



# Encrypted Preshared Key

---

The Encrypted Preshared Key feature allows you to securely store plain text passwords in type 6 (encrypted) format in NVRAM.

## Feature History for Encrypted Preshared Key

Release	Modification
12.3(2)T	This feature was introduced.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Restrictions for Encrypted Preshared Key, page 2](#)
- [Information About Encrypted Preshared Key, page 2](#)
- [How to Configure an Encrypted Preshared Key, page 3](#)
- [Configuration Examples for Encrypted Preshared Key, page 11](#)
- [Where to Go Next, page 13](#)
- [Additional References, page 13](#)
- [Command Reference, page 14](#)



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

## Restrictions for Encrypted Preshared Key

- Old ROM monitors (ROMMONs) and boot images cannot recognize the new type 6 passwords. Therefore, errors are expected if you boot from an old ROMMON.
- For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

## Information About Encrypted Preshared Key

Before Using the Encrypted Preshared Key feature, you should understand the following concepts:

- [Using the Encrypted Preshared Key Feature to Securely Store Passwords, page 2](#)
- [How to Configure an Encrypted Preshared Key, page 3](#)

## Using the Encrypted Preshared Key Feature to Securely Store Passwords

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

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

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

### Changing a Password

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

### Deleting a Password

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



#### Caution

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

## Unconfiguring Password Encryption

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

## Storing Passwords

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

## Configuring New or Unknown Passwords

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

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

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

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

## Enabling the Encrypted Preshared Key

The **password encryption aes** command is used to enable the encrypted password.

## How to Configure an Encrypted Preshared Key

This section contains the following procedures:

- [Configuring an Encrypted Preshared Key, page 4](#) (required)
- [Monitoring Encrypted Preshared Keys, page 5](#) (optional)
- [Configuring an ISAKMP Preshared Key, page 6](#) (optional)
- [Configuring an ISAKMP Preshared Key in ISAKMP Keyrings, page 7](#) (optional)
- [Configuring ISAKMP Aggressive Mode, page 8](#) (optional)
- [Configuring a Unity Server Group Policy, page 9](#) (optional)
- [Configuring an Easy VPN Client, page 10](#) (optional)

## Configuring an Encrypted Preshared Key

To configure an encrypted preshared key, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key config-key password-encryption** *[text]*
4. **password encryption aes**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>key config-key password-encryption</b> <i>[text]</i>  <b>Example:</b> Router (config)# key config-key password-encryption	Stores a type 6 encryption key in private NVRAM. <ul style="list-style-type: none"> <li>• If you want to key in interactively (using the enter key) and an encrypted key already exists, you will be prompted for the following: Old key, New key, and Confirm key.</li> <li>• If you want to key in interactively but an encryption key is not present, you will be prompted for the following: New key and Confirm key.</li> <li>• If you want to remove the password that is already encrypted, you will see the following prompt: “WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:”.</li> </ul>
Step 4	<b>password encryption aes</b>  <b>Example:</b> Router (config)# password-encryption aes	Enables the encrypted preshared key.

### Troubleshooting Tips

If you see the warning message “ciphertext >[for username bar>] is incompatible with the configured master key,” you have entered or cut and pasted cipher text that does not match the master key or there is no master key. (The cipher text will be accepted or saved.) The warning message will allow you to locate the broken configuration line or lines.

## Monitoring Encrypted Preshared Keys

To get logging output for encrypted preshared keys, perform the following steps.

1. **enable**
2. **password logging**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>password logging</b>  <b>Example:</b> Router# password logging	Provides a log of debugging output for a type 6 password operation.

### Examples

The following **password logging** debug output shows that a new master key has been configured and that the keys have been encrypted with the new master key:

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas

Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

### What To Do Next

You can perform any of the following procedures. Each procedure is independent of the others.

