



Internet Key Exchange Security Protocol Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure the Internet Key Exchange (IKE) security protocol.

For detailed information about IKE concepts, configuration tasks, and examples, see the *Implementing Internet Key Exchange Security Protocol on Cisco IOS XR Software* configuration module.

acl

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 *acl-name*

no acl *acl-name*

Syntax Description	<i>acl-name</i> Specifies a group of access control list (ACL) rules that represent protected subnets for split tunneling purposes.
---------------------------	---

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

Command Modes ISAKMP group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 are sent through the VPN tunnel.

```
RP/0/RP0/CPU0:router(config)# crypto isakmp client configuration group cisco
RP/0/RP0/CPU0:router(isakmp-group)# key cisco
RP/0/RP0/CPU0:router(isakmp-group)# acl group1
```

!

```
RP/0/RP0/CPU0:router(config)# 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 policy profile is defined.

address

To specify the IP address for the Rivest, Shamir, and Adelman (RSA) public key of the remote peer you manually configure, use the **address** command in public key configuration mode. To remove the IP address of the remote peer, 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	Public key configuration								
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 2.0</td> <td>This command was introduced on the Cisco CRS-1.</td> </tr> <tr> <td>Release 3.0</td> <td>No modification.</td> </tr> <tr> <td>Release 3.2</td> <td>This command was supported on the Cisco XR 12000 Series Router.</td> </tr> </tbody> </table>	Release	Modification	Release 2.0	This command was introduced on the Cisco CRS-1.	Release 3.0	No modification.	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release	Modification								
Release 2.0	This command was introduced on the Cisco CRS-1.								
Release 3.0	No modification.								
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.								

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **address** command with the **named-key** command to specify the RSA public key for the IP Security (IPSec) peer you manually configure next. This command should be used only when the router has a single interface that processes IPSec.

Examples

The following example manually specifies the RSA public keys of an IPSec peer:

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# named-key otherpeer.example.com
RP/0/RP0/CPU0:router(config-pubkey-key)# address 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 00034B00 30480241 00C5E23B 55D6AB22
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string D58AD221 B583D7A4 71020301 0001
RP/0/RP0/CPU0:router(config-isakmp)# exit
```

■ address

Related Commands	Command	Description
	addressed-key	Specifies the RSA public key of the peer you manually configure.
	crypto key pubkey-chain rsa	Enters public key chain 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 the RSA public key for the peer you manually configure.
	show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

addressed-key

To specify the Rivest, Shamir, and Adelman (RSA) public key for the peer you manually configure, use the **addressed-key** command in public key chain configuration mode. To remove the encryption or signature public key pair of the remote peer, use the **no** form of this command.

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

no addressed-key *key-address* [**encryption** | **signature**]

Syntax Description

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

Defaults

If neither the **encryption** nor the **signature** keyword is used, general-purpose keys are specified.

Command Modes

Public key chain configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **addressed-key** command or the **named-key** command to specify the RSA public key you manually configure for the next IP Security (IPSec) peer.

Follow the **addressed-key** 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** keyword.

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

Examples

The following example shows how to manually specify the RSA public keys of two IPsec peers. The peer at 10.5.5.1 uses general-purpose keys.

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# addressed-key 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# address 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 00034B00 30480241 00C5E23B 55D6AB22
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string D58AD221 B583D7A4 71020301 0001
```

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 the RSA public key for the peer you manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange (IKE) policy, use the **authentication** command in ISAKMP policy configuration mode. To reset the authentication method to the default value, use the **no** form of this command.

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

no authentication { **pre-share** | **rsa-sig** | **rsa-encr** }

Syntax Description		
	pre-share	Specifies preshared keys as the authentication method.
	rsa-sig	Specifies RSA signatures as the authentication method.
	rsa-encr	Specifies Rivest, Shamir, and Adelman (RSA) encrypted nonces as the authentication method.

Defaults RSA signatures

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IKE policies define a set of parameters to be used during IKE negotiation. Use the **authentication** command to specify the authentication method to be used in an IKE policy. If you specify preshared keys, you must also separately configure these preshared keys.

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

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

Examples

The following example shows how to configure an IKE policy with preshared keys as the authentication method (and with all other parameters set to the defaults):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router (config-isakmp)# authentication pre-share
```

