

accounting (line)

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

accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

no accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

Syntax Description

arap	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
commands <i>level</i>	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
default	(Optional) The name of the default method list, created with the aaa accounting command.
<i>list-name</i>	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the aaa accounting command.

Defaults

Accounting is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

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

Examples

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

```
line 10
 accounting commands 15 charlie
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

accounting (gatekeeper)

To enable accounting services on the gatekeeper, use the **accounting** command in gatekeeper configuration mode. To disable accounting services, use the **no** form of this command.

accounting [vsa]

no accounting [vsa]

Syntax Description	vsa	(Optional) Configures the vendor-specific attribute (VSA) method of accounting.
--------------------	-----	---

Defaults	Accounting is disabled.
----------	-------------------------

Command Modes	Gatekeeper configuration
---------------	--------------------------

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
	12.1(5)XM	The vsa keyword was added.
	12.2(2)T	The vsa keyword was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.

Usage Guidelines	Specify a RADIUS server before using the accounting command. There are three different methods of accounting. The H.323 method sends the call detail record (CDR) to the RADIUS server, the syslog method uses the system logging facility to record the CDRs, and the VSA method collects VSAs.
------------------	--

Examples	The following example enables the gateway to report user activity to the RADIUS server in the form of connection accounting records:
----------	--

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting
```

The following example shows how to enable VSA accounting:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting exec vsa
```

■ **accounting (gatekeeper)****Related Commands**

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

accounting (server-group)

To specify an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request, use the **accounting** command in server-group configuration mode.

accounting [**accept** | **reject**] *list-name*

Syntax Description

accept	(Optional) All attributes will be rejected except for required attributes and the attributes specified in the <i>listname</i> .
reject	(Optional) All attributes will be accepted except for the attributes specified in the <i>listname</i> .
<i>list-name</i>	Given name for the accept or reject list.

Defaults

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

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS accounting allows users to send only the accounting attributes their business requires, thereby reducing unnecessary traffic and allowing users to customize their own accounting data.

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



Note

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

Examples

The following example shows how to specify accept list “usage-only” for RADIUS accounting:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 1.1.1.1
accounting accept usage-only
```

```

!
radius-server host 1.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46

```

Related Commands

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

acl (ISAKMP)

To configure split tunneling, use the **acl** command in ISAKMP group configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

acl *number*

no acl *number*

Syntax Description	<i>number</i>	Specifies a group of access control lists (ACLs) that represent protected subnets for split tunneling purposes.
--------------------	---------------	---

Defaults Split tunneling is not enabled; all data is sent via the Virtual Private Network (VPN) tunnel.

Command Modes ISAKMP group configuration

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

Usage Guidelines Use the **acl** command to specify which groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

Examples The following example shows how to correctly apply split tunneling for the group name “cisco.” In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent via the VPN tunnel.

```
crypto isakmp client configuration group cisco
  key cisco
  dns 2.2.2.2 2.3.2.3
  pool dog
  acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands	Command	Description
	crypto isakmp client configuration group	Specifies which group’s policy profile will be defined.

address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command in `rsa-pubkey` configuration mode. To remove the IP address, use the **no** form of this command.

address *ip-address*

no address *ip-address*

Syntax Description

<i>ip-address</i>	IP address of the remote peer.
-------------------	--------------------------------

Defaults

No default behavior or values

Command Modes

Rsa-pubkey configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
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
crypto keyring	Defines a crypto keyring to be used during IKE authentication.
key-string	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

addressed-key

To specify which peer's RSA public key you will manually configure, use the **addressed-key** command in public key chain configuration mode.

addressed-key *key-address* [**encryption** | **signature**]

Syntax Description

<i>key-address</i>	Specifies the IP address of the remote peer's RSA keys.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special usage key.

Defaults

If neither the **encryption** nor **signature** keywords are used, general purpose keys will be specified.

Command Modes

Public key chain configuration. This command invokes public key configuration mode.

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command or the **named-key** command to specify which IP Security peer's RSA public key you will manually configure next.

Follow this command with the **key string** command to specify the key.

If the IPsec remote peer generated general-purpose RSA keys, do not use the **encryption** or **signature** keywords.

If the IPsec remote peer generated special-usage keys, you must manually specify both keys: use this command and the **key-string** command twice and use the **encryption** and **signature** keywords respectively.

Examples

The following example manually specifies the RSA public keys of two IPsec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key otherpeer.example.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 005C300D 06092A86 4886F70D 01010105
Router(config-pubkey)# 00034B00 30480241 00C5E23B 55D6AB22
Router(config-pubkey)# 04AEF1BA A54028A6 9ACC01C5 129D99E4
Router(config-pubkey)# 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
Router(config-pubkey)# BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
Router(config-pubkey)# D58AD221 B583D7A4 71020301 0001
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
```

```

Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption
Router(config-pubkey-key)# 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(config-pubkey-chain)# addressed-key 10.1.1.2 signature
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#

```

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you will manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

arap authentication

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

arap authentication { **default** | *list-name* } [**one-time**]

no arap authentication { **default** | *list-name* }



Caution

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

Syntax Description

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

Defaults

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

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The one-time keyword was added.