- [Configuring an ISAKMP Preshared Key, page 6](#)
- [Configuring an ISAKMP Preshared Key in ISAKMP Keyrings, page 7](#)
- [Configuring ISAKMP Aggressive Mode, page 8](#)
- [Configuring a Unity Server Group Policy, page 9](#)
- [Configuring an Easy VPN Client, page 10](#)

## Configuring an ISAKMP Preshared Key

To configure an ISAKMP preshared key, perform the following procedure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp key *keystring* address *peer-address***
4. **crypto isakmp key *keystring* hostname *hostname***

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto isakmp key <i>keystring</i> address <i>peer-address</i></b>  <b>Example:</b> Router (config)# crypto isakmp key cisco address 10.2.3.4	Configures a preshared authentication key. <ul style="list-style-type: none"> <li>• The <i>peer-address</i> argument specifies the IP address of the remote peer.</li> </ul>
Step 4	<b>crypto isakmp key <i>keystring</i> hostname <i>hostname</i></b>  <b>Example:</b> Router (config)# crypto isakmp key foo hostname foo.com	Configures a preshared authentication key. <ul style="list-style-type: none"> <li>• The <i>hostname</i> argument specifies the fully qualified domain name (FQDN) of the peer.</li> </ul>

### Example

The following sample output shows that an encrypted preshared key has been configured:

```
crypto isakmp key 6 _Hg[^^ECgLGGPF^RXTQfDDWQ][YAAB address 10.2.3.4
crypto isakmp key 6 `eR\eTRaKCUZPYQfDgXRwi_AAB hostname foo.com
```

## Configuring an ISAKMP Preshared Key in ISAKMP Keyrings

To configure an ISAKMP preshared key in ISAKMP keyrings, which are used in IPsec Virtual Route Forwarding (VRF) configurations, perform the following procedure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. **pre-shared-key address** *address* **key** *key*
5. **pre-shared-key hostname** *hostname* **key** *key*

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto keyring</b> <i>keyring-name</i>  <b>Example:</b> Router (config)# crypto keyring foo	Defines a crypto keyring to be used during Internet Key Exchange (IKE) authentication and enters keyring configuration mode.
Step 4	<b>pre-shared-key address</b> <i>address</i> <b>key</b> <i>key</i>  <b>Example:</b> Router (config-keyring)# pre-shared-key address 10.2.3.5 key cisco	Defines a preshared key to be used for IKE authentication. <ul style="list-style-type: none"> <li>• The <i>address</i> argument specifies the IP address of the remote peer.</li> </ul>
Step 5	<b>pre-shared-key hostname</b> <i>hostname</i> <b>key</b> <i>key</i>  <b>Example:</b> Router (config-keyring)# pre-shared-key hostname foo.com key cisco	Defines a preshared key to be used for IKE authentication. <ul style="list-style-type: none"> <li>• The <i>hostname</i> argument specifies the FQDN of the peer.</li> </ul>

### Example

The following **show-running-config** sample output shows that an encrypted preshared key in ISAKMP keyrings has been configured.

```
crypto keyring foo
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname foo.com key 6 aE_REHDCOfYCPf^RXTQfDJYVVNSAAB
```

## Configuring ISAKMP Aggressive Mode

To configure ISAKMP aggressive mode, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer ip-address** *ip-address*
4. **set aggressive-mode client-endpoint** *client-endpoint*
5. **set aggressive-mode password** *password*

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto isakmp peer ip-address</b> <i>ip-address</i>  <b>Example:</b> Router (config)# crypto isakmp peer ip-address 10.2.3.4	To enable an IP Security (IPSec) peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and to enter ISAKMP peer configuration mode.
Step 4	<b>set aggressive-mode client-endpoint</b> <i>client-endpoint</i>  <b>Example:</b> Router (config-isakmp-peer)# set aggressive-mode client-endpoint fqdn cisco.com	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
Step 5	<b>set aggressive-mode password</b> <i>password</i>  <b>Example:</b> Router (config-isakmp-peer)# set aggressive-mode password cisco	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

### Example

The following **show-running-config** sample output shows that an encrypted preshared key in ISAKMP aggressive mode has been configured.

```
crypto isakmp peer address 10.2.3.4
  set aggressive-mode password 6 ^aKPIQ_KJE_PPF^RXTQfDTIaLNeAAB
  set aggressive-mode client-endpoint fqdn cisco.com
```

