Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Cisco Unified Operating System Administration for Cisco Unified Presence

Preparing Your Browser to Optimize Security

To download certificates from the server, you must ensure that your Internet Explorer security settings are configured correctly.

Procedure

1. Start Internet Explorer.
2. Select **Tools > Internet Options**.
3. Click the **Advanced** tab.
4. Scroll down to the Security section on the Advanced tab.
5. If necessary, clear **Do not save encrypted pages to disk**.
6. Click **OK**.

Related Topics

- Getting More Information

How to Manage IPSEC Policies

- Creating an IPSec Policy
- Enabling or Disabling an Existing IPSec Policy
- Deleting an IPSec Policy

Note: IPSec is not automatically established between nodes in a cluster during a Cisco Unified Presence installation.

Creating an IPSec Policy

You can set up a new IPSec policy. Do not, however, attempt to create IPSec policies during a Cisco Unified Presence server upgrade.

Caution! IPSec, especially with encryption, will affect the performance of your system.

Before You Begin

To access the Security menu items, you must log in again to Cisco Unified Operating System Administration using your Administrator password.

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > IPSEC Configuration**.
3. Click **Add New**.
4. Enter the new values in the appropriate fields.

Field	Description
Policy Group Name	Specifies the group name to which the IPSec policy belongs.
Policy Name	Specifies the name of the IPSec policy.
Association Name	Specifies the association name that is given to each IPSec association.
Authentication Method	Specifies the authentication method, for example, Certificate.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Method field.
Peer Type	Specifies whether the peer is the same type or different.

Certificate Name	Specifies the name of the certificate used for authentication.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Tunnel or Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: ◊ TCP ◊ UDP ◊ Any
Encryption Algorithm	From the list box, select the encryption algorithm. Choices include ◊ DES ◊ 3DES
Hash Algorithm	Specifies the hash algorithm: ◊ SHA1-Hash algorithm that is used in phase one IKE negotiation ◊ MD5-Hash algorithm that is used in phase one IKE negotiation
ESP Algorithm	From the list box, select the ESP algorithm. Choices include ◊ NULL_ENC ◊ DES ◊ 3DES ◊ BLOWFISH ◊ RIJNDAEL
Phase One Life Time	Specifies the lifetime for phase one IKE negotiation, in seconds.
Phase One DH	From the list box, select the phase one DH value. Choices include 2, 1, 5, 14, 16, 17, and 18.
Phase Two Life Time	Specifies the lifetime for phase two IKE negotiation, in seconds.
Phase Two DH	From the list box, select the phase two DH value. Choices include 2, 1, 5, 14, 16, 17, and 18.
Enable Policy	Check to enable the IPSec policy.

5. Click **Save**.

What To Do Next

Enabling or Disabling an Existing IPSec Policy

Enabling or Disabling an Existing IPSec Policy

You can enable or disable an existing IPSec policy. Do not, however, attempt to create, enable or disable IPSec policies during a Cisco Unified Presence server upgrade.

Caution! IPSec, especially with encryption, will affect the performance of your system.

Before You Begin

Complete the steps in Creating an IPSec Policy.

Procedure

1. Log in to Cisco Unified Operating System Administration. Perform one of the following actions in the IPSEC Policy Configuration frame:
2. Check **Enable Policy** to enable the policy.
3. Uncheck **Enable Policy** to disable the policy.
4. Click **Save**.

Deleting an IPSec Policy

You can delete one or more IPSec policies. Do not, however, attempt to delete IPSec policies during a Cisco Unified Presence server upgrade.

Caution! IPSec, especially with encryption, will affect the performance of your system.

Before You Begin

To access the Security menu items, you must log in again to Cisco Unified Operating System Administration using your Administrator password.

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > IPSEC Configuration**.
3. Select the policy or policies that you want to delete.
4. Click **Delete**.

Related Topics

- Getting More Information