Usage Guidelines

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

Examples

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

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

■ arap authentication

Related Commands

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

attribute (server-group)

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

```
attribute value1 [value2 [value3]...]
```

```
no attribute value1 [value2 [value3]...]
```

Syntax Description

<i>value1</i> [<i>value2</i> [<i>value3</i>]...]	Attributes to include in an accept or reject list. The value can be a single integer, such as 7, or a range of numbers, such as 56–59. At least one attribute value must be specified.
---	--

Defaults

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

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.

Usage Guidelines

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

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

Required attributes are as follows:

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

**Note**

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

Examples

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

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

Related Commands

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

authentication (IKE policy)

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

authentication { **rsa-sig** | **rsa-encr** | **pre-share** }

no authentication

Syntax Description	Command	Description
	rsa-sig	Specifies RSA signatures as the authentication method.
	rsa-encr	Specifies RSA encrypted nonces as the authentication method.
	pre-share	Specifies preshared keys as the authentication method.

Defaults RSA signatures

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

```
crypto isakmp policy 15
 authentication pre-share
 exit
```

Related Commands	Command	Description
	crypto isakmp key	Configures a preshared authentication key.
	crypto isakmp policy	Defines an IKE policy.

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

authorization

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

```
authorization {arap | commands level | exec | reverse-access} [default | list-name]
```

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

Syntax Description

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

Defaults

Authorization is not enabled.

Command Modes

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

Examples

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

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

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

authorization (server-group)

To specify an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server, use the **authorization** command in server-group configuration mode.

authorization [**accept** | **reject**] *list-name*

Syntax Description

accept	(Optional) Indicates that the required attributes and the attributes specified in the <i>listname</i> will be accepted. All other attributes will be rejected.
reject	(Optional) Indicates that the attributes specified in the <i>list-name</i> will be rejected. All other attributes will be accepted.
<i>list-name</i>	Defines the given name for the accept or reject list.

Defaults

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

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.

Usage Guidelines

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

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



Note

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

Examples

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

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
  server 1.1.1.1
  authorization accept min-author
!
radius-server host 1.1.1.1 key mykey1
radius-server attribute list min-author
  attribute 6-7
```

Related Commands

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

authorization list

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

authorization list *list-name*

no authorization list *list-name*

Syntax Description

<i>list-name</i>	Name of the AAA authorization list.
------------------	-------------------------------------

Defaults

An authorization list is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

authorization username

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

authorization username *subject-name*

no authorization username *subject-name*

Syntax Description

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

Defaults

Parameters for the certificate fields are not specified.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

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

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

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

auto-enroll

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

auto-enroll [regenerate]

no auto-enroll [regenerate]

Syntax Description	regenerate	(Optional) A new key is generated for the certificate even if the named key already exists.
---------------------------	-------------------	---

Defaults	Autoenrollment is not enabled.
-----------------	--------------------------------

Command Modes	Ca-trustpoint configuration
----------------------	-----------------------------

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

Usage Guidelines	<p>Use the auto-enroll command to automatically request a router certificate from the certification authority (CA) that is using the parameters in the configuration. This command will generate a new RSA key only if a new key does not exist with the requested label.</p> <p>A trustpoint that is configured for autoenroll will attempt to reenroll when the router certificate expires. If the regenerate keyword is configured, a new key will be generated. Some CAs require a new key for reenrollment to work.</p>
-------------------------	--

Examples	<p>The following example shows how to configure the router to autoenroll with the CA “frog” on startup. In this example, regenerate is issued, so a new key will be generated for the certificate.</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 revokeme
  rsa-key frog 2048
```

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

auto secure

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

auto secure [**management** | **forwarding**] [**no-interact**]

Syntax Description	
management	(Optional) Only the management plane will be secured.
forwarding	(Optional) Only the forwarding plane will be secured.
no-interact	(Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter.

Defaults Autosecure is not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(1)	This command was introduced.

