The help topics in this section describe the Internet Key Exchange (IKE) configuration screens.

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is a standard method for arranging for secure, authenticated communications. IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across the network.

Cisco SDM lets you create IKE policies that will protect the identities of peers during authentication. Cisco SDM also lets you create pre-shared keys that peers exchange.

What Do You Want to Do?

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about IKE.</td>
<td>Click <strong>More About IKE</strong>.</td>
</tr>
<tr>
<td>Enable IKE.</td>
<td>Click <strong>Global Settings</strong>, and then click <strong>Edit</strong> to enable IKE and make other global settings for IKE.</td>
</tr>
<tr>
<td>You must enable IKE for VPN connections to use IKE negotiations.</td>
<td></td>
</tr>
</tbody>
</table>
Internet Key Exchange (IKE)

IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. This window shows the IKE policies configured on the router, and allows you to add, edit, or remove an IKE policy from the router’s configuration. If no IKE policies have been configured on the router, this window shows the default IKE policy.

After the two peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations apply to all subsequent IKE traffic during the negotiation.

The IKE policies in this list are available to all VPN connections.

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy.

If you want to: | Do this:
--- | ---
Create an IKE policy. | Click the IKE Policy node on the VPN tree. See IKE Policies for more information.
Create a pre-shared key. | Click the Pre-Shared Key node on the VPN tree. See IKE Pre-shared Keys for more information.
Create an IKE profile. | Click the IKE Profile node on the VPN tree. See IKE Profiles for more information.
Hash

The authentication algorithm for negotiation. There are two possible values:
- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.
- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

Type

Either SDM_DEFAULT or User Defined. SDM_DEFAULT policies cannot be edited.

What Do You Want to Do?

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about IKE policies.</td>
<td>See More About IKE Policies.</td>
</tr>
<tr>
<td>Add an IKE policy to the router’s configuration.</td>
<td>Click Add, and configure a new IKE policy in the Add IKE policy window.</td>
</tr>
<tr>
<td>Cisco SDM provides a default IKE policy, but there is no guarantee that the peer has the same policy. You should configure other IKE policies so that the router is able to offer an IKE policy that the peer can accept.</td>
<td>Choose the IKE policy that you want to edit, and click Edit. Then edit the IKE policy in the Edit IKE policy window. Default IKE policies are read only. They cannot be edited.</td>
</tr>
<tr>
<td>Edit an existing IKE policy.</td>
<td>Choose the IKE policy that you want to remove, and click Remove.</td>
</tr>
<tr>
<td>Remove an IKE policy from the router’s configuration.</td>
<td>Choose the IKE policy that you want to remove, and click Remove.</td>
</tr>
</tbody>
</table>
Add or Edit IKE Policy

Add or edit an IKE policy in this window.

**Note**
- Not all routers support all encryption types. Unsupported types will not appear in the screen.
- Not all IOS images support all the encryption types that Cisco SDM supports. Types unsupported by the IOS image will not appear in the screen.
- If hardware encryption is turned on, only those encryption types supported by both hardware encryption and the IOS image will appear in the screen.

**Priority**

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

**Encryption**

The type of encryption that should be used to communicate this IKE policy. Cisco SDM supports a variety of encryption types, listed in order of security. The more secure an encryption type, the more processing time it requires.

**Note**
If your router does not support an encryption type, the type will not appear in the list.

Cisco SDM supports the following types of encryption:
- Data Encryption Standard (DES)—This form of encryption supports 56-bit encryption.
- Triple Data Encryption Standard (3DES)—This is a stronger form of encryption than DES, supporting 168-bit encryption.
- AES-128—Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
• AES-192—Advanced Encryption Standard (AES) encryption with a 192-bit key.
• AES-256—Advanced Encryption Standard (AES) encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. There are two options:
• Secure Hash Algorithm (SHA)
• Message Digest 5 (MD5)

Authentication

The authentication method to be used.
• Pre-SHARE. Authentication will be performed using pre-shared keys.
• RSA_SIG. Authentication will be performed using digital signatures.

D-H Group

Diffie-Hellman (D-H) Group. Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. The options are as follows:
• group1—768-bit D-H Group. D-H Group 1.
• group2—1024-bit D-H Group. D-H Group 2. This group provides more security than group 1, but requires more processing time.
• group5—1536-bit D-H Group. D-H Group 5. This group provides more security than group 2, but requires more processing time.

Note

• If your router does not support group5, it will not appear in the list.
• Easy VPN servers do not support D-H Group 1.
Lifetime

This is the lifetime of the security association, in hours, minutes and seconds. The default is one day, or 24:00:00.

IKE Pre-shared Keys

This window allows you to view, add, edit, and remove IKE pre-shared keys in the router’s configuration. A pre-shared key is exchanged with a remote peer during IKE negotiation. Both peers must be configured with the same key.

Icon

If a pre-shared key is read-only, the read-only icon appears in this column. A pre-shared key will be marked as read-only if it is configured with the no-xauth CLI option

Peer IP/Name

An IP address or name of a peer with whom this key is shared. If an IP address is supplied, it can specify all peers in a network or subnetwork, or just an individual host. If a name is specified, then the key is shared by only the named peer.

