reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time** command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

reauthentication time *seconds*

no reauthentication time *seconds*

Syntax Description

seconds	Number of seconds after which reauthentication occurs. Range is from 1 to 4294967295. Default is 0.

Defaults

0 seconds, which means group members are not required to reauthenticate.

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
Router(config-radsrv-group)# reauthentication time 30
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.

Command	Description
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect** command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url *url*

no redirect url *url*

Syntax Description

url	URL to which clients should be redirected.
url	Valid URL.

Defaults

No default behavior or values

Command Modes

Identity policy configuration (config-identity-policy)

Command History

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

Usage Guidelines

When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples

The following example shows the URL to which clients are redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.example.com
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

redundancy (GDOI)

To enable Group Domain of Interpretation (GDOI) redundancy configuration mode and to allow for key server redundancy, use the **redundancy** command in GDOI local server configuration mode. To disable GDOI redundancy, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Key server redundancy is not supported for a key server.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command must be configured before configuring related redundancy commands, such as for key server peers, local priority, and timer values. Use the **local priority** command to set the local key server priority. Use the **peer address ipv4** command to configure the peer address that belongs to the redundancy key server group.

Examples

The following example shows that key server redundancy has been configured:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.
peer address ipv4	Configures the peer key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

redundancy group

To configure the virtual IP address for the redundancy group, use the **redundancy group** command in interface configuration mode. To remove virtual IP address from the redundancy group, use the **no** form of this command.

redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

no redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

SyntaxDescription

id	Redundancy group ID.
ip *address*	Specifies the IP address of the interface.
exclusive	Specifies whether the interface is not shared with another redundancy group.
decrement *value*	(Optional) Amount decremented from the priority when the L1 state of the interface goes down. This overrides the default amount for the redundancy group. The range is from 1 to 255.

Command Default

Virtual IP address is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The virtual IP address and the physical address must in the same subnet.

Examples

The following example shows how to configure the virtual IP address for the redundancy group:

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# redundancy group 2 ip 10.2.3.4 exclusive
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.

Command	Description
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

redundancy inter-device

To enter inter-device configuration mode, use the **redundancy inter-device** command in global configuration mode. To exit inter-device configuration mode, use the **exit** command. To remove all inter-device configuration, use the no form of this command.

redundancy inter-device

no redundancy inter-device

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not enabled, you cannot configure stateful failover for IPSec.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **redundancy inter-device** command to enter inter-device configuration mode, which allows you to enable and protect Stateful Switchover (SSO) traffic.

Examples

The following example shows how to issue the **redundancy inter-device** command when enabling SSO:

```
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
!
```

The following example shows how to issue the **redundancy inter-device** command when configuring SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the redundant peer.
local-port	Defines the local SCTP that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.
scheme	Defines that redundancy scheme that is used between two devices.

redundancy rii

To configure the redundancy interface identifier (RII) for the redundancy group protected traffic interfaces, use the **redundancy rii** command in interface configuration mode. To remove the control interface from the redundancy group, use the **no** form of this command.

redundancy rii *id*

no redundancy rii *id*

SyntaxDescription

id	Redundancy interface identifier. The range is from 1 to 65535.

Command Default

RII is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Every interface associated with one or more redundancy groups must have a unique RII assigned to it. RII allows interfaces to have a one-to-one mapping between peers.

Examples

The following example shows how to configure the RII for the Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# redundancy rii 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
redundancy group	Configures the virtual IP address for a redundancy group.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancy stateful** command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**

no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Defaults

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

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

Usage Guidelines

The **redundancy stateful** command uses an existing IPSec profile (which is specified via the **crypto ipsec profile** command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description

This command has no arguments or keywords.