The following example shows how to configure an IKE policy with RSA encrypted keys as the authentication method (and with all other parameters set to the defaults):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router (config-isakmp)# authentication rsa-encr
```

The following example configures an IKE policy with RSA signatures as the authentication method (and with all other parameters set to the defaults):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router (config-isakmp)# authentication rsa-sig
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you manually configure.
addressed-key	Specifies the RSA public key of the peer you manually configure.
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy.
crypto key generate rsa	Generates RSA key pairs.
crypto key pubkey-chain rsa	Enters public key configuration mode to allow you to manually specify the RSA public keys of other devices.
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.
key-string (IKE)	Specifies the RSA public key of a remote peer.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
named-key	Specifies which peer RSA public key you manually configure.
show crypto isakmp policy	Displays the parameters for each IKE policy.

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	<i>connection-id</i>	(Optional) Name of connection to clear. If this argument is not used, all existing connections are cleared.
---------------------------	----------------------	---

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



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

■ clear crypto isakmp

Examples

The following example shows how to clear an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
RP/0/RP0/CPU0:router# show crypto isakmp sa

      dst          src          state          conn-id nodeid
172.21.114.123 172.21.114.67  QM_IDLE        1          0
172.0.0.2       172.0.0.1     QM_IDLE        8          0

RP/0/RP0/CPU0:router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

RP/0/RP0/CPU0:router# clear crypto isakmp 1
RP/0/RP0/CPU0:router# show crypto isakmp sa
      dst          src          state          conn-id nodeid
172.0.0.2       172.0.0.1     QM_IDLE        8          0
```

Related Commands

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

crypto isakmp chkpt-disabled

To disable Internet Key Exchange (IKE) checkpointing, use the **crypto isakmp chkpt-disabled** command in global configuration mode. To reenble checkpointing, use the **no** form of this command.

crypto isakmp chkpt-disabled

no crypto isakmp chkpt-disabled

Syntax Description This command has no arguments or keywords.

Defaults IKE checkpointing is enabled.

Command Modes Global configuration

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IKE checkpoints security associations in the local database. If an IKE process restarts, security associations are retrieved from the local database and need not be reestablished with remote peers.

Examples In the following example, IKE checkpointing is disabled:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp chkpt-disabled
```

crypto isakmp client configuration group

To include the configuration of a local group profile, use the **crypto isakmp client configuration group** command in global configuration mode.

crypto isakmp client configuration group *group-name*

Syntax Description	<i>group-name</i>	Text string that specifies the name of a group.
---------------------------	-------------------	---

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

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

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **key** command must be enabled if the client identifies itself with a preshared key.

The following commands are available in the IKE group policy configuration mode:

- **acl** *acl-name*. Configures split tunneling. The *acl-name* argument specifies a group of access control list (ACL) rules that represent protected subnets for split tunneling purposes.
- **key** *preshared-key*. Specifies the Internet Key Exchange (IKE) preshared key for group policy attribute definition. This command must be enabled if the client identifies itself with a preshared key.

Examples

The following example shows how to include the configuration of a local group profile with the group name marketing:

```
RP/0/RP0/CPU0:router (config)# crypto isakmp client configuration group marketing
```

Related Commands	Command	Description
	acl	Configures split tunneling.
	crypto ipsec profile	Configures the IPSec profile.
	crypto isakmp policy	Defines an IKE policy.
	key	Specifies the IKE preshared key for group policy attribute definition.

crypto isakmp enable

To globally enable Internet Key Exchange (IKE) at your peer router, use the **crypto isakmp enable** command in global configuration mode. To disable IKE at the peer, use the **no** form of this command.

crypto isakmp enable

no crypto isakmp enable

Syntax Description This command has no arguments or keywords.

Defaults IKE is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IKE need not be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

Examples The following example shows how to disable IKE at one peer:

