maximum number of times that the router will send an EAP request/identity message to the client PC is 6:

```
Router (config) configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that the switch sends an EAP-request/identity frame to 5 before restarting the authentication process:

```
Router (config)# dot1x max-req 5
```

#### Related Commands

Command	Description
<b>dot1x port-control</b>	Sets an 802.1X port control value.
<b>dot1x re-authentication</b>	Enables periodic reauthentication of the client on the 802.1X interface.
<b>dot1x reauthentication (EtherSwitch)</b>	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
<b>dot1x timeout</b>	Sets retry timeouts.
<b>dot1x timeout (EtherSwitch)</b>	Sets retry timeouts for the Ethernet switch network module.
<b>show dot1x</b>	Displays details for an identity profile.
<b>show dot1x (EtherSwitch)</b>	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

## dot1x max-start

To set the maximum number of times that a router sends an Extensible Authentication Protocol (EAP) start frame to the client before concluding that there are no other authenticators present in the network, use the **dot1x max-start** command in interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

**dot1x max-start** *number*

**no dot1x max-start** *number*

Syntax Description	<i>number</i>	Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3.
--------------------	---------------	---

Defaults	The default maximum number setting is 3.
----------	--

Command Modes	Interface configuration
---------------	-------------------------

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

Examples	The following example shows that the maximum number of EAP over LAN- (EAPOL-) Start requests has been set to 5:
----------	---

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
Router (config-if)# dot1x max-start 5
```

Related Commands	Command	Description
	<b>dot1x pae</b>	Sets the PAE type.
	<b>interface</b>	Configures an interface type.

# dot1x multiple-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**dot1x multiple-hosts**

**no dot1x multiple-hosts**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Multiple hosts are disabled.

**Command Modes** Interface configuration

## Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

## Usage Guidelines

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **show dot1x (EtherSwitch)** privileged EXEC command with the **interface** keyword to verify your current 802.1X multiple host settings.

## Examples

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>dot1x default</b>	Enables manual control of the authorization state of the port.
<b>show dot1x (EtherSwitch)</b>	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

# dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

**dot1x pae** [supplicant | authenticator | both]

**no dot1x pae** [supplicant | authenticator | both]

## Syntax Description

<b>supplicant</b>	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
<b>authenticator</b>	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
<b>both</b>	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

## Defaults

PAE type is not set.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.3(11)T	This command was introduced.

## Usage Guidelines

If the **dot1x system-auth-control** command has not been configured, the **supplicant** keyword will be the only keyword available for use with this command. (That is, if the **dot1x system-auth-control** command has not been configured, you cannot configure the **interface as an authenticator**.)

## Examples

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```

## Related Commands

Command	Description
<b>dot1x</b>	Enables 802.1X SystemAuthControl (port-based authentication).
<b>system-auth-control</b>	
<b>interface</b>	Configures an interface type.

# dot1x port-control

To set an 802.1X port control value, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

```
no dot1x port-control {auto | force-authorized | force-unauthorized}
```

## Syntax Description

<b>auto</b>	Determines authentication status of the client PC by the authentication process. The port state will be set to AUTO.
<b>force-authorized</b>	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The <b>force-authorized</b> keyword is the default.
<b>force-unauthorized</b>	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

## Defaults

The default is **force-authorized**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco routers: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

## Usage Guidelines

### For Ethernet Switch Network Modules

The following guidelines apply to Ethernet switch network modules:

The 802.1X protocol is supported on Layer 2 static-access ports.

You can use the **auto** keyword only if the port is not configured as one of these types:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
- Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

You can verify your settings by entering the **show dot1x** (EtherSwitch) privileged EXEC command and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

### Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x port-control auto
```

### Related Commands

Command	Description
<b>dot1x max-req</b>	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
<b>dot1x re-authentication</b>	Enables periodic reauthentication of the client on the 802.1X interface.
<b>dot1x reauthentication (EtherSwitch)</b>	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
<b>dot1x timeout</b>	Sets retry timeouts.
<b>dot1x timeout (EtherSwitch)</b>	Sets retry timeouts for the Ethernet switch network module.
<b>show dot1x</b>	Displays details for an identity profile.
<b>show dot1x (EtherSwitch)</b>	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

## dot1x re-authenticate (EtherSwitch)

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port on a router with an Ethernet switch network module installed, use the **dot1x re-authenticate** command in privileged EXEC mode.