Defaults

Key rollover is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the certification authority (CA). When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”.

```
crypto ca trustpoint trustme2
 enrollment url http://trustme2.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
```

```
 regenerate
 password revokeme
 rsakeypair trustme2 2048
 exit
crypto ca authenticate trustme2
crypto ca enroll trustme2
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

regexp (profile map configuration)

To create an entry in a cache profile group that allows authentication and authorization matches based on a regular expression, use the **regexp** command in profile map configuration mode. To disable a regular expression entry, use the **no** form of this command.

regexp *matchexpression* {**any** | **only**} [**no-auth**]

no regexp *matchexpression* {**any** | **only**}

Syntax Description

matchexpression	String representing a regular expression on which to match.
any	Specifies that any unique instance of a AAA server response that matches the regular expression is saved in the cache.
only	Specifies that only one instance of a AAA server response that matches the regular expression is saved in the cache.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No regular expression entries are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to create an entry in a cache profile group that matches based on a regular expression, such as .*@example.com or .*@xyz.com.

Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.

Examples

The following example creates an entry in the cache profile group networkusers that authorizes network access to any example company user. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa cache profile networkusers
Router(config-profile-map)# regexp .*@example.com any no-auth
```

Related Commands

Command	Description
profile	Creates an individual authentication and authorization cache profile based on an exact username match.

registration interface

To specify the interface to be used for a Group Domain of Interpretation (GDOI) registration, use the **registration interface** command in GDOI local server configuration mode. To disable an interface, use the **no** form of this command.

registration interface *type slot/port*

no registration interface *type slot/port*

Syntax Description

type	Type of interface (see Table 60 below).
slot/port	Slot and port number of the interface.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Table 60 lists the types of interface that may be used for the *type* argument.

Table 60 Type of Interface

Interface	Description
Async	Async interface
BVI	Bridge-Group Virtual Interface
CDMA-1x	Code division multiple access 1x interface
CTunnel	CTunnel interface
Dialer	Dialer interface
Ethernet	Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink group interface
Null	Null interface
Serial	Serial
Tunnel	Tunnel interface

Table 60 Type of Interface (continued)

Interface	Description
Vif	Pragmatic General Multicast (PGM) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual Template interface
Virtual-TokenRing	Virtual TokenRing

Examples

The following example shows that the interface is Ethernet 0/0:

```
registration interface Ethernet 0/0
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey address ipv4

To specify the source or destination information of the rekey message, use the **rekey address ipv4** command in GDOI local server configuration mode. To remove a source or destination address, use the **no** form of this command.

rekey address ipv4 {*access-list-number* | *access-list-name*}

no rekey address ipv4 {*access-list-number* | *access-list-name*}

Syntax Description

access-list-number	IP access list number. The number can be from 100 through 199, or it can be in the expanded range of 2000 through 2699.
access-list-name	Access list name.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

The source is usually the key server interface from which the message leaves, and the destination is the multicast address on which the group members receive the rekeys (for example, access-list 101 permit 121 permit udp host 10.0.5.2 eq 848 host 192.168.1.2. eq 848).

Examples

The following example shows that the rekey address is access list “101”:

```
rekey address ipv4 101
```

The following example shows that a rekey message is to be sent to access control list (ACL) address 239.10.10.10:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
access-list 120 permit udp host 10.5.90.1 eq 848 host 239.10.10.10 eq 848
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey algorithm

To define the type of encryption algorithm used for a Group Domain of Interpretation (GDOI) group, use the **rekey algorithm** command in GDOI local server configuration mode. To disable an algorithm that was defined, use the **no** form of this command.

rekey algorithm {*type-of-encryption-algorithm*}

no rekey algorithm {*type-of-encryption-algorithm*}

Syntax Description

type-of-encryption-algorithm	Type of encryption algorithm used (see Table 61). The default algorithm is 3des-cbc. • The rekey algorithm is used to encrypt the rekey message that is sent from the key server to the multicast group.

Command Default

If this command is not configured, the default value of 3des-cbc takes effect. However, the default is used only if the commands required for a rekey to occur are specified (see the Note below in "Usage Guidelines").

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Table 61 lists the types of encryption algorithms that may be used.

Table 61 Types of Encryption

Encryption Type	Description
3des-cbc	Cipher Block Chaining mode of the Triple Data Encryption Standard (3des).
aes 128	128-bit Advanced Encrytion Standard (AES).
aes 192	192-bit AES.
aes 256	256-bit AES.
des-cbc	Cipher Block Chaining mode of the Data Encryption Standard (des).

Note At a minimum, the following commands are required for a rekey to occur:

rekey address ipv4 {*access-list-number* | *access-list-name*}

rekey authentication {**mypubkey** | **pubkey**} {*rsa key-name*}

If the **rekey algorithm** command is not configured, the default of 3des-cbc is used if the above minimum rekey configuration is met.

Examples

The following example shows that the 3des-cbc encryption standard is used:

```
rekey algorithm 3des-cbc
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
rekey address ipv4	Specifies the source or destination information of the rekey message.
rekey authentication	Specifies the keys to be used to a rekey to GDOI group members.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey authentication

To specify the keys to be used for a rekey to Group Domain of Interpretation (GDOI) group members, use the **rekey authentication** command in GDOI local server configuration mode. To disable the keys, use the **no** form of this command.

rekey authentication {**mypubkey** | **pubkey**} {**rsa** *key-name*}

no rekey authentication {**mypubkey** | **pubkey**} {**rsa** *key-name*}

Syntax Description

mypubkey	Keypair associated with this device.
pubkey	Public key associated with a different device.
rsa	Identifies an Rivest, Shamir, and Adelman (RSA) keypair.
key-name	Key to be used for rekey.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

For this command to work, Rivest, Shamir, and Adelman (RSA) keys must be generated first on the router using the following command:

crypto key generate rsa {**general keys**} [**label** *key-label*]

For example:

```
crypto key generate rsa general keys label group_1234_key_name
```

Examples

The following example shows that the keypair to be used for a rekey is RSA “group_1234_key_name”:

```
rekey authentication mypubkey rsa group_1234_key_name
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto key generate rsa	Generates RSA key pairs.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey lifetime

To limit the number of seconds for which any one encryption key should be used, use the **rekey lifetime** command in GDOI local server configuration mode. To disable the number of seconds that were set, use the **no** form of this command.

rekey lifetime {**seconds** *number-of-seconds*}

no rekey lifetime {**seconds** *number-of-seconds*}

Syntax Description

number-of-seconds	Lifetime in seconds. Value: 300 through 86400 seconds.

Command Default

If this command is not configured, the default value of 86400 seconds takes effect.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This **rekey** command is not used often. When this rekey limit is sent, a new key encryption key is sent to the group member so that the next rekey after this one will be encrypted with the new key encryption key.

Examples

The following example shows that the rekey lifetime has been set to 600 seconds:

```
rekey lifetime seconds 600
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey retransmit

To specify the number of times the rekey message is retransmitted, use the **rekey retransmit** command in GDOI local server configuration mode. To disable the number of times that were specified, use the **no** form of this command.

rekey retransmit {*number-of-seconds*} [**number** *number-of-retransmissions*]

no rekey retransmit {*number-of-seconds*} [**number** *number-of-retransmissions*]

Syntax Description

number-of-seconds	Number of seconds that the rekey message is retransmitted. Range: 10 through 60. Default=10.
number *number-of-retransmissions*	Number of times the message may be retransmitted. Range: 1 through 10. Default: 2.

Command Default

If this command is not configured, the number of seconds defaults to 10 and the number of transmissions defaults to 2.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command if you are concerned about network loss. Using this command ensures that the rekey message is resent the number of times specified in the retransmit command.

Examples

The following example shows that the rekey message may be retransmitted twice for 15 seconds each time:

```
rekey retransmit 15 number 2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey transport unicast

To configure unicast delivery of rekey messages to group members, use the **rekey transport unicast** command in global configuration mode. To remove unicast delivery of rekey messages and enable the default to multicast rekeying, use the **no** form of this command.

rekey transport unicast

no rekey transport unicast

Syntax Description

This command has no arguments or keywords.

Command Default

If **rekey transport unicast** is not specified or **no rekey transport unicast** is specified, multicast rekeying is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server under the **server local** command, along with other rekey configurations.

Examples

The following example shows that unicast delivery of rekey messages to group members has been configured:

```
crypto gdoi group diffint
 identity number 3333
 server local
  rekey lifetime seconds 300
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa mykeys
  rekey transport unicast
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 64
   address ipv4 10.0.5.2
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the **remark** command in access list configuration mode. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description

remark	Comment that describes the access-list entry, up to 100 characters long.

