

# parameter

To specify parameters for an enrollment profile, use the **parameter** command in ca-profile-enroll configuration mode. To disable specified parameters, use the **no** form of this command.

**parameter** *number* { **value** *value* | **prompt** *string* }

**no parameter** *number* { **value** *value* | **prompt** *string* }

## Syntax Description

<i>number</i>	User parameters. Valid values range from 1 to 8.
<b>value</b> <i>value</i>	To be used if the parameter has a constant value.
<b>prompt</b> <i>string</i>	To be used if the parameter is supplied after the <b>crypto ca authenticate</b> command or the <b>crypto ca enroll</b> command has been entered.
<b>Note</b>	The value of the <i>string</i> argument does not have an effect on the value that is used by the router.

## Defaults

No enrollment profile parameters are 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

The **parameter** command can be used within an enrollment profile after the **authentication command** command or the **enrollment command** has been enabled.

## Examples

The following example shows how to specify parameters for the enrollment profile named "E":

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

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

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>authentication command</b>	Specifies the HTTP command that is sent to the CA for authentication.
<b>crypto ca profile enrollment</b>	Defines an enrollment profile.
<b>enrollment command</b>	Specifies the HTTP command that is sent to the CA for enrollment.

# parser view

To create or change a command-line interface (CLI) view and enter view configuration mode, use the **parser view** command in global configuration mode. To delete a view, use the **no** form of this command.

**parser view** *view-name*

**no parser view** *view-name*

<b>Syntax Description</b>	<i>view-name</i>	View name, which can include 1 to 30 alphanumeric characters.  The <i>view-name</i> argument must not have a number as the first character; otherwise, you will receive the following error message: "Invalid view name."
---------------------------	------------------	---

<b>Defaults</b>	A CLI view does not exist.
-----------------	----------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(7)T	This command was introduced.

<b>Usage Guidelines</b>	A CLI view is a set of operational commands and configuration capabilities that restrict user access to the CLI and configuration information; that is, a view allows users to define what commands are accepted and what configuration information is visible.
-------------------------	---

After you have issued the **parser view** command, you can configure the view via the **password 5** command and the **commands** command.

To use the **parser view** command, the system of the user must be set to root view. The root view can be enabled via the **enable view** command.

<b>Examples</b>	The following example show how to configure two CLI views, "first" and "second."
-----------------	--

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# password 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# password 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

After you have successfully created a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

After you have successfully deleted a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_DELETED: view 'first' successfully deleted.
```

---

**Related Commands**

Command	Description
<b>commands (view)</b>	Adds commands to a CLI view.
<b>password 5</b>	Associates a CLI view or a superview with a password.

# parser view superview

To create a superview and enter view configuration mode, use the **parser view superview** command in global configuration mode. To delete a superview, use the **no** form of this command.

**parser view** *superview-name* **superview**

**no parser view** *superview-name* **superview**

Syntax Description	<i>superview-name</i>	Superview name, which can include 1 to 30 alphanumeric characters.
		The <i>superview-name</i> argument must not have a number as the first character.

Defaults	A superview does not exist.
----------	-----------------------------

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

Command History	Release	Modification
		12.3(11)T

**Usage Guidelines** A superview consists of one or more command-line interface (CLI) views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain the following characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.

### Adding CLI Views to a Superview

You can add a view to a superview only after a password has been configured for the superview (via the **password 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.



#### Note

Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

---

**Examples**

The following sample output from the **show running-config** command shows that “view\_one” and “view\_two” have been added to superview “su\_view1,” and “view\_three” and “view\_four” have been added to superview “su\_view2”:

```
!  
parser view su_view1 superview  
  password5 <encoded password>  
  view view_one  
  view view_two  
!  
parser view su_view2 superview  
  password5 <encoded password>  
  view view_three  
  view view_four  
!
```

---

**Related Commands**

Command	Description
<b>parser view</b>	Creates or changes a CLI view and enters view configuration mode.
<b>password 5</b>	Associates a CLI view or a superview with a password.
<b>view</b>	Adds a normal CLI view to a superview.

# password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

**password** *string*

**no password**

<b>Syntax Description</b>	<i>string</i>	Name of the password.
---------------------------	---------------	-----------------------

<b>Defaults</b>	You are prompted for the password during certificate enrollment.
-----------------	--

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

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

<b>Usage Guidelines</b>	<p>Before you can issue the <b>password</b> command, you must enable the <b>crypto ca trustpoint</b> command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.</p> <p>This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.</p> <p>If this command is enabled, you will not be prompted for a password during certificate enrollment.</p>
-------------------------	---

<b>Examples</b>	<p>The following example shows how to specify the password “revokme” for the certificate request:</p>
-----------------	---