```
dot1x re-authenticate [interface interface-type interface-number]
```

### Syntax Description

<code>interface <i>interface-type interface-number</i></code>	(Optional) Specifies the slot and port number of the interface to reauthenticate.
---	---

### Defaults

There is no default setting.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

### Usage Guidelines

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (reauthperiod) and automatic reauthentication.

### Examples

The following example shows how to manually reauthenticate the device connected to Fast Ethernet interface 0/1:

```
Router# dot1x re-authenticate interface fastethernet 0/1
Starting reauthentication on FastEthernet0/1.
```

## dot1x re-authenticate (privileged EXEC)

To reauthenticate all the authenticated devices that are attached to the specified interface, use the **dot1x re-authenticate** command in privileged EXEC mode. This command does not have a **no** form.

**dot1x re-authenticate** *interface-type interface-number*

### Syntax Description

<i>interface-type</i>	Specifies an interface to be reauthenticated.
<i>interface-name</i>	<ul style="list-style-type: none"> <li>The <i>number of the interface</i> must be 0 or 1.</li> </ul>

### Defaults

An interface is not reauthenticated.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

### Examples

The following example shows that Ethernet 0 is to be reauthenticated:

```
Router# dot1x re-authenticate ethernet 0
```

### Related Commands

Command	Description
<b>clear dot1x</b>	Clears 802.1X interface information.

# dot1x reauthentication

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.

**dot1x reauthentication**

**no dot1x reauthentication**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Periodic reauthentication is not set.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

The reauthentication period can be set using the **dot1x timeout** command.

## Examples

The following example shows that reauthentication has been set for 1800 seconds:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x reauthentication
Router (config-if)# dot1x timeout reauth-period 1800
```

## Related Commands

Command	Description
<b>dot1x max-req</b>	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
<b>dot1x port-control</b>	Sets an 802.1X port control value.
<b>dot1x timeout</b>	Sets retry timeouts.

# dot1x re-authentication (EtherSwitch)

To enable periodic reauthentication of the client for an Ethernet switch network module, use the **dot1x re-authentication** command in global configuration mode. To disable periodic reauthentication, use the **no** form of this command.

**dot1x re-authentication**

**no dot1x re-authentication**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Periodic reauthentication is disabled.

**Command Modes** Global configuration

## Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

## Usage Guidelines

You configure the amount of time between periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

## Examples

The following example shows how to disable periodic reauthentication of the client:

```
Router(config)# no dot1x re-authentication
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

## Related Commands

Command	Description
<b>dot1x timeout (EtherSwitch)</b>	Sets retry timeouts for the Ethernet switch network module.
<b>show dot1x (EtherSwitch)</b>	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

# dot1x system-auth-control

To enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control** command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

**dot1x system-auth-control**

**no dot1x system-auth-control**

## Syntax Description

This command has no arguments or keywords.

## Defaults

System authentication is set to disabled by default. If this command is disabled, all ports behave as if they are force authorized.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Examples

The following example shows that system authentication has been enabled:

```
Router (config)# dot1x system-auth-control
```

## Related Commands

Command	Description
<b>debug dot1x</b>	Displays 802.1X debugging information.
<b>description</b>	Enters an 802.1X description.
<b>device</b>	Statically authorizes or rejects individual devices.
<b>dot1x initialize</b>	Initializes an interface.
<b>dot1x max-req</b>	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
<b>dot1x port-control</b>	Sets an 802.1X port control value.
<b>dot1x re-authenticate</b>	Reauthenticates an 802.1X interface.
<b>dot1x reauthentication</b>	Enables periodic reauthentication of the client PCs on the interface.
<b>dot1x timeout</b>	Sets retry timeouts.
<b>identity profile default</b>	Creates an identity profile and enters dot1x profile configuration mode.
<b>show dot1x</b>	Shows details and statistics for an identity profile.
<b>template</b>	Specifies a virtual template from which commands may be cloned.

# dot1x timeout

To set retry timeouts, use the **dot1x timeout** command in interface configuration mode. To remove the retry timeouts, use the **no** form of this command.