## Configuring a Unity Server Group Policy

To configure a unity server group policy, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **pool** *name*
5. **domain** *name*
6. **key** *name*

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto isakmp client configuration group</b> <i>group-name</i>  <b>Example:</b> Router (config)# crypto isakmp client configuration group foo	Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode.
Step 4	<b>pool</b> <i>name</i>  <b>Example:</b> Router (config-isakmp-group)# pool foopool	Defines a local pool address.
Step 5	<b>domain</b> <i>name</i>  <b>Example:</b> Router (config-isakmp-group)# domain cisco.com	Specifies the Domain Name Service (DNS) domain to which a group belongs.
Step 6	<b>key</b> <i>name</i>  <b>Example:</b> Router (config-isakmp-group)# key cisco	Specifies the IKE preshared key for group policy attribute definition.

## Example

The following **show-running-config** sample output shows that an encrypted key has been configured for a unity server group policy:

```
crypto isakmp client configuration group foo
  key 6 cZZgDZPOE\^dDPF^RXTQfDTIaLNeAAB
  domain cisco.com
  pool foopool
```

## Configuring an Easy VPN Client

To configure an Easy VPN client, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn *name***
4. **peer *ipaddress***
5. **mode client**
6. **group *group-name* key *group-key***
7. **connect manual**

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto ipsec client ezvpn <i>name</i></b>  <b>Example:</b> Router (config)# crypto ipsec client ezvpn foo	Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.
Step 4	<b>peer <i>ipaddress</i></b>  <b>Example:</b> Router (config-isakmp-peer)# peer 10.2.3.4	Sets the peer IP address for the VPN connection.

	Command	Description
Step 5	<b>mode client</b>  <b>Example:</b> Router (config-isakmp-ezpvpy)# mode client	Automatically configures the router for Cisco Easy VPNclient mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations.
Step 6	<b>group group-name key group-key</b>  <b>Example:</b> Router (config-isakmp-ezvpn)# group foo key cisco	Specifies the group name and key value for the VPN connection.
Step 7	<b>connect manual</b>  <b>Example:</b> Router (config-isakmp-ezvpn)# connect manual	Specifies the manual setting for directing the Cisco Easy VPN remote client to wait for a command or application program interface (API) call before attempting to establish the Cisco Easy VPN remote connection.

## Example

The following **show-running-config** sample output shows that an Easy VPN client has been configured. The key has been encrypted.

```
crypto ipsec client ezvpn foo
connect manual
group foo key 6 gdMI`S^[GIcPF^RXTQfDFKEO\RAAB
mode client
peer 10.2.3.4
```

# Configuration Examples for Encrypted Preshared Key

This section provides the following configuration examples:

- [Encrypted Preshared Key: Example, page 11](#)
- [No Previous Key Present: Example, page 12](#)
- [Key Already Exists: Example, page 12](#)
- [Key Already Exists But the User Wants to Key In Interactively: Example, page 12](#)
- [No Key Present But the User Wants to Key In Interactively: Example, page 13](#)
- [Removal of the Password Encryption: Example, page 13](#)

## Encrypted Preshared Key: Example

The following is an example of a configuration for which a type 6 preshared key has been encrypted. It includes the prompts and messages that a user might see.

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show running-config | include crypto isakmp key
crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router (config)# password encryption aes
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

## No Previous Key Present: Example

In the following configuration example, no previous key is present:

```
Router (config)# key config-key password-encryption testkey 123
```

## Key Already Exists: Example

In the following configuration example, a key already exists:

```
Router (config)# key config-key password-encryption testkey123
Old key:
Router (config)#
```

## Key Already Exists But the User Wants to Key In Interactively: Example

In the following configuration example, the user wants to key in interactively, but a key already exists. The Old key, New key, and Confirm key prompts will show on your screen if you enter the **key config-key password-encryption** command and press the enter key to get into interactive mode.

```
Router (config)# key config-key password-encryption
Old key:
New key:
Confirm key:
```

## No Key Present But the User Wants to Key In Interactively: Example

In the following example, the user wants to key in interactively, but no key is present. The New key and Confirm key prompts will show on your screen if you are in interactive mode.

```
Router (config)# key config-key password-encryption
New key:
Confirm key:
```

## Removal of the Password Encryption: Example

In the following configuration example, the user wants to remove the encrypted password. The “WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:” prompt will show on your screen if you are in interactive mode.

```
Router (config)# no key config-key password-encryption

WARNING: All type 6 encrypted keys will become unusable. Continue with master key
deletion ? [yes/no]: y
```

## Where to Go Next

Configure any other preshared keys.