```
RP/0/RP0/CPU0:router(config)# no crypto isakmp enable
```

crypto isakmp identity

To specify the identity used by the router when participating in the Internet Key Exchange (IKE) protocol, use the **crypto isakmp identity** command in global configuration mode. To reset the Internet Security Association Key Management Protocol (ISAKMP) identity to the default value (address), use the **no** form of this command.

crypto isakmp identity {address | hostname}

no crypto isakmp identity

Syntax Description

address	Sets the ISAKMP identity to the IP address of the interface that communicates to the remote peer during IKE negotiations.
hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Defaults

The IP address is used for the ISAKMP identity.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto isakmp identity** command to specify an ISAKMP identity either by IP address or by host name. As a general rule, you should set all identities for peers in the same way—either by IP address or by host name.

Set an ISAKMP identity whenever you specify preshared keys.

Use the **address** keyword when only one interface (and therefore only one IP address) is used by the peer for IKE negotiations, and the IP address is known.

Use the **hostname** keyword if more than one interface on the peer might be used for IKE negotiations, or if the IP address for the interface is unknown (such as with dynamically assigned IP addresses).

Examples

The following example shows how to use preshared keys at two peers and set both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified.

```
RP/0/RP0/CPU0:router(config)# crypto isakmp identity address
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring address 192.168.1.33
```

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified.

```
RP/0/RP0/CPU0:router(config)# crypto isakmp identity address
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring address 10.0.0.1
```

**Note**

In the preceding example, if the **crypto isakmp identity** command had not been performed, the ISAKMP identities would still have been set to the IP address, the default identity.

The following example shows how to use preshared keys at two peers and set both their ISAKMP identities to the host name.

At the local peer the ISAKMP identity is set and the preshared key is specified.

```
RP/0/RP0/CPU0:router(config)# crypto isakmp identity hostname
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring hostname
```

At the remote peer the ISAKMP identity is set and the same preshared key is specified.

```
RP/0/RP0/CPU0:router(config)# crypto isakmp identity hostname
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring hostname
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp key	Configures a preshared authentication key.

crypto isakmp keepalive

To use the Internet Key Exchange (IKE) security association (SA) feature for providing a mechanism for detecting loss of connectivity between two IP Security (IPSec) peers, use the **crypto isakmp keepalive** command in global configuration mode. To disable this feature, use the **no** form of this command.

crypto isakmp keepalive *seconds* *retry-seconds*

no crypto isakmp keepalive

Syntax Description	<i>seconds</i>	Number of seconds between keepalive messages. The range is from 10 to 3600.
	<i>retry-seconds</i>	Number of seconds between retries if keepalive fails. The range is from 2 to 60.

Defaults IKE does not send keepalive messages until specified by this command.

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	
Release 3.0		No modification.
Release 3.2		This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If IKE does not receive the keepalive acknowledge message from the peer after four tries, IKE concludes that it has lost connectivity with its peer.

Examples The following example shows how to set the number of seconds between keepalive messages to 20 seconds, and the number of seconds between retries to 20 seconds if keepalive fails:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp keepalive 20 20
```

Related Commands [crypto isakmp identity](#) Specifies the identity the router uses when participating in the IKE protocol.

crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key** command in global configuration mode. To delete a preshared authentication key, use the **no** form of this command.

```
crypto isakmp key keystring { address peer-address [subnet-address] | hostname peer-hostname }
```

```
no crypto isakmp key keystring { address peer-address | hostname peer-hostname }
```

Syntax Description		
<i>keystring</i>		Preshared key. Use any combination of alphanumeric characters up to 127 bytes. This preshared key must be identical at both peers.
address		Use this keyword if the remote peer Internet Security Association and Key Management Protocol (ISAKMP) identity was set with its IP address.
<i>peer-address</i>		IP address of the remote peer.
<i>subnet-address</i>		(Optional) Subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)
hostname		Use this keyword if the remote peer ISAKMP identity was set with its host name.
<i>peer-hostname</i>		Host name of the remote peer. This is the host name of the peer concatenated with its domain name (for example, myhost.domain.com).

Defaults There is no default preshared authentication key.

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must configure this key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy. You must enter the **crypto isakmp key** command at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers—otherwise the policy cannot be used (the policy is not submitted for matching by the IKE process). The **crypto isakmp key** command is the second task required to configure the preshared keys at the peers. (The first task is accomplished with the **crypto isakmp identity** command.)

Use the command form with the **address** keyword if the remote peer previously set its ISAKMP identity with its IP address.

With the **address** keyword, you can also use the *subnet-address* argument to indicate that the remote peer ISAKMP identity is established using the preshared key only. If the *subnet-address* argument is used, preshared keys are no longer restricted between two users.

**Note**

If you specify a *subnet-address* value, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

Use the **hostname** keyword if the remote peer previously set its ISAKMP identity with its host name.

With the **hostname** keyword, you might also need to map the host name of the remote peer to all IP addresses of the remote peer interfaces that could be used during the IKE negotiation. You need to map the host name to the IP address except when this mapping is already done in a Domain Name System or service (DNS) server.

Examples

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring address 172.16.0.2
255.255.255.254
```