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



Caution

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

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



Caution

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

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

**Note**

Roll-back of the AutoSecure configuration is currently unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Examples

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

```
auto secure management
```

Related Commands

Command	Description
show auto secure config	Displays AutoSecure configurations.

ca trust-point

To identify the trustpoints that will be used to validate a certificate during Internet Key Exchange (IKE) authentication, use the **ca trust-point** command in ISAKMP profile configuration mode. To remove the trustpoint, use the **no** form of this command.

ca trust-point *trustpoint-name*

no ca trust-point *trustpoint-name*

Syntax Description

<i>trustpoint-name</i>	The trustpoint name as defined in the global configuration.
------------------------	---

Defaults

If there is no trustpoint defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

ISAKMP profile configuration

Command History

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

Usage Guidelines

The **ca trust-point** command can be used multiple times to define more than one trustpoint.

This command is useful when you want to restrict validation of certificates to a list of trustpoints. For example, the router global configuration has two trustpoints, A and B, which are trusted by VPN1 and VPN2, respectively. Each Virtual Private Network (VPN) wants to restrict validation only to its trustpoint.

Before you can use this command, you must enter the **crypto isakmp profile** command.



Note

A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate will be rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

Examples

The following example specifies two trustpoints, A and B. The ISAKMP profile configuration restricts each VPN to one trustpoint.

```
crypto ca trustpoint A
enrollment url http://kahului:80
crypto ca trustpoint B
enrollment url http://arjun:80
!
crypto isakmp profile vpn1
 trustpoint A
!
crypto isakmp profile vpn2
 ca trust-point B
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

cache clear age

To specify when, in minutes, cache entries expire and the cache is cleared, use the **cache clear age** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache clear age *minutes*

no cache clear age

Syntax Description

minutes Any value from 0 to 4294967295; the default value is 1440 minutes.

Defaults

1440 minutes (1 day)

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

After enabling the **aaa filterserver** command, which allows you to configure cache filter parameters, you can use the **cache clear age** command to specify when cache entries should expire. If this command is not specified, the default value (1440 minutes) will be enabled.

Examples

The following example shows how to configure the cache entries to expire every 60 minutes:

```
aaa filterserver
cache clear age 60
```

Related Commands

Command	Description
aaa filterserver	Enables filter cache configuration.

cache disable

To disable the cache, use the **cache disable** command in AAA filter configuration mode. To return to the default, use the **no** form of this command.

cache disable

no cache disable

Syntax Description This command has no arguments or keywords.

Defaults Caching is enabled.

Command Modes AAA filter configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines After enabling the **aaa filterserver** command, which allows you to configure cache filter parameters, you can use the **cache disable** command to disable filter caching. This command can be used to verify that the access control lists (ACLs) are being downloaded.

Examples The following example shows how to disable filter caching:

```
aaa filterserver
cache disable
```

Related Commands	Command	Description
	aaa filterserver	Enables filter cache configuration.

cache max

To limit the absolute number of entries that a cache can maintain for a particular server, use the **cache max** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache max *number*

no cache max

Syntax Description	<i>number</i>	Maximum number of entries the cache can maintain. Any value from 0 to 4294967295; the default value is 100 entries.
---------------------------	---------------	---

Defaults	100 entries
-----------------	-------------

Command Modes	AAA filter configuration
----------------------	--------------------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	After enabling the aaa filterserver command, which allows you to configure cache filter parameters, you can use the cache max command to specify the maximum number of entries the cache can have at any given time. If this command is not specified, the default value (100 entries) will be enabled.
-------------------------	---

Examples	The following example shows how to configure the cache to maintain a maximum of 150 entries:
-----------------	--

```
aaa filterserver
 password mycisco
 cache max 150
```

Related Commands	Command	Description
	aaa filterserver	Enables filter cache configuration.

cache refresh

To refresh a cache entry after a new session begins, use the **cache refresh** command in AAA filter configuration mode. To disable this functionality, use the **no** form of this command.

cache refresh

no cache refresh

Syntax Description This command has no arguments or keywords.

Defaults This command is enabled by default.

Command Modes AAA filter configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines The **cache refresh** command is used in an attempt to keep cache entries from the filter server, that are being referred to by new sessions, within the cache. This command resets the idle timer for these entries when they are referenced by new calls.

Examples The following example shows how to disable the **cache refresh** command:

```
aaa filterserver
password mycisco
no cache refresh
cache max 100
```

Related Commands	Command	Description
	aaa filterserver	Enables filter cache configuration.

call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** command in controller configuration mode. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

```
call guard-timer milliseconds [on-expiry {accept | reject}]
```

```
no call guard-timer milliseconds [on-expiry {accept | reject}]
```

Syntax Description		
<i>milliseconds</i>		Specifies the number of milliseconds to wait for a response from the RADIUS server.
on-expiry accept		(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
on-expiry reject		(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

Defaults No default behavior or values.

Command Modes Controller configuration

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

Examples The following example shows a guard timer that is set at 20000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
  call guard-timer 20000 on-expiry accept

aaa preauth
 group radius
  dnis required
```

Related Commands	Command	Description
	aaa preauth	Enters AAA preauthentication configuration mode.

certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

certificate *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number Serial number of the certificate to add or delete.