Defaults

The access-list entries have no remarks.

Command Modes

Standard named or extended named access list configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples

In the following example, the host1 subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.69.2.88 any eq telnet
```

Related Commands

Command	Description
access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

replay counter window-size

To turn on counter-based anti-replay protection for traffic defined inside an access list using Group Domain of Interpretation (GDOI) if there are only two group members in a group, use the **replay counter window-size** command in GDOI SA IPsec configuration mode. To disable counter-based anti-replay protection, use the **no** form of this command.

replay counter window-size [*number*]

no replay counter window-size

Syntax Description

number	Size of the Sychronous Anti-Replay (SAR) clock window expressed in bytes. Values are equal to 64, 128, 256, 512, and 1024 bytes. Default window size is 64 bytes.

Command Default

Counter-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server.

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size in bytes, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

Note GDOI anti-replay can be either counter based or time based. Use this command for counter-based anti-replay protection. For time-based anti-replay protection, use the **replay time window-size** command.

Examples

The following example shows that the anti-replay window size for unicast traffic has been set to 512:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
 sa ipsec 10
   profile group1111
   match address ipv4 101
   replay counter window-size 512
```

Related Commands

Command	Description
replay time window-size	Sets the the window size for anti-replay protection using GDOI if there are more than two group members in a group.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

replay time window-size

To set the window size for anti-replay protection using Group Domain of Interpretation (GDOI) if there are more than two group members in a group, use the **replay time window-size** command in GDOI SA IPsec configuration mode. To disable time-based anti-replay, use the **no** form of this command.

replay time window-size *seconds*

no replay time window-size

Syntax Description

seconds	Number of seconds of the interval duration of the Sychronous Anti-Replay (SAR) clock. The value range is 1 through 100. The default value is 100.

Command Default

Time-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server.

Note GDOI anti-replay can be either counter based or time based. This command turns on time-based anti-replay. For counter-based anti-replay protection, use the **replay counter window-size** command.

Examples

The following example shows that the number of seconds of the interval duration of the SAR clock has been set to 1:

```
sa ipsec 10
 profile group1111
 match address ipv4 101
 replay time window-size 1
```

Related Commands

Command	Description
replay counter window-size	Sets the window size for counter-based anti-replay protection for unicast traffic defined inside an access list.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

request-method

To permit or deny HTTP traffic according to either the request methods or the extension methods, use the **request-method** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

request-method {**rfc** *rfc-method* | **extension** *extension-method*} **action** {**reset** | **allow**} [**alarm**]

no request-method {**rfc** *rfc-method* | **extension** *extension-method*} **action** {**reset** | **allow**} [**alarm**]

Syntax Description

rfc	Specifies that the supported methods of RFC 2616, *Hypertext Transfer Protocol—HTTP/1.1*, are to be used for traffic inspection.
rfc-method	Any one of the following RFC 2616 methods can be specified: **connect**, **default, delete**, **get**, **head**, **options**, **post**, **put**, **trace**.
extension	Specifies that the extension methods are to be used for traffic inspection.
extension-method	Any one of the following extension methods can be specified: **copy**, **default, edit**, **getattribute**, **getproperties**, **index**, **lock**, **mkdir**, **move**, **revadd**, **revlabel**, **revlog**, **save**, **setattribute**, **startrev**, **stoprev**, **unedit, unlock**.
action	Methods and extension methods outside of the specified method are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If a given method is not specified, all methods and extension methods are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

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

Usage Guidelines

Only methods configured by the **request-method** command are allowed thorough the firewall; all other HTTP traffic is subjected to the specified action (**reset** or **allow**).