The remote peer specifies the same preshared key and designates the local peer by its host name:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring hostname
LocalRouter.domain.com
```

Now, the preshared key must be specified at each peer.

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring address 172.21.230.33
255.255.255.255
```

In the following example, the remote peer specifies the same preshared key and designates the local peer by its host name:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp key sharedkeystring hostname
LocalRouter.example.com
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp identity	Defines the identity the router uses when participating in the IKE protocol.

crypto isakmp policy

To define an Internet Key Exchange (IKE) policy, use the **crypto isakmp policy** command in global configuration mode. To delete an IKE policy, use the **no** form of this command.

crypto isakmp policy *priority*

no crypto isakmp policy *priority*

Syntax Description	<i>priority</i>	Value that uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10000, with 1 being the highest priority and 10000 the lowest.
---------------------------	-----------------	---

Defaults	There is a default policy, which always has the lowest priority. The default policy contains default values for the encryption, hash, authentication, Diffie-Hellman group, and lifetime parameters. (The parameter defaults are listed in the “Usage Guidelines” section.) When you create an IKE policy, the default for a particular parameter is used if no value is specified.	
-----------------	---	--

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

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
-------------------------	--

Use the **crypto isakmp policy** command to specify the parameters to use during an IKE negotiation. (These parameters create the IKE security association [SA].)

This command enters ISAKMP policy configuration mode. The following commands are available in this mode to specify the parameters in the policy:

- **authentication** (IKE policy); default = Rivest, Shamir, and Adelman (RSA) signatures.
- **description** (IKE policy); creates a description of an IKE policy.
- **encryption** (IKE policy); default = 56-bit DES-CBC
 - **aes** Selecting this option means that encrypted IKE messages protected by this suite are encrypted using Advanced Encryption Standard (AES) with a 128-bit key.
 - **aes 192** Selecting this option means that encrypted IKE messages protected by this suite are encrypted using AES with a 192-bit key.
 - **aes 256** Selecting this option means that encrypted IKE messages protected by this suite are encrypted using AES with a 256-bit key.

- **group** (IKE policy); default = 768-bit Diffie-Hellman.
- **hash** (IKE policy); default = SHA-1.
- **lifetime** (IKE policy); default = 86,400 seconds (1 day).

If you do not specify one of these commands for a policy, the default value is used for that parameter.

To exit ISAKMP policy configuration mode, type **exit**.

You can configure multiple IKE policies on each peer participating in IP Security (IPSec). When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.

Examples

The following example shows how to configure two policies for the peer:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router(config-isakmp)# hash md5
RP/0/RP0/CPU0:router(config-isakmp)# authentication rsa-sig
RP/0/RP0/CPU0:router(config-isakmp)# group 2
RP/0/RP0/CPU0:router(config-isakmp)# lifetime 5000
RP/0/RP0/CPU0:router(config-isakmp)# exit

RP/0/RP0/CPU0:router(config)# crypto isakmp policy 20
RP/0/RP0/CPU0:router(config-isakmp)# authentication pre-share
RP/0/RP0/CPU0:router(config-isakmp)# lifetime 10000
RP/0/RP0/CPU0:router(config-isakmp)# exit
```

The configuration results in the following policies:

```
Protection suite priority 15
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Message Digest 5
  authentication method: Rivest-Shamir-Adelman Signature
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime: 5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman Group: #1 (768 bit)
  lifetime: 10000 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit
```

IKE policy 15 is the highest priority, and the default policy is the lowest priority.

Related Commands	Command	Description
	authentication (IKE policy)	Specifies the authentication method within an IKE policy.
	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.

crypto key pubkey-chain rsa

To enter public key chain configuration mode when you need to manually specify Rivest, Shamir, and Adelman (RSA) public keys for other IP Security (IPSec) peers, use the **crypto key pubkey-chain rsa** command in global configuration mode. To remove the RSA public key pair chain, use the **no** form of this command.

crypto key pubkey-chain rsa

no crypto key pubkey-chain rsa

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must specify the keys for the other peer when you configure RSA encrypted nonces as the authentication method in an Internet Key Exchange (IKE) policy at your peer router.

Examples

The following example shows how to specify the RSA public keys of two other IPsec peers. Each remote peer uses its IP address as its identity.

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# addressed-key 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 00034B00 30480241 00C5E23B 55D6AB22
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string D58AD221 B583D7A4 71020301 0001
RP/0/RP0/CPU0:router(config-pubkey-key)# exit
RP/0/RP0/CPU0:router(config-pubkey-chain)# addressed-key 10.1.1.2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 0738BC7A 2BC3E9F0 679B00FE 53987BCC
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 0738BC7A 2BC3E9F0 679B00FE 53987BCC
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 01030201 42DD06AF E228D24C 458AD228
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 58BB5DDD F4836401 2A2D7163 219F882E
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CE69D4 B583748A 241BED0F 6E7F2F16
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 0DE0986E DF02031F 4B0B0912 F68200C4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string C625C389 0BFF3321 A2598935 C1B1
RP/0/RP0/CPU0:router(config-pubkey-key)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you manually configure.
addressed-key	Specifies the RSA public key of the peer you manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

description (IKE policy)

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

description *string*

no description

Syntax Description	<i>string</i>	Character string describing the IKE policy.
---------------------------	---------------	---

Defaults	The default description is blank.
-----------------	-----------------------------------

Command Modes	ISAKMP policy configuration
----------------------	-----------------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	<p>To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.</p> <p>Use the description command inside the ISAKMP policy configuration submode to create a description for an IKE policy.</p>
-------------------------	--

Examples	The following example shows the creation of an IKE policy description:
-----------------	--

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router(config-isakmp)# description this is a sample IKE policy
```

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in ISAKMP policy configuration mode. To reset the encryption algorithm to the default value, use the **no** form of this command.

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

```
no encryption
```

Syntax Description

des	Specifies 56-bit DES-CBC as the encryption algorithm. This option is the default value.
3des	Specifies 168-bit Digital Encryption Standard (DES) as the encryption algorithm.
aes	Specifies 128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
aes 192	Specifies 192-bit AES as the encryption algorithm.
aes 256	Specifies 256-bit AES as the encryption algorithm.

Defaults

The 56-bit DES-CBC encryption algorithm (**des**).

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IKE policies define a set of parameters to be used during IKE negotiation. Use the **encryption** command to specify the encryption algorithm to be used in an IKE policy.

Examples

The following example shows how to configure an IKE policy with the 3DES encryption algorithm (and with all other parameters set to the defaults):

```
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router(config-isakmp)# encryption 3des
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
group (IKE policy)	Specifies the 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.

group (IKE policy)

To specify the Diffie-Hellman group identifier within an Internet Key Exchange (IKE) policy, use the **group** command in ISAKMP policy configuration mode. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

group { **1** | **2** | **5** }

no group

Syntax Description		
	1	Specifies the 768-bit Diffie-Hellman group. This option is the default.
	2	Specifies the 1024-bit Diffie-Hellman group.
	5	Specifies the 1536-bit Diffie-Hellman group.

Defaults 768-bit Diffie-Hellman (group 1)

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IKE policies define a set of parameters to be used during IKE negotiation. Use this command to specify the Diffie-Hellman group to be used in an IKE policy.

■ group (IKE policy)

Examples

The following example shows how to configure an IKE policy with the 1024-bit Diffie-Hellman group (all other parameters are set to the defaults):

```
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router(config-isakmp)# group 2
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm 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.

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange (IKE) policy, use the **hash** command in ISAKMP policy configuration mode. To reset the hash algorithm to the default SHA-1 hash algorithm, use the **no** form of this command.

hash {**sha** | **md5**}

no hash

Syntax Description	sha	md5
	Specifies SHA-1 (Hashed Message Authentication Code [HMAC]) as the hash algorithm. This option is the default.	Specifies Message Digest 5 (MD5) (HMAC variant) as the hash algorithm.