Defaults

No default behavior or values.

Command Modes

Certificate chain configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

You could use this command to manually specify a certificate. However, this command is rarely used in this manner. Instead, this command is usually used only to add or delete certificates.

Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used in this example to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

myrouter# configure terminal
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
```

Related Commands

Command	Description
crypto ca certificate chain	Enters the certificate chain configuration mode.

clear aaa cache filterserver acl

To clear the cache status for a particular filter or all filters, use the **clear aaa cache filterserver acl** command in EXEC mode.

```
clear aaa cache filterserver acl [filter-name]
```

Syntax Description	<i>filter-name</i> (Optional) Cache status of a specified filter is cleared.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	After you clear the cache status for a particular filter or all filters, it is recommended that you enable the show aaa cache filterserver command to verify that the cache status.
-------------------------	--

Examples	The following example shows how to clear the cache for all filters:
-----------------	---

```
clear aaa cache filterserver acl
```

Related Commands	Command	Description
	show aaa cache filterserver	Displays the cache status.

clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template** command in EXEC mode.

clear access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*]

Syntax Description

<i>access-list-number</i>	(Optional) Number of the dynamic access list from which the entry is to be deleted.
<i>name</i>	(Optional) Name of an IP access list from which the entry is to be deleted. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
<i>dynamic-name</i>	(Optional) Name of the dynamic access list from which the entry is to be deleted.
<i>source</i>	(Optional) Source address in a temporary access list entry to be deleted.
<i>destination</i>	(Optional) Destination address in a temporary access list entry to be deleted.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

Examples

The following example clears any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
clear access-template vendor 172.20.1.12
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-template	Places a temporary access list entry on a router to which you are connected manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

clear crypto engine accelerator counter

To reset the statistical and error counters of the hardware accelerator of the router to zero, use the **clear crypto engine accelerator counter** command in privileged EXEC mode.

clear crypto engine accelerator counter

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
	12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.

Examples The following example shows the statistical and error counters of the router being cleared to zero:

```
clear crypto engine accelerator counter
```

Related Commands	Command	Description
	crypto ca	Defines the parameters for the certification authority used for a session.
	crypto cisco	Defines the encryption algorithms and other parameters for a session.
	crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
	crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPsec encryption.
	crypto ipsec	Defines the IPsec security associations and transformation sets.
	crypto isakmp	Enables and defines the IKE protocol and its parameters.
	crypto key	Generates and exchanges keys for a cryptographic session.
	crypto map	Creates and modifies a crypto map for a session.
	debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.

Command	Description
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

clear crypto ipsec client ezvpn

To reset the Cisco Easy VPN Remote state machine and bring down the Cisco Easy VPN Remote connection on all interfaces or on a given interface (tunnel), use the **clear crypto ipsec client ezvpn** command in privileged EXEC mode.

```
clear crypto ipsec client ezvpn [name]
```

Syntax Description

<i>name</i>	(Optional) Identifies the IP Security (IPSec) Virtual Private Network (VPN) tunnel that is to be disconnected or cleared with a unique, arbitrary name. If a tunnel name is specified, only the specified tunnel is cleared; if no name is specified, then all existing tunnels are disconnected or cleared.
-------------	--

Defaults

If no tunnel name is specified, all active tunnels on the machine are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)YA	This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel to be cleared or disconnected for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **clear crypto ipsec client ezvpn** command resets the Cisco Easy VPN Remote state machine, bringing down the current Cisco Easy VPN Remote connection and bringing it back up on the interface. If you specify a tunnel name, only that tunnel is cleared. If no tunnel name is specified, all active tunnels on the machine are cleared.

If the Cisco Easy VPN Remote connection for a particular interface is configured for autoconnect, this command also initiates a new Cisco Easy VPN Remote connection.

Examples

The following example shows the Cisco Easy VPN Remote state machine being reset:

```
clear crypto ipsec client ezvpn
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates a Cisco Easy VPN Remote configuration.
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN Remote configuration to an interface.

clear crypto isakmp

To clear active Internet Key Exchange (IKE) connections, use the **clear crypto isakmp** command in EXEC mode .

clear crypto isakmp [*connection-id*]

Syntax Description

connection-id (Optional) Specifies which connection to clear. If this argument is not used, all existing connections will be cleared.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to clear active IKE connections.



Caution

If the *connection-id* argument is not used, all existing IKE connections will be cleared when this command is issued.