```
crypto ca trustpoint frog
enrollment url http://frog.phoobin.com/
subject-name OU=Spiral Dept., O=tiedye.com
ip-address ethernet-0
auto-enroll regenerate
password revokme
```

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

# password (line configuration)

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

**password** *password*

**no password**

<b>Syntax Description</b>	<i>password</i>	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.
<b>Defaults</b>	No password is specified.	
<b>Command Modes</b>	Line configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
<b>Usage Guidelines</b>	When an EXEC process is started on a line with password protection, the EXEC prompts for the password. If the user enters the correct password, the EXEC prints its normal privileged prompt. The user can try three times to enter a password before the EXEC exits and returns the terminal to the idle state.	
<b>Examples</b>	The following example removes the password from virtual terminal lines 1 to 4: <pre>line vty 1 4 no password</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>enable password</b>	Sets a local password to control access to various privilege levels.

# password 5



## Note

Effective with Cisco IOS Release 12.3(14)T, this command is replaced by the **secret** command.

To associate a command-line interface (CLI) view or a superview with a password, use the **password 5** command in view configuration mode.

**password 5** *password*

## Syntax Description

*password* Password for users to enter the CLI view or superview. A password can contain any combination of alphanumeric characters.

**Note** The password is case sensitive.

## Defaults

A user cannot access a CLI view or superview.

## Command Modes

View configuration

## Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	This command was enhanced to support superviews.
12.3(14)T	This command was replaced by the secret command.

## Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **password 5** command has been issued.

## Examples

The following example show how to configure two CLI views, “first” and “second” and associate each view with a password:

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# password 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# password 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

**Related Commands**

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

# password encryption aes

To enable a type 6 encrypted preshared key, use the **password encryption aes** command in global configuration mode. To disable password encryption, use the **no** form of this command.

**password encryption aes**

**no password encryption aes**

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

**Defaults** Preshared keys are not encrypted.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(2)T	This command was introduced.

**Usage Guidelines** You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```



**Note** For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

## Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command, the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

### Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.



#### Caution

If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

### Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

### Storing Passwords

Because no one can “read” the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot “know” what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

### Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

#### Examples

The following example shows that a type 6 encrypted preshared key has been enabled:

```
Router (config)# password encryption aes
```

#### Related Commands

Command	Description
<b>key config-key password-encryption</b>	Stores a type 6 encryption key in private NVRAM.
password logging	Provides a log of debugging output for a type 6 password operation.

# password logging

To get a log of debugging output for a type 6 password operation, use the **password logging** command in privileged EXEC mode. To disable the debugging, use the **no** form of this command.

**password logging**

**no password logging**

---

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

---

**Defaults** Debug logging is not enabled.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.3(2)T	This command was introduced.

---



---

**Examples** The following example shows that debug logging is configured:

```
Router# password logging
```

---

Related Commands	Command	Description
	<b>key config-key password-encryption</b>	Stores an encryption key in private NVRAM.
	password encryption aes	Enables a type 6 encrypted preshared key.

---

## permit (reflexive)

To create a reflexive access list and to enable its temporary entries to be automatically generated, use the **permit** command in access-list configuration mode. To delete the reflexive access list (if only one protocol was defined) or to delete protocol entries from the reflexive access list (if multiple protocols are defined), use the **no** form of this command.

**permit** *protocol source source-wildcard destination destination-wildcard reflect name [timeout seconds]*

**no permit** *protocol source-wildcard destination destination-wildcard reflect name*

Syntax Description	
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords <b>gre</b> , <b>icmp</b> , <b>ip</b> , <b>ipinip</b> , <b>nos</b> , <b>tcp</b> , or <b>udp</b> , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol, Transmission Control Protocol, and User Datagram Protocol), use the keyword <b>ip</b> .
<i>source</i>	Number of the network or host from which the packet is being sent. There are three other ways to specify the source: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format.</li> <li>• Use the keyword <b>any</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section “Usage Guidelines”).</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of source 0.0.0.0.</li> </ul>
<i>source-wildcard</i>	Wildcard bits (mask) to be applied to source. There are three other ways to specify the source wildcard: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</li> <li>• Use the keyword <b>any</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section “Usage Guidelines”).</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of source 0.0.0.0.</li> </ul>
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three other ways to specify the destination: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format.</li> <li>• Use the keyword <b>any</b> as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section “Usage Guidelines”).</li> <li>• Use <b>host destination</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of destination 0.0.0.0.</li> </ul>

<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three other ways to specify the destination wildcard: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</li> <li>• Use the keyword <b>any</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally <i>not</i> recommended (see the section “Usage Guidelines”).</li> <li>• Use <b>host</b> <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li> </ul>
<b>reflect</b>	Identifies this access list as a reflexive access list.
<i>name</i>	Specifies the name of the reflexive access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. The name can be up to 64 characters long.
<b>timeout</b> <i>seconds</i>	(Optional) Specifies the number of seconds to wait (when no session traffic is being detected) before entries expire in this reflexive access list. Use a positive integer from 0 to $2^{32}-1$ . If not specified, the number of seconds defaults to the global timeout value.

### Defaults

If this command is not configured, no reflexive access lists will exist, and no session filtering will occur. If this command is configured without specifying a **timeout** value, entries in this reflexive access list will expire after the global timeout period.

### 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.

For this command to work, you must also nest the reflexive access list using the **evaluate** command.

This command creates a reflexive access list and triggers the creation of entries in the same reflexive access list. This command must be an entry (condition statement) in 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 outbound 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 inbound traffic.

IP sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the extended named IP access list, the packet is also evaluated against this reflexive **permit** entry.

As with all access list entries, the order of entries is important, because they are evaluated in sequential order. When an IP packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive **permit** entry, the packet will not be evaluated by the reflexive **permit** entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive **permit** entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive **permit** entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating the packet belongs to a session in progress). The temporary entry specifies criteria that permits traffic into your network only for the same session.

### Characteristics of Reflexive Access List Entries

This command enables the creation of temporary entries in the same reflexive access list that was defined by this command. The temporary entries are created when a packet exiting your network matches the protocol specified in this command. (The packet “triggers” the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a **permit** entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except the port numbers are swapped.

If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: the temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).

- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IP traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IP packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configurable length of time (the timeout period), the entry will expire.

### Examples

The following example defines a reflexive access list *tcptraffic*, in an outbound access list that permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic and denies all ICMP traffic. This example is for an external interface (an interface connecting to an external network).

First, the interface is defined and the access list is applied to the interface for outbound traffic.