```
dot1x timeout {auth-period seconds | held-period seconds | quiet-period seconds |
ratelimit-period seconds | reauth-period seconds | server-timeout seconds | start-period
seconds | tx-period seconds}
```

```
no dot1x timeout {auth-period seconds | held-period seconds | quiet-period seconds |
ratelimit-period seconds | reauth-period seconds | server-timeout seconds | start-period
seconds | tx-period seconds}
```

Syntax	Description
<b>auth-period</b> <i>seconds</i>	Timeout for authenticator reply. <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 30 seconds.</li> </ul>
<b>held-period</b> <i>seconds</i>	Timeout for authentication retries. <ul style="list-style-type: none"> <li>The value is from 1 to 56535 seconds. The default is 60 seconds.</li> </ul>
<b>quiet-period</b> <i>seconds</i>	Quiet period. <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 120 seconds.</li> </ul>
<b>ratelimit-period</b> <i>seconds</i>	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of router processing power). <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. By default, rate-limiting is disabled.</li> </ul>
<b>reauth-period</b> <i>seconds</i>	Time after which an automatic reauthentication should be initiated. <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 3600 seconds.</li> </ul>
<b>server-timeout</b> <i>seconds</i>	Timeout for RADIUS retries. <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 30 seconds.</li> <li>If an 802.1X packet is sent to the server and the server does not send a response, after the period specified by <b>server-timeout</b> value, the packet will be sent again.</li> </ul>
<b>start-period</b> <i>seconds</i>	Timeout for Extensible Authentication Protocol over LAN- (EAPOL-) Start retries. <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 30 seconds.</li> </ul>
<b>tx-period</b> <i>seconds</i>	Sets the timeout for supplicant (client PC) retries. <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 30 seconds.</li> <li>If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.</li> </ul>

**Defaults** Periodic reauthentication and periodic rate-limiting are not done.

**Command Modes** Interface configuration

**Command History**

Release	Modification
12.3(2)X	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The <b>auth-period</b> , <b>held-period</b> , and <b>start-period</b> keywords were added.

**Examples**

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x port-control auto
Router (config-if)# dot1x reauthentication
Router (config-if)# dot1x timeout auth-period 2000
Router (config-if)# dot1x timeout held-period 2400
Router (config-if)# dot1x timeout reauth-period 1800
Router (config-if)# dot1x timeout quiet-period 600
Router (config-if)# dot1x timeout start-period 90
Router (config-if)# dot1x timeout tx-period 60
Router (config-if)# dot1x timeout server-timeout 60
```

**Related Commands**

Command	Description
<b>dot1x max-req</b>	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
<b>dot1x port-control</b>	Sets an 802.1X port control value.
<b>dot1x reauthentication</b>	Enables periodic reauthentication of the client PCs on the 802.1X interface.

# dot1x timeout (EtherSwitch)

To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
dot1x timeout {quiet-period seconds | re-authperiod seconds | tx-period seconds}
```

```
no dot1x timeout {quiet-period seconds | re-authperiod seconds | tx-period seconds}
```

## Syntax Description

<b>quiet-period</b> <i>seconds</i>	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.
<b>re-authperiod</b> <i>seconds</i>	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
<b>tx-period</b> <i>seconds</i>	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.

## Defaults

**quiet-period:** 60 seconds  
**re-authperiod:** 3660 seconds  
**tx-period:** 30 seconds

## Command Modes

Global configuration

## Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

## Usage Guidelines

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

### quiet-period Keyword

During the quiet period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number than the default.

**re-authperiod Keyword**

The **re-authperiod** keyword affects the behavior of the the Ethernet switch network module only if you have enabled periodic reauthentication by using the **dot1x re-authentication** global configuration command.

**Examples**

The following example shows how to set the quiet time on the switch to 30 seconds:

```
Router(config)# dot1x timeout quiet-period 30
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

The following example shows how to set 60 seconds as the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config)# dot1x timeout tx-period 60
```

**Related Commands**

Command	Description
<b>dot1x max-req</b>	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
<b>dot1x re-authentication (EtherSwitch)</b>	Enables periodic reauthentication of the client for the Ethernet switch network module.
<b>show dot1x (EtherSwitch)</b>	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

# eap

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

<b>username</b> <i>name</i>	Username that will be sent to Request-Id packets.
<b>password</b> <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.

## 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
<b>identity profile</b>	Creates an identity profile.

# 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 <b>no</b> 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.

## 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\$5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$5Rkls3LoyxzS8t9
```

**Related Commands**

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

<b>level</b> <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 <b>no</b> form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the <b>no</b> 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 <b>enable password</b> 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.