## Additional References

The following sections provide references related to Encrypted Preshared Key.

## Related Documents

Related Topic	Document Title
Configuring passwords	The section “ <a href="#">Part 4: IP Security and Encryption</a> ” of the <i>Cisco IOS Security Configuration Guide</i> <i>Cisco IOS Security Command Reference</i> , Release 12.3 T

## Standards

Standards	Title
This feature has no new or modified standards.	—

## MIBs

MIBs	MIBs Link
This feature has no new or modified MIBs.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
This feature has no new or modified RFCs.	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

### New Commands

- [key config-key password-encryption](#)
- [password encryption aes](#)
- [password logging](#)

### Modified Commands

- [crypto ipsec client ezvpn \(global\)](#)
- [crypto isakmp client configuration group](#)
- [crypto isakmp key](#)
- [pre-shared-key](#)
- [set aggressive-mode password](#)

# crypto ipsec client ezvpn (global)

To create a Cisco Easy VPN Remote configuration and enter the Cisco Easy VPN Remote configuration mode, use the **crypto ipsec client ezvpn** command in global configuration mode. To delete the Cisco Easy VPN Remote configuration, use the **no** form of this command.

**crypto ipsec client ezvpn** *name*

**no crypto ipsec client ezvpn** *name*



## Note

A separate **crypto ipsec client ezvpn** command exists in interface configuration mode that assigns a Cisco Easy VPN Remote configuration to the interface.

## Syntax Description

<i>name</i>	Identifies the Cisco Easy VPN Remote configuration with a unique, arbitrary name.
-------------	---

## Defaults

Newly created Cisco Easy VPN Remote configurations default to the **client** mode.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to manually establish and terminate an IP Security (IPSec) Virtual Private Network (VPN) tunnel on demand for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	This command was modified so that <b>show</b> output for the <b>group</b> subcommand will show that the preshared key is either encrypted or unencrypted.

**Usage Guidelines**

The **crypto ipsec client ezvpn** command creates a Cisco Easy VPN Remote configuration and then enters the Cisco Easy VPN Remote configuration mode, at which point you can enter the following subcommands:

- **connect [auto | manual]**—Manually establishes and terminates an IPsec VPN tunnel on demand.
  - **auto**—(Optional) The default setting. The IPsec VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface.
  - **manual**—(Optional) Specifies the manual setting to direct the Cisco Easy VPN Remote Client to wait for a command or application program interface (API) call before attempting to establish the Cisco Easy VPN Remote connection. When the tunnel times out or fails, subsequent connections have to wait for the command to reset to manual or for an API call.
- **default**—Sets the subcommand that follows to its default values.
- **exit**—Exits Cisco Easy VPN configuration mode and returns to global configuration mode.
- **group group-name key group-key**—Specifies the group name and key value for the VPN connection.

Output for the **group** command will show that the preshared key is either encrypted or unencrypted. Output for an unencrypted key would be as follows:

```
group ez key key123
```

Output for a type 6 encrypted key would be as follows:

```
group ez key 6 2GIS[FEoHPhROiBA/OgCi
```

- **local-address interface-name**—Informs the Cisco Easy VPN Client of the interface that is used to determine the public IP address. This interface is used to source the tunnel. The **local-address** subcommand applies only to the Cisco uBR905 and Cisco uBR925 cable access routers.
  - The value of the *interface-name* argument specifies the interface used for tunnel traffic.