```
interface Serial 1
  description Access to the Internet via this interface
  ip access-group outboundfilters out
```

Next, the outbound access list is defined and the reflexive access list *tcptraffic* is created with a reflexive **permit** entry.

```
ip access-list extended outboundfilters
  permit tcp any any reflect tcptraffic
```

## ■ permit (reflexive)

Related Commands	Command	Description
	<b>evaluate</b>	Nests a reflexive access list within an access list.
	<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.

# pfs

To configure a server to notify the client of the central-site policy regarding whether PFS is required for any IP Security (IPSec) Security Association (SA), use the **pfs** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

**pfs**

**no pfs**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The server will not notify the client of the central-site policy regarding whether PFS is required for any IPSec SA.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Before you use the **pfs** command, you must first configure the **crypto isakmp client configuration group** command.

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

```
ipsec:pfs=1
```

## Examples

The following example shows that the server has been configured to notify the client of the central-site policy regarding whether PFS is required for any IPSec SA:

```
crypto isakmp client configuration group
pfs
```

## Related Commands

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

# pki-server

To specify the certificate server that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the easy secure device deployment (EzSDD) petitioner and the EzSDD registrar, use the **pki-server** command in tti-registrar configuration mode. To change the specified certificate server, use the **no** form of this command.

**pki-server** *label*

**no pki-server** *label*

<b>Syntax Description</b>	<i>label</i>	Name of certificate server.
---------------------------	--------------	-----------------------------

<b>Defaults</b>	A certificate server is not associated with the TTI exchange; thus, the petitioner and registrar will not be able to communicate.	
-----------------	---	--

<b>Command Modes</b>	tti-registrar configuration	
----------------------	-----------------------------	--

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

<b>Usage Guidelines</b>	Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.
-------------------------	--

<b>Examples</b>	The following example shows how to associate the certificate server “cs1” with the TTI exchange:
-----------------	--

```
crypto wui tti registrar
pki-server cs1
```

<b>Related Commands</b>	Command	Description
	<b>crypto pki server</b>	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
<b>crypto wui tti registrar</b>	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.	

## pool (isakmp-group)

To define a local pool address, use the **pool** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a local pool from your configuration, use the **no** form of this command.

**pool** *name*

**no pool** *name*

### Syntax Description

<i>name</i>	Name of the local pool address.
-------------	---------------------------------

### Defaults

No default behavior or values.

### Command Modes

ISAKMP group configuration

### Command History

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

### Usage Guidelines

Use the **pool** command to refer to an IP local pool address, which defines a range of addresses that will be used to allocate an internal IP address to a client. Although a user must define at least one pool name, a separate pool may be defined for each group policy.



#### Note

This command must be defined and refer to a valid IP local pool address, or the client connection will fail.

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

### Examples

The following example shows how to refer to the local pool address “dog”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
ip local pool dog 10.1.1.1 10.1.1.254
```

## ■ pool (isakmp-group)

## 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>ip local pool</b>	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

# port-forward

To list the set of forwarded ports to which a user has access, use the **port-forward** command in Web VPN configuration mode. To remove ports, use the **no** form of this command.

```
port-forward {list list-name} {local-port port-number} {remote-server
server-name-or-IP-address} {remote-port port-number}
```

```
no port-forward {list list-name} {local-port port-number} {remote-server
server-name-or-IP-address} {remote-port port-number}
```

Syntax Description		
<b>list</b> <i>list-name</i>		Used to group port-forwarding entries into a list that can be applied to a username or group policy. Multiple entries may be specified for a given list name.
<b>local-port</b> <i>port-number</i>		Specifies the local port that is listened upon. A local port value may be used only once within a given list name. Values may be from 1 through 65535.
<b>remote-server</b> <i>server-name-or-IP-address</i>		Specifies the domain name system (DNS) name or IP address of the remote server to which the user will connect (usually the name or IP address of an e-mail server).
<b>remote-port</b> <i>port-number</i>		Specifies the port on the remote server to which the user will connect. The port value may be from 1 through 65535.

**Defaults** No default behavior or values.

**Command Modes** Web VPN configuration

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

**Usage Guidelines** This command is used for TCP port forwarding.

**Examples** The following example shows that the list name is POP3, the local port is 60002, the remote server is mail.youremail.com, and the remote port number is 25:

```
Router (config)# webvpn
Router (config-webvpn)# port-forward list POP3 local-port 60002 remote-server
mail.youremail.com remote-port 25
```

Related Commands	Command	Description
	<b>webvpn</b>	Enters Web VPN configuration mode.