## 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**

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

# 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

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

## Defaults

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 <b>3des</b> option was added.
12.2(13)T	The following keywords were added: <b>aes</b> , <b>aes 192</b> , and <b>aes 256</b> .

## 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**

<b>Command</b>	<b>Description</b>
<b>authentication (IKE policy)</b>	Specifies the authentication method within an IKE policy.
<b>crypto isakmp policy</b>	Defines an IKE policy.
<b>group (IKE policy)</b>	Specifies the DH 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.

# 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
	<b>crypto ca profile enrollment</b>	Defines an enrollment profile.
	<b>parameter</b>	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*

<b>Syntax Description</b>	<i>label</i>	Name of the certification authority (CA) trustpoint of another vendor.
<b>Defaults</b>	No default behavior or values.	
<b>Command Modes</b>	Ca-profile-enroll configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(11)T	This command was introduced.

**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**

<b>Command</b>	<b>Description</b>
<b>crypto pki profile enrollment</b>	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	Parameter	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.

**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
	<b>crypto ca trustpoint</b>	Declares the CA that your router should use.
	<b>enrollment</b>	Specifies the enrollment parameters of your CA.

## enrollment mode ra

The **enrollment mode ra** command is replaced by the [enrollment](#) command. See the [enrollment](#) 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**

<b>Command</b>	<b>Description</b>
<b>crypto ca profile enrollment</b>	Defines an enrollment profile.
<b>crypto ca trustpoint</b>	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

No default behavior or values

## Command Modes

ca-trustpoint configuration

## Command History

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

## 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
<b>crypto pki trustpoint</b>	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
	<b>crypto ca profile enrollment</b>	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 <b>pem</b> keyword 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**

<b>Command</b>	<b>Description</b>
<b>crypto ca authenticate</b>	Authenticates the CA (by getting the certificate of the CA).
<b>crypto ca enroll</b>	Obtains the certificate(s) of your router from the certification authority.
<b>crypto ca import</b>	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
<b>crypto ca trustpoint</b>	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-trustpoint)

To specify the enrollment parameters of a 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 period minutes*] [*retry count number*] *url url* [*pem*]

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

### Syntax Description

<b>mode</b>	(Optional) Registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
<b>retry period</b> <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 through 60 minutes.)
<b>retry count</b> <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 through 100 retries.)
<b>url</b> <i>url</i>	URL of the file system where your router should send certificate requests. For enrollment method options, see <a href="#">Table 22</a> .
<b>pem</b>	(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 **url** *url*.

### Command Modes

Ca-trustpoint configuration

### Command History

Release	Modification
11.3T	This command was introduced as the <b>enrollment url (ca-identity)</b> command.
12.2(8)T	This command replaced the <b>enrollment url (ca-identity)</b> command. The <b>mode</b> , <b>retry period</b> <i>minutes</i> , and <b>retry count</b> <i>number</i> keywords and arguments were added.
12.2(13)T	The <b>url</b> <i>url</i> option was enhanced to support TFTP enrollment.
12.3(4)T	The <b>pem</b> keyword was added, and the <b>url</b> <i>url</i> option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).

### 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 period of time (the retry period), the router will send another

certificate request. By default, the router will send a maximum of 10 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 pki authenticate** command.

Use the **url url** option to specify or change the URL of the CA. [Table 22](#) lists the available enrollment methods.

**Table 22 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
SCEP <sup>1</sup>	Enroll via Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL)
null	Enroll via null: file system
nvramp	Enroll via NVRAM: file system
rcp	Enroll via remote copy protocol (rcp): file system
scp	Enroll via secure copy protocol (scp): file system
system	Enroll via system: file system
TFTP <sup>2</sup>	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 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 **pki-trustpoint**.