After specifying the local address used to source tunnel traffic, the IP address can be obtained in two ways:

  - The **local-address** subcommand can be used with the **cable-modem dhcp-proxy {interface loopback number} command to obtain a public IP address and to automatically assign it to the loopback interface.**
  - The IP address can be manually assigned to the loopback interface.
- **mode {client | network-extension}**—Specifies the mode of operation of the VPN of the router:
  - **client**—(the default) Automatically configures the router for Cisco Easy VPN Client mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations. When the Cisco Easy VPN Remote configuration is assigned to an interface, the router automatically creates the NAT or PAT and access-list configuration needed for the VPN connection.
  - **network-extension**—Specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the address space of the enterprise network.
- **no**—Removes the command or sets it to its default values.
- **peer {ipaddress | hostname}**—Sets the peer IP address or host name for the VPN connection. A host name can be specified only when the router has a domain naming system (DNS) server available for hostname resolution.



**Note** The Cisco Easy VPN Remote feature attempts to resolve the host name when the **peer** command is given, not when the VPN tunnel is created. If the host name cannot be resolved at that time, the **peer** command is not accepted.

After configuring the Cisco Easy VPN Remote configuration, use the **exit** command to exit the Cisco Easy VPN Remote configuration mode and return to global configuration mode.



**Note** You cannot use the **no crypto ipsec client ezvpn** command to delete a Cisco Easy VPN Remote configuration that is assigned to an interface. You must remove that Cisco Easy VPN Remote configuration from the interface before you can delete the configuration.

### Examples

The following example shows a Cisco Easy VPN Remote configuration named telecommuter-client being created on a Cisco uBR905 or Cisco uBR925 cable access router and being assigned to cable interface 0:

```
Router# configure terminal
Router(config)# crypto ipsec client ezvpn telecommuter-client
Router(config-crypto-ezvpn)# group telecommute-group key secret-telecommute-key
Router(config-crypto-ezvpn)# peer telecommuter-server
Router(config-crypto-ezvpn)# mode client
Router(config-crypto-ezvpn)# exit
Router(config)# interface c0
Router(config-if)# crypto ezvpn telecommuter-client
Router(config-if)# exit
```



**Note** Specifying the **mode client** option as shown above is optional because this is the default configuration for these options.

The following example shows the Cisco Easy VPN Remote configuration named telecommuter-client being removed from the interface and then deleted:

```
Router# configure terminal
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

### Related Commands

Command	Description
<b>crypto ipsec client ezvpn (interface)</b>	Assigns a Cisco Easy VPN Remote configuration to an interface.

# crypto isakmp client configuration group

To specify to which group a policy profile will be defined, use the **crypto isakmp client configuration group** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

```
crypto isakmp client configuration group {group-name | default}
```

```
no crypto isakmp client configuration group {group-name | default}
```

## Syntax Description

<i>group-name</i>	Group definition that identifies which policy is enforced for users.
<b>default</b>	Policy that is enforced for all users who do not offer a group name that matches a <i>group-name</i> argument. The <b>default</b> keyword can only be configured locally.

## Defaults

No default behavior or values

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	The <b>access-restrict</b> , <b>firewall are-u-there</b> , <b>group-lock</b> , <b>include-local-lan</b> , and <b>save-password</b> commands were added. These commands are added during Mode Configuration. In addition, this command was modified so that output for this command will show that the preshared key is either encrypted or unencrypted.

## Usage Guidelines

Use the **crypto isakmp client configuration group** command to specify group policy information that needs to be defined or changed. You may wish to change the group policy on your router if you decide to connect to the client using a group ID that does not match the *group-name* argument.

After enabling this command, which puts you in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode, you can specify characteristics for the group policy using the following commands:

- **access-restrict**—Ties a particular Virtual Private Network (VPN) group to a specific interface for access to the Cisco IOS gateway and the services it protects.
- **acl**—Specifies a group of access control lists (ACLs) that represent protected subnetworks for split tunneling purposes.
- **dns**—Specifies the primary and secondary Domain Name Service (DNS) servers for the group.
- **domain**—Specifies group domain membership.
- **firewall are-u-there**—Adds the firewall are-u-there attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.

- **group-lock**—Use if preshared key authentication is used with Internet Key Exchange (IKE). Allows you to enter your extended authentication (Xauth) username. The group delimiter is compared against the group identifier sent during IKE aggressive mode.
- **include-local-lan**—Configures the include-local-lan attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
- **key**—Specifies the IKE preshared key when defining group policy information for Mode Configuration push.
- **pool**—Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **save-password**—Saves your extended authentication (Xauth) password locally on your PC.
- **set aggressive-mode client-endpoint**—Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.
- **wins**—Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

Output for the **crypto isakmp client configuration group** command (using the **key** subcommand) will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp client configuration group key test
```