## port-misuse

To permit or deny HTTP traffic through the firewall on the basis of specified applications in the HTTP message, use the **port-misuse** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

**port-misuse** {p2p | tunneling | im | default} action {reset | allow} [alarm]

**no port-misuse** {p2p | tunneling | im | default} action {reset | allow} [alarm]

Syntax Description		
<b>p2p</b>	Peer-to-peer protocol applications subject to inspection: Kazaa and Gnutella.	
<b>tunneling</b>	Tunneling applications subject to inspection: HTTPPort/HTTPHost, GNU Httptunnel, GotoMyPC, Firethru, Http-tunnel.com Client	
<b>im</b>	Instant messaging protocol applications subject to inspection: Yahoo Messenger.	
<b>default</b>	All applications are subject to inspection.	
<b>action</b>	Applications detected within the HTTP messages that are outside of the specified application are subject to the specified action ( <b>reset</b> or <b>allow</b> ).	
<b>reset</b>	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.	
<b>allow</b>	Forwards the packet through the firewall.	
<b>alarm</b>	(Optional) Generates system logging (syslog) messages for the given action.	

**Defaults** If this command is not enabled, HTTP messages are permitted through the firewall if any of the applications are detected within the message.

**Command Modes** appfw-policy-http configuration

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

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

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
    strict-http action allow alarm
    content-length maximum 1 action allow alarm
    content-type-verification match-req-rsp action allow alarm
    max-header-length request 1 response 1 action allow alarm
    max-uri-length 1 action allow alarm
    port-misuse default action allow alarm
```

```
request-method rfc default action allow alarm
request-method extension default action allow alarm
transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

# ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

**ppp accounting default**

**no ppp accounting**

Syntax Description	<b>default</b>	The name of the method list is created with the <b>aaa accounting</b> command.
Defaults	Accounting is disabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	11.3 T	This command was introduced.
Usage Guidelines	After you enable the <b>aaa accounting</b> command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the <b>ppp accounting</b> command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.	
Examples	The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:  <pre>interface async 4   encapsulation ppp   ppp accounting charlie</pre>	
Related Commands	Command	Description
	<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security purposes.

# ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

**no ppp authentication**

Syntax Description	
<i>protocol1</i> [ <i>protocol2...</i> ]	At least one of the keywords described in <a href="#">Table 29</a> .
<b>if-needed</b>	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
<i>list-name</i>	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the <b>aaa authentication ppp</b> command.
<b>default</b>	(Optional) Name of the method list created with the <b>aaa authentication ppp</b> command.
<b>callin</b>	(Optional) Authentication on incoming (received) calls only.
<b>one-time</b>	(Optional) The username and password are accepted in the username field.
<b>optional</b>	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

**Defaults** PPP authentication is not enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(1)	The <b>optional</b> keyword was added.
	12.1(3)XS	The <b>optional</b> keyword was added.
	12.2(2)XB5	Support for the <b>eap</b> authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
	12.2(13)T	The <b>eap</b> authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines**

When you enable PAP, CHAP, or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

**Caution**

If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 29 lists the protocols used to negotiate PPP authentication.

**Table 29** *ppp authentication Protocols*

<b>chap</b>	Enables CHAP on a serial interface.
<b>eap</b>	Enables EAP on a serial interface.
<b>ms-chap</b>	Enables MS-CHAP on a serial interface.
<b>pap</b>	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

**Examples**

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

---

**Related Commands**

Command	Description
<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
<b>aaa new-model</b>	Enables the AAA access control model.
<b>autoselect</b>	Configures a line to start an ARAP, PPP, or SLIP session.
<b>encapsulation</b>	Sets the encapsulation method used by the interface.
<b>ppp accm</b>	Identifies the ACCM table.
<b>username</b>	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

# ppp authentication ms-chap-v2

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication on a network access server (NAS), use the **ppp authentication ms-chap-v2** command in interface configuration mode. To disable MSCHAP V2 authentication, use the **no** form of this command.

**ppp authentication ms-chap-v2**

**no ppp authentication ms-chap-v2**

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

**Defaults** MSCHAP V2 authentication is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(2)XB5	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** To enable MSCHAP V2 authentication, first configure PPP on the NAS. For the NAS to properly interpret authentication failure attributes and vendor-specific attributes, the **ppp max-bad-auth** command must be configured to allow at least two authentication retries and the **radius-server vsa send** command and **authentication** keyword must be enabled. The NAS must be able to interpret authentication failure attributes and vendor-specific attributes to support the ability to change an expired password.

**Examples** The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 username client password secret
```

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
```

```
no peer default ip address
ppp max-bad-auth 3
ppp authentication ms-chap-v2
exit
aaa authentication ppp default group radius
radius-server host 10.0.0.2 255.0.0.0
radius-server key secret
radius-server vsa send authentication
```

**Related Commands**

Command	Description
<b>debug aaa authentication</b>	Displays information on AAA/TACACS+ authorization.
<b>debug ppp</b>	Displays information on traffic and exchanges in a network that is implementing PPP.
<b>debug radius</b>	Displays information associated with RADIUS.
<b>ppp max-bad-auth</b>	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
<b>radius-server vsa send</b>	Configures the network access server to recognize and use VSAs.

# ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization** command in interface configuration mode. To disable authorization, use the **no** form of this command.

**ppp authorization** [**default** | *list-name*]

**no ppp authorization**

Syntax Description	default	(Optional) The name of the method list is created with the <b>aaa authorization</b> command.
	<i>list-name</i>	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the <b>aaa authorization</b> command.

**Defaults** Authorization is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

**Usage Guidelines** After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

**Examples** The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp authorization charlie
```

Related Commands	Command	Description
	<b>aaa authorization</b>	Sets parameters that restrict user access to a network.

# ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname** command in interface configuration mode. To disable this function, use the **no** form of this command.

**ppp chap hostname** *hostname*

**no ppp chap hostname** *hostname*

## Syntax Description

*hostname* The name sent in the CHAP challenge.

## Defaults

Disabled. The router name is sent in any CHAP challenges.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.2	This command was introduced.

## Usage Guidelines

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

## Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specifies “ppp” as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username *ISPCorp* will be sent in all CHAP challenges and responses.