---

**Examples**

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

```
crypto pki trustpoint ka
  enrollment url http://kahului:80
```

---

**Related Commands**

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

# eou allow

To allow additional Extensible Authentication Protocol over UDP (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

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

## Defaults

No additional EAPoUDP options are allowed.

## Command Modes

Global configuration

## Command History

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

## 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
<b>eou clientless</b>	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

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

## Defaults

Username and password values are clientless.

## Command Modes

Global configuration

## Command History

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

## 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
<b>eou allow</b>	Allows additional EAPoUDP options.

# eou default

To set global Extensible Authentication Protocol over UDP (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  
Interface configuration

---

**Command History**

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

---

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

**Defaults** No default behaviour or values

**Command Modes** Global configuration

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

**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
```

Related Commands	Command	Description
	<b>eou revalidate</b>	Revalidates an EAPoUDP association.

# eou logging

To enable Extensible Authentication Protocol over UDP (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

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

**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=192.43.2.1| HOST=REMOVED|
Interface=FastEthernet0/0.420
```

# eou max-retry

To set the number of maximum retry attempts for Extensible Authentication Protocol over UDP (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*

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

<b>Defaults</b>	The default number of retries is 3.
-----------------	-------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(8)T	This command was introduced.

<b>Usage Guidelines</b>	You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.
-------------------------	---

<b>Examples</b>	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show eou</b>	Displays information about EAPoUDP global values or EAPoUDP session cache entries.

# eou port

To set the UDP port for Extensible Authentication Protocol over UDP (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

## Command History

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

## 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
<b>show eou</b>	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

## Command History

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

## 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 UDP (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

<b>all</b>	Enables revalidation of all EAPoUDP clients. This keyword option is the default.
<b>authentication</b>	Specifies the authentication type.
<b>clientless</b>	Clientless authentication type.
<b>eap</b>	EAP authentication type.
<b>static</b>	Static authentication type.
<b>interface</b> <i>interface-name</i>	Name of the interface. (See <a href="#">Table 23</a> for the types of interface that may be shown.)
<b>ip</b> <i>ip-address</i>	IP address of the client.
<b>mac</b> <i>mac-address</i>	The 48-bit hardware address of the client.
<b>posturetoken</b> <i>string</i>	Name of the posture token.

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

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

[Table 23](#) lists the interface types that may be used with the **interface** keyword.

**Table 23** Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface

**Table 23** Description of Interface Types (continued)

Interface Type	Description
<b>CTunnel</b>	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
<b>Dialer</b>	Dialer interface
<b>Ethernet</b>	IEEE 802.3 standard interface
<b>Lex</b>	Lex interface
<b>Loopback</b>	Loopback interface
<b>MFR</b>	Multilink Frame Relay bundle interface
<b>Multilink</b>	Multilink-group interface
<b>Null</b>	Null interface
<b>Serial</b>	Serial interface
<b>Tunnel</b>	Tunnel interface
<b>Vif</b>	Pragmatic General Multicast (PGM) Multicast Host interface
<b>Virtual-PPP</b>	Virtual PPP interface
<b>Virtual-Template</b>	Virtual template interface
<b>Virtual-TokenRing</b>	Virtual TokenRing interface

**Examples**

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

```
Router# eou revalidate all
```

**Related Commands**

Command	Description
<b>eou initialize</b>	Manually initializes EAPoUDP state machines.

# eou timeout

To set the Extensible Authentication Protocol over UDP (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

<b>aaa</b> <i>seconds</i>	Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.
<b>hold-period</b> <i>seconds</i>	Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.
<b>retransmit</b> <i>seconds</i>	Retransmit period, in seconds. The value range is from 1 through 60. Default=3.
<b>revalidation</b> <i>seconds</i>	Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.
<b>status query</b> <i>seconds</i>	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  
Interface configuration

## Command History

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

## 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
<b>show eou</b>	Displays information about EAPoUDP global values.

# 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

<i>name</i>	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 <b>permit</b> (reflexive) command.
-------------	---

## Defaults

Reflexive access lists are not evaluated.

## Command Modes

Access-list configuration

## Command History

Release	Modification
11.3	This command was introduced.

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