



## Working with Groups and Sensors

---

Management Center for IPS Sensors (IPS MC) uses a hierarchy of groups and sensors. A group can contain sensors, other groups, or a combination of sensors and groups. When you start IPS MC, you always have at least one active, defined group—the Global group. The IPS MC hierarchy can contain many levels of groups and sensors in the same way that a folder in Windows 2000 can contain many levels of folders and files.

The IPS MC hierarchy of groups and sensors enables you to configure more than one sensor at a time because a sensor can acquire settings from its parent group. A sensor *must*, in fact, acquire settings from its parent group if a parent defines those settings as mandatory. A child cannot override the values for such settings.

This chapter explains how to add groups to your IPS MC hierarchy and to perform other tasks that include using the Progress Viewer (for status and confirmation of background tasks), viewing device statistics, and managing SSL certificates.

To add a sensor, use Cisco Security Manager. Adding a sensor to Cisco Security Manager automatically adds it to IPS MC. For more information, refer to "Adding Devices to the Security Manager Inventory" in the online help for Cisco Security Manager.



### Note

---

Adding a sensor to Cisco Security Manager *always* adds it to the Global group. After you add a sensor, you can move it from the Global group to another group. For more information see: [Defining Identification Properties for a 4.x Sensor, page 5-44](#); [Defining Identification Properties for a 5.X Sensor, page 5-60](#); or [Defining Identification Properties for an IOS IPS Device, page 5-128](#).

---

**Caution**

---

After adding a sensor to Cisco Security Manager, you cannot use it in IPS MC unless you re-import it on the Devices > Sensor page.

---

This chapter contains the following topics:

- [Re-Importing and Rebooting Sensors, page 4-2](#)
- [Using the Progress Viewer, page 4-11](#)
- [Viewing Device Statistics, page 4-11](#)
- [Managing SSL Certificates, page 4-13](#)

## Re-Importing and Rebooting Sensors

On the Devices > Sensor page, you can re-import or reboot a sensor.

To re-import a sensor, select it in the tree and then click **Re-Import**.

**Caution**

---

After adding a sensor to Cisco Security Manager, you cannot use it in IPS MC unless you re-import it on the Devices > Sensor page.

---

Device icons for 5.x sensors in the Object Selector indicate when you need to reboot. To reboot a sensor, select it in the tree and then click **Reboot**.

## Creating Sensor Subgroups

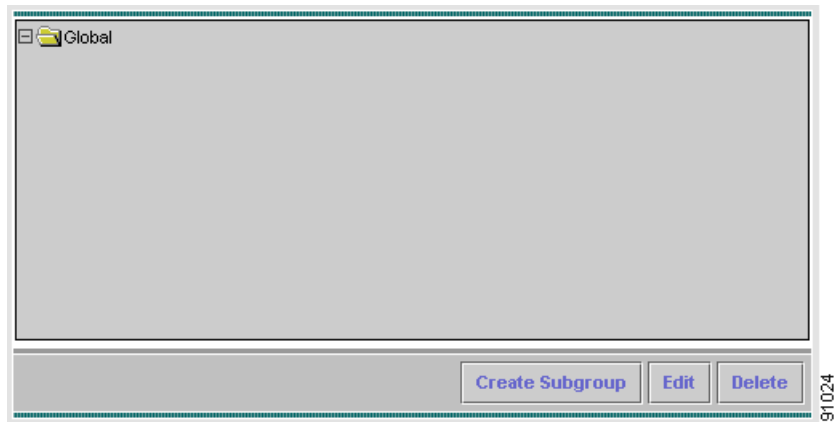
You can add a subgroup to any sensor group, including the Global group.

To create a sensor subgroup, follow these steps:

---

**Step 1** Select **Devices > Sensor Group**.

The Sensor Group page appears.



91024

**Step 2** In the tree, select the name of the sensor group that you want to add a subgroup to.

**Step 3** Click **Create Subgroup**.

The Add Group page appears.