```
interface dialer 0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ISPCorp
```

## Related Commands

Command	Description
<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
<b>ppp authentication</b>	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
<b>ppp chap password</b>	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
<b>ppp chap refuse</b>	Refuses CHAP authentication from peers requesting it.
<b>ppp chap wait</b>	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

# ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password** command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

**ppp chap password** *secret*

**no ppp chap password** *secret*

<b>Syntax Description</b>	<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.2	This command was introduced.
<b>Usage Guidelines</b>	<p>This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.</p> <p>This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.</p>	
<b>Examples</b>	<p>The commands in the following example specify ISDN BRI number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.</p> <pre>interface bri 0  encapsulation ppp  ppp chap password 7 1234567891</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
	<b>ppp authentication</b>	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
<b>ppp authentication ms-chap-v2</b>	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
<b>ppp chap refuse</b>	Refuses CHAP authentication from peers requesting it.
<b>ppp chap wait</b>	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

# ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

**ppp chap refuse [callin]**

**no ppp chap refuse [callin]**

<b>Syntax Description</b>	<b>callin</b> (Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.
---------------------------	--

<b>Defaults</b>	Disabled
-----------------	----------

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3	This command was introduced.
Release	Modification				
10.3	This command was introduced.				

**Usage Guidelines** This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

**Examples** The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication.

```
interface bri 0
 encapsulation ppp
 ppp chap refuse
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>aaa authentication ppp</b></td> <td>Specifies one or more AAA authentication methods for use on serial interfaces running PPP.</td> </tr> <tr> <td><b>ppp authentication</b></td> <td>Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.</td> </tr> </tbody> </table>	Command	Description	<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.	<b>ppp authentication</b>	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Command	Description						
<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.						
<b>ppp authentication</b>	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.						

Command	Description
<b>ppp authentication ms-chap-v2</b>	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
<b>ppp chap password</b>	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
<b>ppp chap wait</b>	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

# ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

**ppp chap wait** *secret*

**no ppp chap wait** *secret*

<b>Syntax Description</b>	<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------------------	---------------	--

<b>Defaults</b>	Enabled
-----------------	---------

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

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

<b>Usage Guidelines</b>	This command (which is enabled by default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The <b>no</b> form of this command specifies that the router will respond immediately to an authentication challenge.
-------------------------	--

<b>Examples</b>	The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves.
-----------------	---

```
interface bri 0
 encapsulation ppp
 no ppp chap wait
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
	<b>ppp authentication</b>	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
	<b>ppp authentication ms-chap-v2</b>	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.

Command	Description
<b>ppp chap password</b>	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
<b>ppp chap refuse</b>	Refuses CHAP authentication from peers requesting it.

# ppp eap identity

To specify the Extensible Authentication Protocol (EAP) identity, use the **ppp eap identity** command in interface configuration mode. To remove the EAP identity from your configuration, use the **no** form of this command.

**ppp eap identity** *string*

**no ppp eap identity** *string*

<b>Syntax Description</b>	<i>string</i>	EAP identity.
---------------------------	---------------	---------------

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XB5	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

<b>Usage Guidelines</b>	Use the <b>ppp eap identity</b> command to configure the client to use a different identity when requested by the peer.
-------------------------	---

<b>Examples</b>	The following example shows how to enable EAP on dialer interface 1 and set the identity to “cat”:
-----------------	--

```
interface dialer 1
 encapsulation ppp
 ppp eap identity cat
```

# ppp eap local

To authenticate locally instead of using the RADIUS back-end server, use the **ppp eap local** command in interface configuration mode. To reenble proxy mode (which is the default), use the **no** form of this command.

**ppp eap local**

**no ppp eap local**

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

**Defaults** Authentication is performed via proxy mode.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(2)XB5	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** By default, Extensible Authentication Protocol (EAP) runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the **ppp eap local** command.

In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

**Examples** The following example shows how to configure EAP to authenticate locally:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
 ppp eap local
```

Related Commands	Command	Description
	<b>ppp authentication</b>	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

# ppp eap password

To set the Enhanced Authentication Protocol (EAP) password for peer authentication, use the **ppp eap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

**ppp eap password** [*number*] *string*

**no ppp eap password** [*number*] *string*

Syntax Description		
	<i>number</i>	(Optional) Encryption type, including values 0 through 7; 0 means no encryption.
	<i>string</i>	Character string that specifies the EAP password.

**Defaults** No default behavior or values

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(2)XB5	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** For remote EAP authentication only, you can configure your router to create a common EAP password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor or from an older running version of the Cisco IOS software) to which a new (that is, unknown) router has been added, the common password will be used to respond to the new router. The **ppp eap password** command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

**Examples** The following example shows how to set the EAP password “7 141B1309” on the client:

```
ppp eap identity user
ppp eap password 7 141B1309
```

# ppp eap refuse

To refuse Enhanced Authentication Protocol (EAP) from peers requesting it, use the **ppp eap refuse** command in interface configuration mode. To return to the default, use the **no** form of this command.