Defaults SHA-1 hash algorithm

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **hash** command to specify the hash algorithm to be used in an IKE policy. IKE policies define a set of parameters to be used during IKE negotiation.

Examples

The following example shows how to configure an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router(config-isakmp)# hash md5
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier 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.

key

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the **key** command in ISAKMP group configuration mode. To remove a preshared key, use the **no** form of this command.

key *preshared-key*

no key *preshared-key*

Syntax Description	<i>preshared-key</i> IKE preshared key for group policy attribute definition.
---------------------------	---

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

Command Modes	ISAKMP group configuration
----------------------	----------------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
-------------------------	--

Use the **key** command to specify the IKE preshared key when defining group policy information for mode configuration push. (It follows the **crypto isakmp client configuration group** command.) You *must* configure the **key** command if the client identifies itself to the router with a preshared key. (You need not enable this command if the client uses a certificate for identification.)

Examples	The following example shows how to specify the preshared key named cisco:
-----------------	---

```
RP/0/RP0/CPU0:router(config)# crypto isakmp client configuration group default
RP/0/RP0/CPU0:router(isakmp-group)# key cisco
RP/0/RP0/CPU0:router(isakmp-group)# acl group1
```

Related Commands	Command	Description
	crypto isakmp client configuration group	Specifies the group whose policy profile is defined.

key-string (IKE)

To manually specify the Rivest, Shamir, and Adelman (RSA) public key of a remote peer, use the **key-string** command in public key configuration mode.

key-string *key-string*

Syntax Description	<i>key-string</i> Public key for a remote peer. Enter the key in hexadecimal format.
---------------------------	--

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

Command Modes	Public key configuration
----------------------	--------------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **key-string** command to manually specify the RSA public key of an IP Security (IPSec) peer. Before using this command, you must identify the remote peer using either the **addressed-key** or **named-key** command.

To avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

On each line you enter a key, you must type *key-string* argument before the key. When you finish specifying the RSA key, you must return to global configuration mode by typing **exit** at the config-pubkey-key prompt.

Examples

The following example shows how to manually specify the RSA public keys of an IPSec peer:

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# named-key otherpeer.example.com
RP/0/RP0/CPU0:router(config-pubkey-key)# address 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 00034B00 30480241 00C5E23B 55D6AB22
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string D58AD221 B583D7A4 71020301 0001
RP/0/RP0/CPU0:router(config-pubkey-key)# exit
```

Related Commands	Command	Description
	addressed-key	Specifies the RSA public key of the peer you will manually configure.
	crypto key pubkey-chain rsa	Enters public key configuration mode to allow you to manually specify the RSA public keys of other devices.
	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.

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime** command in ISAKMP policy configuration mode. To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description	<i>seconds</i>	Length of time (in seconds) that each SA should exist before expiring. Use an integer from 60 to 86400 seconds.
---------------------------	----------------	---

Defaults	<i>seconds</i> : 86400 seconds (1 day)
-----------------	--

Command Modes	ISAKMP policy configuration
----------------------	-----------------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
-------------------------	--

Use the **lifetime** command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, it first agrees upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the lifetime of the SA expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when new IP Security (IPSec) SAs are set up.

To save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.



Note

When your local peer initiates an IKE negotiation between itself and a remote peer, if the lifetimes are not equal, an IKE policy with the shorter lifetime is selected.

Examples

The following example shows how to configure an IKE policy with an SA lifetime of 600 seconds (all other parameters are set to the defaults):

```
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15  
RP/0/RP0/CPU0:router(config-isakmp)# lifetime 600
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
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.
show crypto isakmp policy	Displays the parameters for each IKE policy.

named-key

To specify the Rivest, Shamir, and Adelman (RSA) public key for the peer you will manually configure, use the **named-key** command in public key chain configuration mode. To remove the encryption or signature public key pair of the remote peer, use the **no** form of this command.

named-key *key-name* [**encryption** | **signature**]

no named-key *key-name* [**encryption** | **signature**]

Syntax Description

<i>key-name</i>	RSA key name of the remote peer. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
encryption	(Optional) Indicates that the RSA public key is an encryption special-usage key.
signature	(Optional) Indicates that the RSA public key is a signature special-usage key.

Defaults

If neither the **encryption** nor the **signature** keyword is used, general-purpose keys are specified.