 A screenshot of the 'Add Group' form. It includes fields for Group Name, Parent (Global), and Description. There are two radio buttons for Settings: 'Default (use parent values)' and 'Copy settings from group' (with a dropdown menu showing 'Global'). There are 'OK' and 'Cancel' buttons at the bottom.

78122

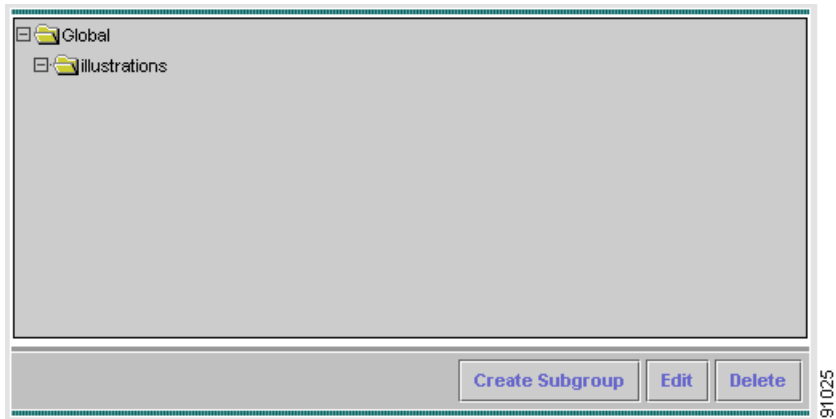
**Step 4** In the Group Name field, enter the name of the subgroup you want to add.

**Step 5** Do either step A or step B, below:

- a. Click the **Default (use parent values)** radio button.
- b. Click the **Copy settings from group** radio button and select the name of the group from the associated list box.

**Step 6** Click **OK**.

The Sensor Group page appears, showing the sensor subgroup that you just added.



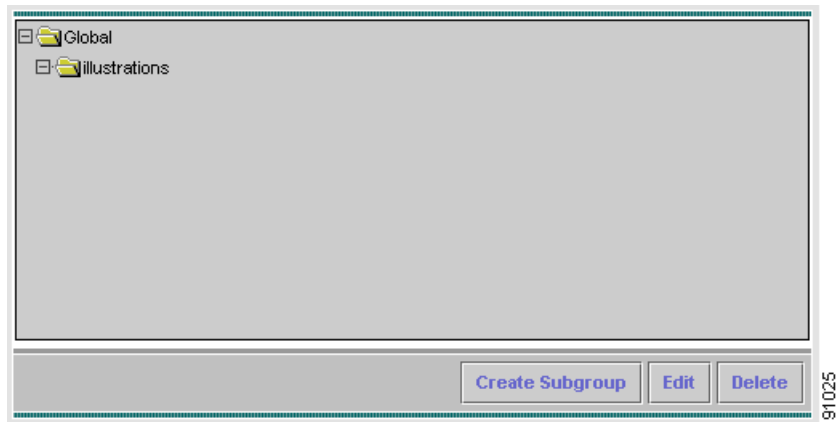
## Deleting Sensor Subgroups

You can delete any subgroup from any sensor group, including the Global group. The Global group is the only group you can not delete.

To delete a sensor group, follow these steps:

**Step 1** Select **Devices > Sensor Group**.

The Sensor Group page appears.



**Step 2** In the tree, select the group that you want to delete.



**Caution**

If you choose to delete a sensor group, IPS MC does not ask you to confirm your choice.

**Step 3** Click **Delete**.

The Sensor Group page appears again and the group you just deleted does not appear under its parent group.

## Learn More About the Secure Shell Protocol

*The Secure Shell (SSH)* is a protocol for secure remote login and other secure network services over an insecure network. For more information about SSH, see [Cisco.com](http://Cisco.com).



**Note**

IPS MC makes SSH available because of the importance transmitting login information (including passwords) in an encrypted form.

More information about using public keys for SSH authentication when using PuTTY (which is used with IPS MC for Windows 2000 and 2003) is available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>.