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

```
crypto isakmp client configuration group
key 6 JK_JHZPeJV_XFZTKCQFYAAB
```

## Examples

The following example shows how to define group policy information for Mode Configuration push. In this example, the first group name is “cisco” and the second group name is “default.” Thus, the default policy will be enforced for all users who do not offer a group name that matches “cisco.”

```
crypto isakmp client configuration group cisco
key cisco
dns 2.2.2.2 2.2.2.3
wins 6.6.6.6
domain cisco.com
pool fred
acl 199
!
crypto isakmp client configuration group default
key cisco
dns 2.2.2.2 2.3.2.3
pool fred
acl 199
```

## Related Commands

Command	Description
<b>access-restrict</b>	Ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it protects.
<b>acl</b>	Configures split tunneling.
<b>dns</b>	Specifies the primary and secondary DNS servers.
<b>domain (isakmp-group)</b>	Specifies the DNS domain to which a group belongs.
<b>firewall are-u-there</b>	Adds the firewall are-u-there attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.

<b>Command</b>	<b>Description</b>
<b>group-lock</b>	Used if preshared key authentication is used with IKE.
<b>include-local-lan</b>	Configures the include-local-lan attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
<b>key (isakmp-group)</b>	Specifies the IKE preshared key for group policy attribute definition.
<b>pool (isakmp-group)</b>	Defines a local pool address.
<b>save-password</b>	Saves your Xauth password locally on your PC.
<b>set aggressive-mode client-endpoint</b>	Specifies the primary and secondary WINS servers.
<b>wins</b>	Specifies the primary and secondary WINS servers.

# 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 [mask] | hostname hostname} [no-xauth]
```

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

## Syntax Description

<i>keystring</i>	Specifies the preshared key. Use any combination of alphanumeric characters up to 128 bytes. This preshared key must be identical at both peers.
<b>address</b>	Use this keyword if the remote peer Internet Security Association Key Management Protocol (ISAKMP) identity was set with its IP address. The <i>peer-address</i> argument specifies the IP address of the remote peer.
<i>peer-address</i>	Specifies the IP address of the remote peer.
<i>mask</i>	(Optional) Specifies the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)
<b>hostname</b> <i>hostname</i>	Fully qualified domain name (FQDN) of the peer.
<b>no-xauth</b>	(Optional) Use this keyword if router-to-router IP Security (IPSec) is on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco-IOS IPSec. This keyword prevents the router from prompting the peer for extended authentication (Xauth) information (username and password).

## Defaults

There is no default preshared authentication key.

## Command Modes

Global configuration

## Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1)T	The <i>mask</i> argument was added.
12.2(4)T	The <b>no-xauth</b> keyword was added.
12.3(2)T	This command was modified so that output for this command will show that the preshared key is either encrypted or unencrypted.

## Usage Guidelines

You must use this command to configure a key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy; you must enable this 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 will not be 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 using the **crypto isakmp identity** command.)

Use the **address** keyword if the remote peer ISAKMP identity was set with its IP address.

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

**Note**

If you specify *mask*, 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.)

Preshared keys no longer work when the hostname keyword is sent as the identity; thus, the hostname keyword as the identity in preshared key authentication is no longer supported. According to the way preshared key authentication is designed in IKE main mode, the preshared keys *must* be based on the IP address of the peers. Although a user can still send the hostname as identity in preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address), the negotiation will fail.

If **crypto isakmp identity hostname** is configured as identity, the preshared key *must* be configured with the peer's IP address for the process to work.

Use the **no-xauth** keyword to prevent the router from prompting the peer for Xauth information (username and password). This keyword disables Xauth for static IPsec peers. The **no-xauth** keyword should be enabled when configuring the preshared key for router-to-router IPsec—not VPN-client-to-Cisco-IOS IPsec.

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