**ppp eap refuse [callin]**

**no ppp eap refuse [callin]**

<b>Syntax Description</b>	<b>callin</b> (Optional) Authentication is refused for incoming calls only.
---------------------------	---

<b>Defaults</b>	The server will not refuse EAP authentication challenges received from the peer.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	

<b>Usage Guidelines</b>	Use the <b>ppp eap refuse</b> command to disable EAP authentication for all calls. If the <b>callin</b> keyword is used, the server will refuse to answer EAP authentication challenges received from the peer but will still require the peer to answer any EAP challenges the server sends.
-------------------------	---

<b>Examples</b>	The following example shows how to refuse EAP authentication on incoming calls from the peer:
-----------------	---

```
ppp authentication eap
ppp eap local
ppp eap refuse callin
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ppp authentication</b>	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

# ppp eap wait

To configure the server to delay the Enhanced Authentication Protocol (EAP) authentication until after the peer has authenticated itself to the server, use the **ppp eap wait** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

**ppp eap wait**

**no ppp eap wait**

---

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

---

**Defaults** No default behavior or values

---

**Command Modes** Interface configuration

---

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

---

---

**Usage Guidelines** Use the **ppp eap wait** command to specify that the server will not authenticate to a peer requesting EAP authentication until after the peer has authenticated itself to the server.

---

**Examples** The following example shows how to configure the server to wait for the peer to authenticate itself first:

```
ppp authentication eap
ppp eap local
ppp eap wait
```

---

Command	Description
<b>ppp authentication</b>	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

---

# ppp pap refuse

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol (PAP), use the **ppp pap refuse** command in interface configuration mode. To disable the refusal, use the **no** form of this command.

**ppp pap refuse**

**no ppp pap refuse**

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

**Defaults** No default behavior or values.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.

**Usage Guidelines** Use this command to refuse remote PAP support; for example, to respond to the peer request to authenticate with PAP.

This is a per-interface command.

**Examples** The following example shows how to enable the **ppp pap** command to refuse a peer request for remote authentication:

```
interface dialer 0
 encapsulation ppp
 ppp pap refuse
```

Related Commands	Command	Description
	<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP and TACACS+.
	<b>encapsulation ppp</b>	Sets PPP as the encapsulation method used by a serial or ISDN interface.
	<b>ppp authentication</b>	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication are selected on the interface.
	<b>ppp pap sent-username</b>	Reenables remote PAP support for an interface and uses the <b>sent-username</b> and <b>password</b> in the PAP authentication request packet to the peer.

# ppp pap sent-username

To reenble remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

**ppp pap sent-username** *username* **password** *password*

**no ppp pap sent-username**

Syntax Description		
	<i>username</i>	Username sent in the PAP authentication request.
	<b>password</b>	Password sent in the PAP authentication request.
	<i>password</i>	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

**Defaults** Remote PAP support disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.

**Usage Guidelines** Use this command to reenble remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

This is a per-interface command. You must configure this command for each interface.

**Examples** The following example identifies dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. *ISPCorp* is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
 ppp authentication chap pap callin
 ppp chap hostname ISPCorp
 ppp pap sent username ISPCorp password 7 fjhfeu
```

Related Commands	Command	Description
	<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
	<b>ppp authentication</b>	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
	<b>ppp authentication ms-chap-v2</b>	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
	<b>ppp chap password</b>	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.

# pre-shared-key

To define a preshared key to be used for Internet Key Exchange (IKE) authentication, use the **pre-shared-key** command in keyring configuration mode. To disable the preshared key, use the **no** form of this command.

```
pre-shared-key {address address [mask] | hostname hostname} key key
```

```
no pre-shared-key {address address [mask] | hostname hostname} key key
```

Syntax Description	
<b>address</b> <i>address</i> [ <i>mask</i> ]	IP address of the remote peer or a subnet and mask. The <i>mask</i> argument is optional.
<b>hostname</b> <i>hostname</i>	Fully qualified domain name (FQDN) of the peer.
<b>key</b> <i>key</i>	Specifies the secret.

**Defaults** No default behaviors or values

**Command Modes** Keyring configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.3(2)T	This command was modified so that output for the <b>pre-shared-key</b> command will show that the preshared key is either encrypted or unencrypted.

**Usage Guidelines** Before configuring preshared keys, you must configure an Internet Security Association and Key Management Protocol (ISAKMP) profile.

Output for the **pre-shared-key** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key test123
```

An output example for a type 6 encrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key 6 RHZE[JACMUI\|bcbTdELISAAB
```

**Examples** The following example shows how to configure a preshared key using an IP address and host name:

```
Router (config)# crypto keyring vpnkeyring
Router (config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
Router (config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

# primary

To assign a specified trustpoint as the primary trustpoint of the router, use the **primary** command in ca-trustpoint configuration mode.

**primary** *name*

<b>Syntax Description</b>	<i>name</i>	Name of the primary trustpoint of the router.
---------------------------	-------------	---

<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>	Use the <b>primary</b> command to specify a given trustpoint as primary. Before you can configure this command, you must enable the <b>crypto ca trustpoint</b> command, which defines the trustpoint and enters ca-trustpoint configuration mode.
-------------------------	---

<b>Examples</b>	The following example shows how to configure the trustpoint “ka” as the primary trustpoint:
-----------------	---