Examples

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

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

request-timeout

To set the number of seconds before an authentication request times out, use the **request-timeout** command in webvpn sso server configuration mode.

request-timeout *number-of-seconds*

no request-timeout *number-of-seconds*

Syntax Description

number-of-seconds	Number of seconds. Value = 10 through 30. Default = 15.

Command Default

None

Command Modes

Webvpn sso server configuration

Command History

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

Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

Examples

The following example shows that the number of seconds before an authentication request times out is 25:

```
webvpn context context1
 sso-server test-sso-server
  request-timeout 25
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

reset (policy-map)

To reset an SMTP connection with an SMTP sender (client) if it violates the specified policy, use the **reset** command in policy-map configuration mode. This action sends an error code to the sender and closes the connection gracefully.

reset

Command Default No default behavior or values.

Command Modes Policy-map configuration

Command History

12.4(20)T	This command was introduced in Cisco IOS Release 12.4(20)T.

Examples The following example displays the reset command configuration for DSP 1:

```
Router(config)# policy-map type inspect smtp p1
Router(config-pmap)# class type inspect smtp c1
Router(config-pmap)# reset
```

reset (zone-based policy)

To reset a TCP connection if the data length of the Simple Mail Transfer Protocol (SMTP) body exceeds the value that you configured in the **class-map type inspect smtp** command, use the **reset** command in policy-map configuration mode.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

The TCP connection is not reset.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

You can enter **reset** only for TCP traffic.

Examples

The following example creates a Layer 7 SMTP policy map named mysmtp-policy and applies the reset action to each of the match criteria:

```
policy-map type inspect smtp mysmtp-policy
 class-map type inspect smtp huge-mails
  reset
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

responder-only

To configure a device as responder-only, use the **responder-only** command in IPsec profile configuration mode. To remove the responder-only setting, use the no form of this command.

responder-only

no responder-only

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not configured as responder-only.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

This command is relevant only for a virtual interface scenario and is configurable only under an IPsec profile. Neither static nor crypto maps are supported.

Examples

The following example shows that the device has been configured as a responder-only:

```
crypto ipsec profile vti
 set transform-set 3dessha
 set isakmp-profile clients
 responder-only
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.

retired (IPS)

specify whether or not a retired signature or signature category definition should be saved in the router memory, use the **retired** command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

retired {**true** | **false**}

no retired

Syntax Description

true	Retires all signatures within a given category.
false	"Unretires" all signatures within a given category.

Command Default

Signature or signature category definitions are not saved in the system.

Command Modes

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

Command History

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

Usage Guidelines

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a "top-down" order, you should first retire all signatures, followed by "unretiring" specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

Examples

The following example shows how to retire all signatures and configure the Basic "ios_ips" category:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
enabled	Changes the enabled status of a given signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Enters the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature.

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

Effective with Cisco IOS Release 12.4(15)T

reverse-route [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]

no reverse-route [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]

Before Cisco IOS Release 12.4(15)T

reverse-route [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

no reverse-route [static | tag *tag-id* **[static] | remote-peer [static] | remote-peer** *ip-address* [**static**]]

Syntax Description

tag *tag-id*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. **Note** The **tag** keyword and *tag-id* argument were deleted effective with Cisco IOS Release 12.4(15)T.
remote-peer	(Optional) Indicates two routes: one for the tunnel endpoint, with the next hop being the interface to which the crypto map is bound. **Note** The **remote-peer** keyword and its variants (*ip-address* argument and **gateway** keyword) are applicable only to crypto maps.
ip-address	(Optional) If used without the optional **gateway** keyword, there is only one route: the protected subnet. The next hop is determined by the user-added value for the *ip-address* argument.
gateway	(Optional) Used with the *ip-address* argument. If the **gateway** keyword is used, there are two routes: one to the protected subnet by way of the remote-tunnel endpoint and the other to the remote-tunnel endpoint that is determined by the user-added value for the *ip-address* argument. **Note** The optional **gateway** keyword enables the behavior of the **reverse-route remote-peer** *ip-address* command syntax used for software releases before Cisco IOS Release 12.3(14)T.
static	(Optional) Creates routes on the basis of crypto ACLs, regardless of whether flows have been created for these ACLs.

Defaults

No default behavior or values.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The **remote-peer** keyword and *ip-address* argument were added.
12.3(14)T	The **static** and **tag** keywords and *tag-id* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The **tag** keyword and *tag-id* argument were deleted. The **gateway** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be applied on a per-crypto map basis.

Reverse route injection (RRI) provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IP Security (IPSec) Virtual Private Network (VPN) tunnel.

When enabled in an IPSec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPSec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

Examples

Before Cisco IOS Release 12.3(14)T

The following is an example in which RRI has been configured when crypto ACLs exist. The example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto ACL.

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Note In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword will be necessary, that is, **reverse-route static.**

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

- Remote Tunnel Endpoint