Examples

The following example clears an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
Router# show crypto isakmp sa

      dst          src          state          conn-id  slot
172.21.114.123 172.21.114.67  QM_IDLE        1         0
209.165.201.1 209.165.201.2  QM_IDLE        8         0

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# clear crypto isakmp 1
Router(config)# exit
Router# show crypto isakmp sa

      dst          src          state          conn-id  slot
209.165.201.1 209.165.201.2  QM_IDLE        8         0

Router#
```

Related Commands

Command	Description
show crypto isakmp sa	Displays all current IKE SAs at a peer.

clear crypto sa

To delete IP Security (IPSec) security associations (SAs), use the **clear crypto sa** command in EXEC mode.

```
clear crypto sa
```

Virtual Routing and Forwarding (VRF) Syntax

```
clear crypto sa peer [vrf fvr-f-name] address
```

```
clear crypto sa [vrf ivrf-name]
```

Crypto Map Syntax

```
clear crypto sa map map-name
```

IP Address, Security Protocol Standard, and SPI Syntax

```
clear crypto sa entry destination-address protocol spi
```

Traffic Counters Syntax

```
clear crypto sa counters
```

Syntax Description

peer [vrf <i>fvr-f-name</i>] <i>address</i>	Deletes any IPSec SAs for the specified peer. The <i>fvr-f-name</i> argument specifies the front door VRF (FVRF) of the peer address.
map <i>map-name</i>	Deletes any IPSec SAs for the named crypto map set. Specifies the name of a crypto map set.
entry <i>destination-address</i>	Deletes the IPSec SA with the specified address, protocol, and security parameter index (SPI). Specifies the IP address of the remote peer.
<i>protocol</i>	Specifies either the Encapsulation Security Protocol (ESP) or Authentication Header (AH).
<i>spi</i>	Specifies an SPI (found by displaying the SA database).
counters	Clears the traffic counters maintained for each SA; the counters keyword does not clear the SAs themselves.
vrf <i>ivrf-name</i>	Clears all IPSec SAs whose inside virtual routing and forwarding (IVRF) is the same as the <i>ivrf-name</i> .

Defaults

If the **peer**, **map**, **entry**, or **counters** keywords are not used, all IPSec SAs are deleted.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(15)T	The vrf keyword and <i>fvr</i> -name argument for clear crypto sa peer were added. The vrf keyword and <i>ivr</i> -name argument for clear crypto sa were added.

Usage Guidelines

This command clears (deletes) IPsec SAs.

If the SAs were established via Internet Key Exchange (IKE), they are deleted and future IPsec traffic will require new SAs to be negotiated. (When IKE is used, the IPsec SAs are established only when needed.)

If the SAs are manually established, the SAs are deleted and reinstalled. (When IKE is not used, the IPsec SAs are created as soon as the configuration is completed.)

If the **peer**, **map**, **entry**, or **counters** keywords are not used, all IPsec SAs will be deleted.

- The **peer** keyword deletes any IPsec SAs for the specified peer.
- The **map** keyword deletes any IPsec SAs for the named crypto map set.
- The **entry** keyword deletes the IPsec SA with the specified address, protocol, and SPI.

If any of the above commands cause a particular SA to be deleted, all the “sibling” SAs—that were established during the same IKE negotiation—are deleted as well.

The **counters** keyword simply clears the traffic counters maintained for each SA; it does not clear the SAs themselves.

If you make configuration changes that affect SAs, these changes will not apply to existing SAs but to negotiations for subsequent SAs. You can use the **clear crypto sa** command to restart all SAs so that they will use the most current configuration settings. In the case of manually established SAs, if you make changes that affect SAs you must use the **clear crypto sa** command before the changes take effect.

If the router is processing active IPsec traffic, it is suggested that you only clear the portion of the SA database that is affected by the changes, to avoid causing active IPsec traffic to temporarily fail.

Note that this command only clears IPsec SAs; to clear IKE state, use the **clear crypto isakmp** command.

Examples

The following example clears (and reinitializes if appropriate) all IPsec SAs at the router:

```
clear crypto sa
```

The following example clears (and reinitializes if appropriate) the inbound and outbound IPsec SAs established, along with the SA established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
clear crypto sa entry 10.0.0.1 AH 256
```

The following example clears all the SAs for VRF VPN1:

```
clear crypto sa vrf vpn1
```

Related Commands

Command	Description
clear crypto isakmp	Clears active IKE connections.

clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** command in EXEC mode.

clear ip audit configuration

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **clear ip audit configuration** EXEC command to disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources.

Examples The following example clears the existing IP audit configuration:

```
clear ip audit configuration
```

clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** command in EXEC mode.

clear ip audit statistics

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **clear ip audit statistics** EXEC command to reset statistics on packets analyzed and alarms sent.