```
crypto ca trustpoint ka
  enrollment url http://xxx
  primary
  crl optional
```

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

# privilege

To configure a new privilege level for users and associate commands with that privilege level, use the **privilege** command in global configuration mode. To reset the privilege level of the specified command or commands to the default and remove the privilege level configuration from the running configuration file, use the **no** form of this command.



## Note

As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

**privilege mode** [**all**] {**level level** / **reset**} *command-string*

**no privilege mode** [**all**] {**level level** / **reset**} *command-string*

## Syntax Description

<i>mode</i>	Configuration mode for the specified command. See <a href="#">Table 30</a> in the “Usage Guidelines” section for a list of options for this argument.
<b>all</b>	(Optional) Changes the privilege level for all the suboptions to the same level.
<b>level level</b>	Specifies the privilege level you are configuring for the specified command or commands. The level argument must be a number from 0 to 15.
<b>reset</b>	Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running configuration file.  <b>Note</b> For Cisco IOS software releases earlier than Release 12.3(6) and Release 12.3(6)T, you use the <b>no</b> form of this command to reset the privilege level to the default. The default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the <b>reset</b> keyword.
<i>command-string</i>	Command associated with the specified privilege level. If the <b>all</b> keyword is used, specifies the command and subcommands associated with the privilege level.

## Defaults

User EXEC mode commands are privilege level 1.

Privileged EXEC mode and configuration mode commands are privilege level 15.

## Command Modes

Global configuration

## Command History

Release	Modification
10.3	This command was introduced.
12.0(22)S, 12.2(13)T	The <b>all</b> keyword was added.
12.3(6), 12.3(6)T	The <b>no</b> form of the command performs the same function as the <b>reset</b> keyword.

**Usage Guidelines**

The password for a privilege level defined using the **privilege** global configuration command is configured using the **enable secret** command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

**Note**

There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15—unless you set them individually to different levels. This is necessary because you can't execute, for example, the **show ip** command unless you have access to **show** commands.

To change the privilege level of a group of commands, use the **all** keyword. When you set a group of commands to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if you set the **show ip** keywords to level 5, **show** and **ip** will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

Table 30 shows some of the keyword options for the mode argument in the **privilege** command. The available mode keywords will vary depending on your hardware and software version. To see a list of available mode options on your system, use the **privilege ?** command.

**Table 30** mode Argument Options

Command	Description
<b>accept-dialin</b>	VPDN group accept dialin configuration mode
<b>accept-dialout</b>	VPDN group accept dialout configuration mode
<b>address-family</b>	Address Family configuration mode
<b>alps-ascu</b>	ALPS ASCU configuration mode
<b>alps-circuit</b>	ALPS circuit configuration mode
<b>atm-bm-config</b>	ATM bundle member configuration mode
<b>atm-bundle-config</b>	ATM bundle configuration mode
<b>atm-vc-config</b>	ATM virtual circuit configuration mode
<b>atmsig_e164_table_mode</b>	ATMSIG E164 Table
<b>cascustom</b>	Channel-associated signalling (cas) custom configuration mode
<b>config-rtr-http</b>	RTR HTTP raw request Configuration
<b>configure</b>	Global configuration mode
<b>controller</b>	Controller configuration mode
<b>crypto-map</b>	Crypto map config mode
<b>crypto-transform</b>	Crypto transform config modeCrypto transform configuration mode

Table 30 mode Argument Options (continued)

Command	Description
<b>dhcp</b>	DHCP pool configuration mode
<b>dspfarm</b>	DSP farm configuration mode
<b>exec</b>	Exec mode
<b>flow-cache</b>	Flow aggregation cache configuration mode
<b>gateway</b>	Gateway configuration mode
<b>interface</b>	Interface configuration mode
<b>interface-dlci</b>	Frame Relay DLCI configuration mode
<b>ipenacl</b>	IP named extended access-list configuration mode
<b>ipsnacl</b>	IP named simple access-list configuration mode
<b>ip-vrf</b>	Configure IP VRF parameters
<b>lane</b>	ATM Lan Emulation Leacs Configuration Table
<b>line</b>	Line configuration mode
<b>map-class</b>	Map class configuration mode
<b>map-list</b>	Map list configuration mode
<b>mpoa-client</b>	MPOA Client
<b>mpoa-server</b>	MPOA Server
<b>null-interface</b>	Null interface configuration mode
<b>preaut</b>	AAA Preauth definitions
<b>request-dialin</b>	VPDN group request dialin configuration mode
<b>request-dialout</b>	VPDN group request dialout configuration mode
<b>route-map</b>	Route map configuration mode
<b>router</b>	Router configuration mode
<b>rsvp_policy_local</b>	
<b>rtr</b>	RTR Entry Configuration
<b>sg-radius</b>	RADIUS server group definition
<b>sg-tacacs+</b>	TACACS+ server group
<b>sip-ua</b>	SIP UA configuration mode
<b>subscriber-policy</b>	Subscriber policy configuration mode
<b>tcl</b>	Tcl mode
<b>tdm-conn</b>	TDM connection configuration mode
<b>template</b>	Template configuration mode
<b>translation-rule</b>	Translation Rule configuration mode
<b>vc-class</b>	VC class configuration mode
<b>voiceclass</b>	Voice Class configuration mode
<b>voiceport</b>	Voice configuration mode

Table 30 mode Argument Options (continued)

Command	Description
<b>voipdialpeer</b>	Dial Peer configuration mode
<b>vpdn-group</b>	VPDN group configuration mode

## Examples

The following example shows how to set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands:

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

The following example shows how to set the **show** and **ip** keywords to level 5. The suboptions coming under **ip** will also be allowed to users with privilege level 5 access:

```
Router(config)# privilege exec all level 5 show ip
```

The following two examples demonstrate the difference in behavior between the **no** form of the command and the use of the **reset** keyword when using Cisco IOS software releases earlier than Releases 12.3(6) and Release 12.3(6)T.



### Note

As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no privilege exec level 3 configure terminal
Router(config)# end
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 15 configure terminal
privilege exec level 15 configure
```

Note that in the **show running-config** output above, the privilege command for “configure terminal” still appears, but now has the default privilege level assigned.