  ```
  ip route 10.1.1.1 255.255.255.255 192.168.1.1
  ```

- VPN Services Module (VPNSM)

  ```
  ip route 10.1.1.1 255.255.255.255 vlan0.1
  ```

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured.

```
reverse-route remote-peer
```

Configuring RRI with the Enhancements Added in Cisco IOS Release 12.3(14)T

The following configuration example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
   match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

The following example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The previous example yields the following before Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
table)
```

Effective with Cisco IOS Release 12.4(15)T

In the following example, routes are created from the destination information in the access control list (ACL). One route will list 10.2.2.2 as the next hop route to the ACL information, and one will indicate that to get to 10.2.2.2, the route will have to go by way of 10.1.1.1. All routes will have a metric of 10. Routes are created only at the time the map and specific ACL rule are created.

```
crypto map map1 1 ipsec-isakmp
 set peer 10.2.2.2
 reverse-route remote-peer 10.1.1.1 gateway
 set reverse-route distance 10
 match address 101
Configuring RRI with Route Tags 12.4(15)T or later: Example
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

revocation-check *method1* [*method2*[*method3*]]

no revocation-check *method1* [*method2*[*method3*]]

Syntax Description

method1 [*method2*[*method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

Defaults

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the **crl best-effort** and **crl optional** commands.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **revocation-check** command to specify at least one method that is to be used to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer's certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

Note The **none** keyword replaces the **optional** keyword that is available from the **crl** command. If you enter the **crl optional** command, it will be written back as the **revocation-check none** command. However, there is a difference between the **crl optional** command and the **revocation-check none** command. The **crl optional** command will perform revocation checks against any applicable in-memory CRL. If a CRL is not available, a CRL will not be downloaded and the certificate is treated as valid; the **revocation-check none** command ignores the revocation check completely and always treats the certificate as valid.

Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your router should use.
ocsp url	Enables an OCSP server.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

root tftp *server-hostname filename*

no root tftp *server-hostname filename*

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
server-hostname filename	Specifies a name for the server and a name for the file that will store the trustpoint CA.

Defaults

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

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

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

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
 root tftp xxx fff
 crl optional
```

Related Commands

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

root CEP

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

root PROXY

The **root PROXY** command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy** command for more information.

root TFTP

The **root TFTP** command is replaced by the **root** command. See the **root** command for more information.

rsakeypair

To specify which Rivest, Shamir, and Adelman (RSA) key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

rsakeypair *key-label* [*key-size* [*encryption-key-size*]]

Syntax Description

key-label	Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
key-size	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key pair. If the size is not specified, the existing key size is used.
encryption-key-size	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Defaults

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was added.

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair "exampleCAkeys":

```
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during Internet Key Exchange (IKE) authentication, use the **rsa-pubkey** command in keyring configuration mode. To remove the manual key that was defined, use the **no** form of this command.

rsa-pubkey {**address** *address* | **name** *fqdn*} [**encryption** | **signature**]

no rsa-pubkey {**address** *address* | **name** *fqdn*} [**encryption** | **signature**]

Syntax Description

address *address*	IP address of the remote peer.
name *fqdn*	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Defaults

No default behavior or values

Command Modes

Keyring configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

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