## Using SSH in IPS MC

IPS MC supports SSH for secure remote login to an IOS IPS device. IPS MC does not manage SSH keys, however. The IOS IPS device software provides the SSH server, and IPS MC provides support for an SSH Windows client—PuTTY—.

Versions 2.0 and later of IPS MC for Windows 2000 and 2003 use PuTTY 0.55.



### Note

When using IPS MC (any version), you should not install PuTTY (Windows 2000 and 2003), because the IPS MC installation program handles their installation for you.

Directions for using SSH keys with PuTTY are available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>.

PuTTY's Pageant utility is an SSH authentication agent. We recommend using Pageant to manage your keys in IPS MC for Windows 2000 and 2003. More information on Pageant is available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>.

Appliances running IDS software have a `/usr/nr/.ssh` directory. When using an appliance (not an IDSM), you must create the `authorized_keys` file (if it does not already exist) and then place that `authorized_keys` file in the `/usr/nr/.ssh` directory. Finally, you must place your public key in the `~/.ssh/authorized_keys` file.

To use SSH keys in IPS MC, follow these steps:

- Step 1** To use SSH keys in IPS MC for Windows 2000 and 2003, follow these steps:
- a. Use PuttyGen to generate your keys. Instructions are available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>.
  - b. When using a 4.x or 5.x device of any kind, go to its command-line interface, and then verify that you are in the conf mode. On the command line, enter the *ssh authorized-key* command with the public key, as shown in the following example:

```
ssh authorized-key foo 1024 37
1596368250624423681854398922811045907684812910415253843029783
7678 [in the config mode]
```

Use care with text editors and clipboards, especially when working with line breaks and white space. In the example shown above, *ssh authorized-key* is the command; *foo* is an optional keyword; *1024* is the number of bits in the key; *37* is the exponent of the key; and the very large integer is the modulus of the key. The descriptive comment that is an optional part of an authorized keys file can have a format such as *RSA-KEY-2004-03-11*. do not include the descriptive comment must not be included in this step.

- c. Save the private key to a disk file. "This file is the one you will need to tell PuTTY to use for authentication . . . or tell Pageant to load. . . ," according to the PuTTY documentation. We recommend the name `sensorname.key` for the private key, and we use it in this example.

**Caution**

---

Guard your private key carefully because of its importance to the security of your network, and back it up to a secure location.

---

- d. Create a session for the IOS IPS device and perform the following steps:
    1. At a command line prompt, enter *putty*.
    2. Enter the hostname or its IP address. (If the Host Name field is not already visible, select **Session** in the Category pane of the PuTTY Configuration window.)
    3. Under Protocol, click **SSH**. (If the SSH button is not already visible, select **Session** in the Category pane of the PuTTY Configuration window.)
    4. Select **Connection > SSH > Auth**.
    5. Enter, or browse to, the private key file for authentication: *sensorname.key*.
    6. Click **Open**.
    7. Select **Session**.
    8. Select **Load**.
    9. Select **Save**.
    10. Click **Connection**.
-

## Learn More About SSH Fingerprints

SSH fingerprints are described in the following material, which is quoted verbatim from the *PuTTY User Manual* (<http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>). PuTTY is copyright 1997-2001 Simon Tatham.

"If you are using SSH to connect to a server for the first time, you will probably see a message [similar to the following]:

```
"The server's host key is not cached in the registry. You have no
guarantee that the server is the computer you think it is.
```

```
"The server's key fingerprint is: ssh-rsa 1024
7b:e5:6f:a7:f4:f9:81:62:5c:e3:1f:bf:8b:57:6c:5a
```

```
"If you trust this host, hit Yes to add the key to PuTTY's cache and
carry on connecting.
```

```
"If you want to carry on connecting just once, without adding the key
to the cache, hit No.
```

```
"If you do not trust this host, hit Cancel to abandon the connection.
```

"This is a feature of the SSH protocol. It is designed to protect you against a network attack known as *spoofing*: secretly redirecting your connection to a different computer, so that you send your password to the wrong machine. Using this technique, an attacker would be able to learn the password that guards your login account, and could then log in as . . . you and use the account for [his or her] own purposes.