Examples The following example clears all IP audit statistics:

```
clear ip audit statistics
```

clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

```
clear ip auth-proxy cache { * | host-ip-address }
```

Syntax Description		
*		Clears all authentication proxy entries, including user profiles and dynamic access lists.
<i>host-ip-address</i>		Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

Command Modes	
	EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	
	Use this command to clear entries from the translation table before they time out.

Examples The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

Related Commands	Command	Description
	show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

clear ip trigger-authentication

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

Examples The following example clears the remote host table:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host      Time Stamp
172.21.127.114   2940514234
Router# clear ip trigger-authentication
Router# show ip trigger-authentication
```

Related Commands	Command	Description
	show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

clear ip urlfilter cache

To clear the cache table, use the **clear ip urlfilter cache** command in EXEC mode.

```
clear ip urlfilter cache {ip-address | all}
```

Syntax Description		
	<i>ip-address</i>	Clears the cache table of a specified server IP address.
	all	Clears the cache table completely.

Command Modes EXEC

Command History	Release	Modification
	12.2(11)YU	This command was introduced.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines The cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address.

Examples The following example shows how to clear the cache table of IP address 172.18.139.21:

```
clear ip urlfilter cache 172.18.139.21
```

The following example shows how to clear the cache table of all IP addresses:

```
clear ip urlfilter cache all
```

Related Commands	Command	Description
	ip urlfilter cache	Configures cache parameters.
	show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

clear kerberos creds

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines Credentials are deleted when this command is issued.
Cisco supports Kerberos 5.

Examples The following example illustrates the **clear kerberos creds** command:

```
Router# show kerberos creds
Default Principal: chet@cisco.com
Valid Starting      Expires      Service Principal
18-Dec-1995 16:21:07  19-Dec-1995 00:22:24  krbtgt/CISCO.COM@CISCO.COM

Router# clear kerberos creds
Router# show kerberos creds
No Kerberos credentials.
```

Related Commands	Command	Description
	show kerberos creds	Displays the contents of your credentials cache.

clid

To preauthenticate calls on the basis of the Calling Line Identification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
aaa preauth
  group radius
  clid required
```

Related Commands

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

client authentication list

To configure Internet Key Exchange (IKE) extended authentication (Xauth) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list** command in ISAKMP profile configuration mode. To restore the default behavior, which is that Xauth is not enabled, use the **no** form of this command.

client authentication list *list-name*

no client authentication list *list-name*

Syntax Description

<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.
------------------	---

Defaults

No default behaviors or values

Command Modes

ISAKMP profile configuration

Command History

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

Usage Guidelines

Before configuring Xauth, you must set up an authentication list using AAA commands. Xauth can be enabled on a profile basis if it has been disabled globally.

Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
  client authentication list xauthlist
```

The following example shows that Xauth has been disabled globally and enabled for the profiles “vpn-login” and “isakmpauth”:

```
no crypto xauth FastEthernet0/0
!
crypto isakmp policy 1
  encr 3des
  group 2
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp client configuration group HRZ
```

```
crypto isakmp client configuration group vpngroup
  key cisco123
  pool vpnpool
crypto isakmp profile cert_sig
  match identity group HRZ
  isakmp authorization list isakmpauth
  client configuration address respond
  client configuration group HRZ
crypto isakmp profile nocerts
  match identity group vpngroup
  client authentication list vpn-login
  isakmp authorization list isakmpauth
  client configuration address respond
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address** command in ISAKMP profile configuration mode. To disable IKE configuraton mode, use the **no** form of this command.

client configuration address {initiate | respond}

no client configuration address {initiate | respond}

Syntax Description	initiate	Router will attempt to set IP addresses for each peer.
	respond	Router will accept requests for IP addresses from any requesting peer.

Defaults IKE configuration is not enabled.

Command Modes ISAKMP profile configuration

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

Usage Guidelines Before you can use this command, you must enter the **crypto isakmp profile** command.

Examples The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called "vpnprofile":

```
crypto isakmp profile vpnprofile
client configuration address initiate
client configuration address respond
```

Related Commands	Command	Description
	crypto isakmp profile	Defines an ISAKMP profile.

crl best-effort



Note

Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To download the certificate revocation list (CRL) but accept certificates if the CRL is not available, use the **crl best-effort** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, CRL checking is mandatory before your router can accept a certificate. That is, if CRL downloading is attempted and it fails, the certificate will be considered invalid and will be rejected.

Command Modes

Ca-identity configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	This command was replaced by the revocation-check command.

Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the appropriate CRL is in the router memory, the CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.)

When a CA system uses multiple CRLs, the certificate of the peer will indicate which CRL applies in its CDP extension and should be downloaded by your router.