Network Mask

The network mask specifies how much of the peer IP address is used for the network address and how much is used for the host address. A network mask of 255.255.255.255 indicates that the peer IP address is an address for a specific host. A network mask containing zeros in the least significant bytes indicates that the peer IP address is a network or subnet address. For example a network mask of 255.255.248.0 indicates that the first 22 bits of the address are used for the network address and that the last 10 bits are for the host part of the address.

Pre-Shared Key

The pre-shared key is not readable in Cisco SDM windows. If you need to examine the pre shared key, go to View->Running Config. This will display the running configuration. The key is contained in the crypto isakmp key command.
Chapter 16  Internet Key Exchange

Internet Key Exchange (IKE)

Add or Edit Pre Shared Key

Use this window to add or edit a pre-shared key.

**Key**

This is an alphanumeric string that will be exchanged with the remote peer. The same key must be configured on the remote peer. You should make this key difficult to guess. Question marks (?) and spaces must not be used in the pre-shared key.

**Reenter Key**

Enter the same string that you entered in the Key field, for confirmation.

**Peer**

Select **Hostname** if you want the key to apply to a specific host. Select **IP Address** if you want to specify a network or subnetwork, or if you want to enter the IP address of a specific host because there is no DNS server to translate host names to IP addresses.

**Hostname**

This field appears if you selected “Hostname” in the Peer field. Enter the peer’s host name. There must be a DNS server on the network capable of resolving the host name to an IP address.
Internet Key Exchange (IKE)

IP Address/Subnet Mask

These fields appear if you selected “IP Address” in the Peer field. Enter the IP address of a network or subnet in the IP Address field. The pre-shared key will apply to all peers in that network or subnet. For more information, refer to IP Addresses and Subnet Masks.

Enter a subnet mask if the IP address you entered is a subnet address, and not the address of a specific host.

User Authentication [Xauth]

Check this box if site-to-site VPN peers use XAuth to authenticate themselves. If Xauth authentication is enabled in VPN Global Settings, it is enabled for site-to-site peers as well as for Easy VPN connections.

IKE Profiles

IKE profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPSec tunnels. An IKE profile applies parameters to an incoming IPSec connection identified uniquely through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, fully qualified domain name (FQDN), and group (the virtual private network [VPN] remote client grouping).

For more information on ISAKMP profiles, and how they are configured using the Cisco IOS CLI, go to Cisco.com and follow this path:

Products and Services > Cisco IOS Software > Cisco IOS Security > Cisco IOS IPSec > Product Literature > White Papers > ISAKMP Profile Overview

IKE Profiles

The IKE Profiles area of the screen lists the configured IKE profiles and includes the profile name, the IPSec profile it is used by, and a description of the profile if one has been provided. If no IPSec profile uses the selected IKE profile, the value <none> appears in the Used By column.

When you create an IKE profile from this window, the profile is displayed in the list. IKE profiles created when you create
Details of IKE Profile

The details area of the screen lists the configuration values for the selected profile. You can use it to view details without clicking the Edit button and displaying an additional dialog. If you need to make changes, click Edit and make the changes you need in the displayed dialog. To learn more about the information shown in this area, click Add or Edit an IKE Profile.

Add or Edit an IKE Profile

Enter information and make settings in this dialog to create an IKE profile and associate it with a virtual tunnel interface.

IKE Profile Name

Enter a name for this IKE profile. If you are editing a profile, this field is enabled.

Virtual Tunnel Interface

Choose the virtual tunnel interface to which you want to associate this IKE profile from the Virtual Tunnel Interface list. If you need to create a virtual tunnel interface, click Add and create the interface in the displayed dialog.

Match Identity Type

The IKE profile includes match criteria that allow the router to identify the incoming and outgoing connections to which the IKE connection parameters are to apply. Match criteria can currently be applied to VPN groups. Group is automatically chosen in the Match Identity Type field.

Click Add to build a list of the groups that you want to be included in the match criteria.

Choose Add External Group Name to add the name of a group that is not configured on the router, and enter the name in the dialog displayed.

Choose Select From Local Groups to add the name of a group that is configured on the router. In the displayed dialog, check the box next to the group that you want to add. If all the local groups are used in other IKE profiles, SDM informs you that all groups have been selected.
Mode Configuration

Choose **Respond** in the Mode Configuration field if the router is to respond to mode configuration requests.

Choose **Initiate** if the router is to initiate mode configuration requests.

Choose **Both** if the router is to both initiate and respond to mode configuration requests.

Group Policy Lookup Authorization Policy

You must specify an authorization policy that controls access to group policy information on the AAA server. Choose **default** if you want to grant access to group policy lookup information. To specify a policy, choose an existing policy in the list, or click **Add** to create a policy in the displayed dialog.

User Authentication Policy

You can specify a user authentication policy to use for XAuth logins. Choose **default** if you want to allow XAuth logins. To specify a policy to control XAuth logins, choose an existing policy in the list, or click **Add** to create a policy in the displayed dialog.

Dead Peer Discovery

Click **Dead Peer Discovery** to enable the router to send dead peer detection (DPD) messages to peers. If a peer does not respond to DPD messages, the connection with it is dropped.

Specify the number of seconds between DPD messages in the Keepalive Interval field. The range is from 1 to 3600 seconds.

Specify the number of seconds between retries if DPD messages fail in the Retries field. The range is from 2 to 60 seconds.

Dead peer discovery helps manage connections without administrator intervention, but it generates packets that both peers must process in order to maintain the connection.

Description

You can add a description of the IKE profile that you are adding or editing.