```
crypto isakmp key test123 address 10.1.0.1
```

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

```
crypto isakmp key 6 RHZE[JACMUI\bcbTdELISAAB address 10.1.0.1
```

**Examples**

In the following example, the remote peer “RemoteRouter” specifies an ISAKMP identity by address:

```
crypto isakmp identity address
```

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:

```
crypto isakmp key sharedkeystring address 172.21.230.33 255.255.255.255
```

**Related Commands**

Command	Description
<b>crypto ipsec security-association lifetime</b>	Specifies the authentication method within an IKE policy.
<b>crypto isakmp identity</b>	Defines the identity the router uses when participating in the IKE protocol.
<b>ip host</b>	Defines a static host name-to-address mapping in the host cache.

# key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encryption** command in global configuration mode. To disable the encryption, use the **no** form of this command.

**key config-key password-encryption** [*text*]

**no key config-key password-encryption** [*text*]

## Syntax Description

*text* (Optional) Password or master key.

**Note** It is recommended that you do not use the *text* argument but instead use interactive mode (using the enter key after you enter the **key config-key password-encryption** command) so that the preshared key will not be printed anywhere and therefore cannot be seen.

## Defaults

No type 6 password encryption

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

### Changing a Password

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

### Deleting a Password

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



#### Caution

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

### Unconfiguring Password Encryption

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

### Storing Passwords

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

### Configuring New or Unknown Passwords

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

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

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

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

### Examples

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

### Related Commands

Command	Description
<b>password encryption aes</b>	Enables a type 6 encrypted preshared key.
<b>password logging</b>	Provides a log of debugging output for a type 6 password operation.

# password encryption aes

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

**password encryption aes**

**no password encryption aes**

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

**Defaults** Preshared keys are not encrypted.

**Command Modes** Global configuration

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

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

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

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



**Note**

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

### Changing a Password

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

### Deleting a Password

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



#### Caution

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

### Unconfiguring Password Encryption

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

### Storing Passwords

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

### Configuring New or Unknown Passwords

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

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

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

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

### Examples

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

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

### Related Commands

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

# password logging

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

**password logging**

**no password logging**

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

**Defaults** Debug logging is not enabled.

**Command Modes** Privileged EXEC

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

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

```
Router# password logging
```

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

# pre-shared-key

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

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

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

## Syntax Description

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

## Defaults

No default behaviors or values

## Command Modes

Keyring configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

## Examples

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

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

## set aggressive-mode password

To specify the Tunnel-Password attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode password** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

```
set aggressive-mode password password
```

```
no set aggressive-mode password password
```

<b>Syntax Description</b>	<i>password</i>	Password that is used to authenticate the peer to a remote server. The tunnel password is used as the Internet Key Exchange (IKE) preshared key.
---------------------------	-----------------	--

<b>Defaults</b>	The Tunnel-Password attribute is not defined.
-----------------	---

<b>Command Modes</b>	ISAKMP policy configuration
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.
12.3(2)T	This command was modified so that output for this command will show that the preshared key is either encrypted or unencrypted.	

**Usage Guidelines** Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation, the **set aggressive-mode password** command, along with the **set aggressive-mode client-endpoint** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.

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

```
set aggressive-mode password test123
```

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

```
set aggressive-mode password 6 DV'P[aTVVWbcbgKU]T\T\QhZAAB
```

**Examples** The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
Router (config)# crypto isakmp peer address 10.4.4.1
Router (config-isakmp-peer)# set aggressive-mode client-endpoint user-fqdn user@cisco.com
Router (config-isakmp-peer)# set aggressive-mode password cisco123
```

Related Commands	Command	Description
	<b>crypto isakmp peer</b>	Enables an IPsec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
	<b>set aggressive-mode client-endpoint</b>	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

■ set aggressive-mode password