If your router does not have the applicable CRL in memory and is unable to obtain one, your router will reject the certificate of the peer—unless you include the **crl best-effort** command in your configuration. When the **crl best-effort** command is configured, your router will try to obtain a CRL, but if it cannot obtain a CRL, it will treat the certificate of the peer as not revoked.

When your router receives additional certificates from peers, the router will continue to attempt to download the appropriate CRL if it was previously unsuccessful. The **crl best-effort** command specifies only that when the router cannot obtain the CRL, the router will not be forced to reject the certificate of a peer.

Examples

The following configuration example declares a CA and permits your router to accept certificates when CRLs are not obtainable:

```
crypto ca identity myid
enrollment url http://mycaserver
crl best-effort
```

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.

crl optional



Note

Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

crl optional

no crl optional

Syntax Description

This command has no arguments or keywords.

Defaults

The router must have and check the appropriate CRL before accepting the certificate of another IP Security peer.

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(2)T	This command was replaced by the revocation-check command.

Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.) To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.



Note

If the CRL already exists in the memory (for example, by using the **crypto ca crl request** command to manually download the CRL), the CRL will still be checked even if the **crl optional** command is configured.

Examples

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
crypto ca identity myca
  enrollment url http://ca_server
```

```
enrollment retry-period 20
enrollment retry-count 100
crl optional
```

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.

crl query

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 **crl query** 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.

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

```
no crl query ldap://hostname:[port]
```

Syntax Description

ldap://hostname	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).
:port	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

Defaults

Not enabled. If **crl query 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
12.1(1)T	This command was introduced.
12.2(8)T	This command replaced the query url 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
  crl query 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.

crypto ca authenticate

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *name*

Syntax Description

<i>name</i>	Specifies the name of the CA. This is the same name used when the CA was declared with the crypto ca identity command.
-------------	---

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However, the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the “RSA public key chain”).



Note

If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

```
error retrieving certificate :incomplete chain
```

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)# crypto ca authenticate myca  
Certificate has the following attributes:  
Fingerprint: 0123 4567 89AB CDEF 0123  
Do you accept this certificate? [yes/no] y#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto ca certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca certificate chain

To enter the certificate chain configuration mode, use the **crypto ca certificate chain** command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

crypto ca certificate chain *name*

Syntax Description	<i>name</i>
	Specifies the name of the CA. Use the same name as when you declared the CA using the crypto ca identity command.

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

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

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines	This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the certificate command.
------------------	--

Examples	The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.
----------	--

```
Router# show crypto ca certificates
```

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

```
Router# configure terminal
Rrouter(config)# crypto ca certificate chain myca
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
Router(config)#
```

Related Commands

Command	Description
certificate	Adds certificates manually.

crypto ca certificate map

To define certificate-based access control lists (ACLs), use the **crypto ca certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the **no** form of this command.

crypto ca certificate map *label sequence-number*

no crypto ca certificate map *label sequence-number*

Syntax Description

<i>label</i>	A user-specified label that is referenced within the crypto ca trustpoint command.
<i>sequence-number</i>	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

Defaults

No default behavior or value.

Command Modes

Ca-certificate-map configuration

Command History

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

Usage Guidelines

Issuing this command places the router in CA certificate map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

field-name match-criteria match-value

The *field-name* in the above example is one of the certificate fields. Field names are similar to the names used in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.509 standard. The **name** field is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name**, **subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name**—Case-insensitive string.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name**—Case-insensitive string.
- **name**—Case-insensitive string.
- **subject-name**—Case-insensitive string.
- **unstructured-subject-name**—Case-insensitive string.
- **valid-start**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

**Note**

The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* in the example is one of the following logical operators:

- **eq**—equal (valid for name and date fields)
- **ne**—not equal (valid for name and date fields)
- **co**—contains (valid only for name fields)
- **nc**—does not contain (valid only for name fields)
- **lt**—less than (valid only for date fields)
- **ge**—greater than or equal to (valid only for date fields)

The *match-value* is a case-insensitive string or a date.

Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco, and the sequence is 10.

```
crypto ca certificate map Cisco 10
  issuer-name co Cisco Systems
  unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto ca certificate map Group 10
  issuer-name co Cisco Systems
  subject-name co DIAL
crypto ca certificate map Group 20
  issuer-name co Cisco Systems
  subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Cisco Systems” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Cisco Systems” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Cisco Systems” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o =Cisco,” and so on.

Related Commands

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

crypto ca certificate query (ca-trustpoint)

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto ca certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the **no** form of this command.

crypto ca certificate query

no crypto ca certificate query

Syntax Description

This command has no arguments or keywords.

Defaults

CA trustpoints are stored locally in the router's NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)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 put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto ca certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.