To remove a previously configured privilege command entirely from the configuration, use the **reset** keyword, as shown in the following example:

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# privilege exec reset configure terminal
Router(config)#
```

```
Router# show running-config | include priv
privilege configure all level 3 interface
Router#
```

---

**Related Commands**

Command	Description
<b>enable password</b>	Sets a local password to control access to various privilege levels.
<b>enable secret</b>	Specifies an additional layer of security over the <b>enable password</b> command.
<b>privilege level</b>	Sets the default privilege level for a line.

# privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

**privilege level** *level*

**no privilege level**

Syntax Description	<i>level</i>	Privilege level associated with the specified line.
--------------------	--------------	---

Defaults	Level 15 is the level of access permitted by the enable password. Level 1 is normal EXEC-mode user privileges.
----------	---

Command Modes	Line configuration
---------------	--------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the <b>disable</b> command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.
------------------	--

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict line usage.

Examples	The following example configures the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:
----------	--

```
line aux 0
 privilege level 5
```

The following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The following example sets the **show ip route** to level 7 and the **show** and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

---

**Related Commands**

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

# qos-group

To apply a quality of service (QoS) group value to an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **qos-group** command in ISAKMP profile configuration mode. To disable the group value, use the **no** form of this command.

**qos-group** *group-number*

**no qos-group** *group-number*

<b>Syntax Description</b>	<i>group-number</i>	Number of the group number. The value ranges from 1 through 99. (There is no default value.)
---------------------------	---------------------	--

**Defaults** A QoS group value is not applied to an ISAKMP profile.

**Command Modes** ISAKMP profile configuration

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

**Usage Guidelines** If there is no matching QoS group set in a QoS policy, or if a service policy is not configured or applied to an interface that also has a crypto map applied, the ISAKMP profile setting (using the **qos-group** command) is not enforced.

**Examples** The following example shows that QoS group “2” has been applied to the ISAKMP profile “class1”:

```
Router (config)# crypto isakmp profile class1
Router (conf-isa-prof)# qos-group 2
! A profile is deemed incomplete until it has match identity statements.
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>crypto isakmp profile</b>	Defines an ISAKMP profile and audits IPsec user sessions.

# query certificate

To configure query certificates on a per-trustpoint basis, use the **query certificate** command in ca-trustpoint configuration mode. To disable creation of query certificates per trustpoint, use the **no** form of this command.

**query certificate**

**no query certificate**

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

**Defaults** Query certificates are stored in NVRAM.

**Command Modes** Ca-trustpoint configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.

**Usage Guidelines** Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to prevent certificates from being stored locally; instead, they are retrieved from a specified certification authority (CA) trustpoint when needed. This will save NVRAM space but could result in a slight performance impact. Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.

### Using the query certificate Command with a Specific Trustpoint

When the **query certificate** command is used, certificates associated with the specified trustpoint will not be written into NVRAM, and the certificate query will be attempted during the next reload of the router.

### Applying the Query Mode Globally

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certificate query** command is used, any previously query certificate configuration will be removed from all trustpoints, and any query in progress will be halted and the feature disabled.

**Examples** The following example shows how to configure a trustpoint and initiate query mode for certificate authority:

```
crypto ca trustpoint trustpoint1
  enrollment url http://trustpoint1
  crl query ldap://trustpoint1
```

## ■ query certificate

```
query certificate
exit
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>crypto ca certificate query</b>	Specifies that certificates should not be stored locally but retrieved from a CA trustpoint.
<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

# query url



## Note

Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **cr1 query** command.

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **query url** command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete (LDAP) URL, use **no** form of this command.

```
query url ldap://hostname:[port]
```

```
query url ldap://hostname:[port]
```

## Syntax Description

<b>ldap://hostname</b>	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
<b>:port</b>	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

## Defaults

No enabled. If **query url ldap://hostname:[port]** is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap://myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

## Command Modes

Ca-trustpoint configuration

## Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	This command was replaced by the <b>cr1 query</b> command.

## Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example 1: http://10.10.10.10:81/myca.crl)
- LDAP URL (Example 2: ldap://10.10.10.10:3899/CN=myca, O=cisco or Example 3: ldap:///CN=myca, O=cisco)

- LDAP/X.500 DN (Example 4: CN=myca, O=cisco)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The **ldap://hostname:[port]** keywords and arguments are used to provide this information.



#### Note

The **crypto ca 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 ca-trustpoint.

#### Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint mytp
  enrollment url http://bar.cisco.com
  query url ldap://bar.cisco.com:3899
```

#### Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

# quit

To exit from the key-string mode while defining the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **quit** command in public key configuration mode.

**quit**

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

**Defaults** No default behavior or values

**Command Modes** Public key configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

**Usage Guidelines** Use this command to exit text mode while defining the RSA public key.

**Examples** The following example shows that the RSA public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands	Command	Description
	<b>address</b>	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
	<b>key-string (IKE)</b>	Specifies the RSA public key of a remote peer.