Encrypted Preshared Key

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

How to Configure an Encrypted Preshared Key

Configuring Preshared Keys

Note Preshared keys do not scale well with a growing network.

Restrictoins for Mask Preshared Keys

- The SA cannot be established between the IPsec peers until all IPsec peers are configured for the same preshared key.
- The mask preshared key must be distinctly different for remote users requiring varying levels of authorization. A new preshared key should be configured for each level of trust and correct keys must be assigned to the correct parties. Otherwise, an untrusted party may obtain access to protected data.

```
enable
configure terminal
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth
crypto isakmp key sharedkeystring address 10.0.0.1
end
```

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

```
enable
configure terminal
password logging
end
```

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
```

Configuring ISAKMP Preshared Key

```
enable
configure terminal
crypto isakmp key cisco address 10.2.3.4
crypto isakmp key mykey hostname mydomain.com
end
```

Configuring ISAKMP Preshared Key in ISAKMP Keyrings

```
enable
configure terminal
crypto keyring mykeyring
pre-shared-key address 10.2.3.5 key cisco
pre-shared-key hostname mydomain.com key cisco
end
```

Configuring ISAKMP Aggressive Mode

```
enable
configure terminal
isakmp peer ip-address 10.2.3.4
set aggressive-mode client-endpoint fqdn cisco.com
set aggressive-mode password cisco
end
```

Configuration Examples for Encrypted Preshared Key

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-encrypt testkey 123
```

Key Already Exists Example

In the following configuration example, a key already exists:

```
Router (config)# key config-key password-encrypt 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-encrypt** command and press the enter key to get into interactive mode.

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

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