Note

This command deprecates the **crypto ca certificate query** command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto ca trustpoint ka
.
.
.
crypto ca certificate query
```

■ **crypto ca certificate query (ca-trustpoint)****Related Commands**

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

crypto ca certificate query (global)

The **crypto ca certificate query** command in global configuration mode is replaced by the **crypto ca certificate query** command in ca-trustpoint configuration mode. See the **crypto ca certificate query** command for more information.

crypto ca crl request



Note

Effective with Cisco IOS Release 12.3(7)T, this command was replaced by the **crypto pki crl request** command.

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto ca crl request** command in global configuration mode.

crypto ca crl request *name*

Syntax Description

<i>name</i>	Specifies the name of the CA. This is the same name used when the CA was declared with the crypto pki trustpoint command.
-------------	--

Defaults

Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(7)T	This command was replaced by the crypto pki crl request command.

Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto ca crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.



Note

This command should be used only after the trustpoint is enrolled.

Examples

The following example immediately downloads the latest CRL to your router:

```
crypto ca crl request
```

crypto ca enroll

To obtain the certificate(s) of your router from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto ca enroll *name*

no crypto ca enroll *name*

Syntax Description

<i>name</i>	Specifies the name of the CA. Use the same name as when you declared the CA using the crypto ca identity command.
-------------	--

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto ca enroll** command is not saved in the router configuration.



Note

If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate(s), you must reissue the command.

Responding to Prompts

When you issue the **crypto ca enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

**Note**

This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPsec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password: <mypassword>
Re-enter password: <mypassword>

% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)# Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210

%CRYPTO-6-CERTRET: Certificate received from Certificate Authority

Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto ca certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca export pkcs12

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto ca export pkcs12** command in global configuration mode.

crypto ca export *trustpointname* **pkcs12** *destination url* *passphrase*

Syntax Description

<i>trustpointname</i>	Name of the trustpoint who issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name.
<i>destination url</i>	Location of the PKCS12 file to which a user wants to import the RSA key pair.
<i>passphrase</i>	Passphrase that is used to encrypt the PKCS12 file for export.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **crypto ca export pkcs12** command creates a PKCS 12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS#12 file, the RSA key pair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the passphrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto ca export mytp pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto ca import pkcs12	Imports RSA keys.

crypto ca identity

The **crypto ca identity** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca import pkcs12

To import Rivest, Shamir, and Adelman (RSA) keys, use the **crypto ca import pkcs12** command in global configuration mode.

```
crypto ca import trustpointname pkcs12 source url passphrase
```

Syntax Description

<i>trustpointname</i>	Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name.
<i>source url</i>	The location of the PKCS12 file to which a user wants to export the RSA key pair.
<i>passphrase</i>	Passphrase that must be entered to undo encryption when the RSA keys are imported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Usage Guidelines

When you enter the **crypto ca import pkcs12** command, a ke pair and a trustpoint are generated. If you then decide you want to remove the key pair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto ca trustpoint** command to remove the trustpoint.



Note

After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint “forward” is to be imported:

```
Router(config)# crypto ca import forward pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto ca export pkcs12	Exports RSA keys.
crypto ca trustpoint	Declares the CA that your router should use.
crypto key zeroize rsa	Deletes all RSA keys from your router.

crypto ca import

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto ca import** command in global configuration mode.

crypto ca import *name* **certificate**

Syntax Description	<i>name</i> certificate	Name of the certification authority (CA). This name is the same name used when the CA was declared with the crypto ca trustpoint command.
--------------------	--------------------------------	--

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Examples The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

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

Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.
	enrollment	Specifies the enrollment parameters of your CA.
	enrollment terminal	Specifies manual cut-and-paste certificate enrollment.

crypto ca trusted-root

The **crypto ca trusted-root** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca trustpoint



Note

Effective with Cisco IOS Release 12.3(7)T, the **crypto ca trustpoint** command is replaced with the **crypto pki trustpoint** command. See the **crypto pki trustpoint** command for more information.

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

Syntax Description

<i>name</i>	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)
-------------	--

Defaults

Your router does not recognize any CAs until you declare a CA using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The match certificate subcommand was introduced.
12.3(7)T	This command was replaced by the crypto pki trustpoint command. You can still enter the crypto ca trustpoint command, but the command will be written in the configuration as “crypto pki trustpoint.”

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto ca trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **match certificate**—Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.

- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

**Note**

Beginning with Cisco IOS Release 12.2(8)T, the **crypto ca trustpoint** command unified the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, the configuration mode and command will be written in the configuration as “crypto ca trustpoint.”

The following example shows how to declare the CA named “ka” and specify enrollment and CRL parameters:

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

The following example shows a certificate-based access control list (ACL) with the label “Group” defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca | pki trustpoint** command:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
!
crypto ca trustpoint pki
  match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.