Command Modes

Public key chain configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **named-key** command or the **addressed-key** command to specify the RSA public key you manually configure for the next IP Security (IPSec) peer.

Follow the **named-key** command with the **key-string** command to specify the key.

If you use the **named-key** command, you also need to use the **address** command to specify the IP address of the peer.

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

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 shows how to manually specify 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.

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# named-key otherpeer.example.com

address 10.5.5.1
key-string 005C300D 06092A86 4886F70D 01010105
key-string 005C300D 06092A86 4886F70D 01010105
key-string 00034B00 30480241 00C5E23B 55D6AB22
key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
key-string D58AD221 B583D7A4 71020301 0001
exit
addressed-key 10.1.1.2 encryption
key-string 00302017 4A7D385B 1234EF29 335FC973
key-string 00302017 4A7D385B 1234EF29 335FC973
key-string 2DD50A37 C4F4B0FD 9DADE748 429618D5
key-string 18242BA3 2EDFBDD3 4296142A DDF7D3D8
key-string 08407685 2F2190A0 0B43F1BD 9A8A26DB
key-string 07953829 791FCDE9 A98420F0 6A82045B
key-string 90288A26 DBC64468 7789F76E EE21
exit
addressed-key 10.1.1.2 signature
key-string 0738BC7A 2BC3E9F0 679B00FE 098533AB
key-string 0738BC7A 2BC3E9F0 679B00FE 098533AB
key-string 01030201 42DD06AF E228D24C 458AD228
key-string 58BB5DDD F4836401 2A2D7163 219F882E
key-string 64CE69D4 B583748A 241BED0F 6E7F2F16
key-string 0DE0986E DF02031F 4B0B0912 F68200C4
key-string C625C389 0BFF3321 A2598935 C1B1
exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you manually configure.
addressed-key	Specifies the RSA public key of the peer you manually configure.
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.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

show crypto isakmp key

To display the Internet Security Association and Key Management Protocol (ISAKMP) preshared keys for a router, use the **show crypto isakmp key** command in EXEC mode.

show crypto isakmp key

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples The following example shows how to display the IP hostname and address preshared keys:

```
RP/0/RP0/CPU0:router# show crypto isakmp key

Hostname/Address      Preshared Key
10.1.1.1              abc
10.1.1.2              cde
10.1.1.3              123
```

[Table 6](#) describes the significant fields shown in the display.

Table 6 *show crypto isakmp key* Field Descriptions

Field	Description
Hostname/Address	IP hostname or address of the router.
Preshared Key	ISAKMP preshared key for the router.

show crypto isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in EXEC mode.

show crypto isakmp policy

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples The following sample output is from the **show crypto isakmp policy** command after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
RP/0/RP0/CPU0:router# show crypto isakmp policy

Protection suite priority 15
  encryption algorithm:DES - Data Encryption Standard (56 bit keys)
  hash algorithm:Message Digest 5
  authentication method:Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group:#2 (1024 bit)
  lifetime:5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm:DES - Data Encryption Standard (56 bit keys)
  hash algorithm:Secure Hash Standard
  authentication method:preshared Key
  Diffie-Hellman Group:#1 (768 bit)
  lifetime:10000 seconds, no volume limit
Default protection suite
  encryption algorithm:DES - Data Encryption Standard (56 bit keys)
  hash algorithm:Secure Hash Standard
  authentication method:Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group:#1 (768 bit)
  lifetime:86400 seconds, no volume limit
```

**Note**

Although the output shows “no volume limit” for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

Table 7 describes the significant fields shown in the display.

Table 7 *show crypto isakmp policy Field Descriptions*

Field	Description
encryption algorithm	Encryption algorithm within the IKE policy.
hash algorithm	Hash algorithm within the IKE policy.
authentication method	Authentication method used in the IKE policy.
Diffie-Hellman group	Diffie-Hellman group identifier in the IKE policy.
lifetime	Length of time (in seconds) the security association (SA) exists before expiring.

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
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 sa

To display all current Internet Key Exchange (IKE) security associations (SAs) at a peer, use the **show crypto isakmp sa** command in EXEC mode.

show crypto isakmp sa

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples The following sample output is from the **show crypto isakmp sa** command, after IKE negotiations have been successfully completed between two peers:

```
RP/0/RP0/CPU0:router# show crypto isakmp sa
```

```
dst                src                state              conn-id           nodeid
172.21.114.123    172.21.114.67     QM_IDLE           1                 0
172.16.0.2        172.16.0.1        QM_IDLE           8                 0
```

[Table 8](#) describes the significant fields shown in the display.

Table 8 *show crypto isakmp sa* Field Descriptions

Field	Description
dst	Destination IP address.
src	Source IP address.
conn-id	Connection ID.
nodeid	Node ID.

Table 9 shows the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it is most likely in its quiescent state (QM_IDLE). For long exchanges, some MM_XXX states may be observed.

Table 9 Mode States

State: Main Mode Exchange	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state makes the transition immediately to QM_IDLE, and a quick mode exchange begins.
AG_NO_STATE	The ISAKMP SA has been created but nothing else has happened yet. It is “larval” at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state makes the transition immediately to QM_IDLE, and a quick mode exchange begins.
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto key pubkey-chain rsa

To display the Rivest, Shamir, and Adelman (RSA) public keys stored on your router for the peer, use the **show crypto key pubkey-chain rsa** command in EXEC mode.

show crypto key pubkey-chain rsa [*name key-name* | *address key-address*]

Syntax Description	
name <i>key-name</i>	(Optional) Displays the name of a particular public key.
address <i>key-address</i>	(Optional) Displays the address of a particular public key.

Defaults All RSA public keys stored on your router is displayed.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use this command to display RSA public keys stored on your router. The display includes the RSA public keys for the peer that were manually configured at your router and keys received by your router through other means (such as by a certificate, if certification authority support is configured).

If a router reboots, any public key derived by certificates are lost because the router asks for certificates again, at which time the public key is derived again.

Use the **name** or **address** keyword to display details about a particular RSA public key stored on your router.

If no keyword is used, this command displays a list of all RSA public keys stored on your router.

Examples The following sample output is from the **show crypto key pubkey-chain rsa** command:

```
RP/0/RP0/CPU0:router# show crypto key pubkey-chain rsa
```

Codes: M - Manually Configured, C - Extracted from certificate

Code	Usage	IP-address	Name
M	Signature	10.0.0.1	myrouter.example.com
M	Encryption	10.0.0.1	myrouter.example.com
C	Signature	172.16.0.1	routerA.example.com
C	Encryption	172.16.0.1	routerA.example.com
C	General	192.168.10.3	routerB.domain1.com

The following example shows manually configured special-usage RSA public keys for the peer named somerouter. This example also shows three keys obtained from peer certificates: two special-usage keys for peer routerA and a general-purpose key for peer routerB.

Certificate support is used in the example; if certificate support were not in use, none of the peer keys would show “C” in the Code column, and would all need to be manually configured.

Table 10 describes the significant fields shown in the display.

Table 10 show crypto key pubkey-chain rsa Field Descriptions

Field	Description
Code	RSA public keys that were manually configured on your router (M) and keys received by your router through other means, such as by a certificate (C).
Usage	Type of RSA keys generated.
IP-address	IP address of the local or remote peer for which RSA keys are being configured.
Name	Name of the local or remote peer.

The following sample output is from the **show crypto key pubkey-chain rsa name somerouter.example.com** command:

```
RP/0/RP0/CPU0:router# show crypto key pubkey-chain rsa name somerouter.example.com
```

```
Key name: somerouter.example.com
Key address: 10.0.0.1
Usage: Signature Key
Source: Manual
Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

Key name: somerouter.example.com
Key address: 10.0.0.1
Usage: Encryption Key
Source: Manual
Data:
 00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```



Note

The Source field in the example indicates “Manual,” meaning that the keys were manually configured on the router, not received in the certificate from the peer.

The following sample output is from the **show crypto key pubkey-chain rsa address 192.168.10.3** command:

```
RP/0/RP0/CPU0:router# show crypto key pubkey-chain rsa address 192.168.10.3
```

```
Key name: routerB.example.com
```

```
Key address: 192.168.10.3
```

```
Usage: General Purpose Key
```

```
Source: Certificate
```

```
Data:
```

```
0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
```

```
58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
```

```
0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

The Source field in the example indicates “Certificate,” meaning that the keys were received by the router by way of the certificate from the other router.

■ show crypto key pubkey-chain rsa