"To prevent this attack, each server has a unique identifying code, called a *host key*. These keys are created in a way that prevents one server from forging another server's key. So if you connect to a server and it sends you a different host key from the one you were expecting, PuTTY can warn you that the server may have been switched and that a spoofing attack might be in progress.

"PuTTY records the host key for each server you connect to, in the Windows Registry. Every time you connect to a server, it checks that the host key presented by the server is the same host key [that was presented] the last time you connected. If it is not, you will see a warning, and you will have the chance to abandon your connection before you type any private information (such as a password) into it."

## Handling Rejected SSH Fingerprints

Several situations can cause an SSH fingerprint to be rejected during the authentication process.

When an SSH fingerprint is rejected, you may see one of the following messages:

- Error importing configuration files from the sensor: Could not find version in string "Unknown version."
- Import failed. Please check the Audit Log for details.

The IPS MC audit log will contain one of the following messages:

- The SSH fingerprint has changed. Please refer to the documentation for instructions on how to handle rejected fingerprints.
- *sensorname*:Error executing SSH while importing sensor version from the sensor - Sensor authentication error. Check username, passphrase, and SSH keys.



---

**Note**

*sensorname* refers to the name of the affected sensor.

---



---

**Caution**

A rejected SSH fingerprint can indicate a spoofing attack on your network. Benign causes of a rejected SSH fingerprint include a change in a device on your network, such as a network card or an IP address. You can accept the rejected fingerprint, but the security of your network depends on your doing so only after you establish that the rejection is due to benign causes.

---

To accept a rejected SSH fingerprint, follow these steps:

---

**Step 1** Run the following command:

```
C:\>plink -ssh userid@ipAddress
```

where:

the *userid* is initially **cisco** for sensor appliances and **ciscoids** for IDSMs. You may have changed the *userid* on your system.

*ipAddress* is the IP address to the sensor.

You will see something similar to the following:

```
WARNING -POTENTIAL SECURITY BREACH! The server's host key does not
match the one PuTTY has cached in the registry. This means that either
the server administrator has changed the host key, or you have actually
connected to another computer pretending to be the server. The new key
fingerprint is: 1024 2a:c5:3f:aa:d4:59:82:1d:83:65:58:a1:4e:59:06:bf.
If you were expecting this change and trust the new key, enter "y" to
update PuTTY's cache and continue connecting. If you want to carry on
connecting but without updating the cache, enter "n". If you want to
abandon the connection completely, press Return to cancel. Pressing
Return is the ONLY guaranteed safe choice. Update cached key? (y/n,
Return cancels connection) Connection abandoned.
```

**Step 2** Enter *y*.

**Step 3** Enter the password of the sensor when prompted.

**Step 4** Terminate the session by entering *exit*.

**Step 5** Verify that the fingerprint was accepted by running the command again (Steps 1, 3, and 4).

This time you should not get the warning message and update cached key prompt.

**Step 6** Verify that you can communicate with your sensor by using IPS MC.

---

# Using the Progress Viewer

For each sensor, the Progress Viewer shows the status and percent completion for deployment of configurations to sensors, signature updates, and signature update downloads from Cisco.com to the IPS MC server.

To use the Progress Viewer, follow these steps:

---

**Step 1** Select **Devices > Progress Viewer**.

The View Progress Tasks page appears in the current browser window. To open the Progress Viewer in a new window, click **New Window** at the bottom of the View Progress Tasks page.



---

**Tip** You can also directly open the Progress Viewer in a new window by clicking on the Progress Viewer icon in the Path bar.

---

**Step 2** To view messages for a background task, select the background task in the Progress Viewer table and then click **Show Messages**.

The messages for the background task appear in a new browser window.

**Step 3** To delete messages from the Progress Viewer table, select the item(s) and then click **Delete**.**Step 4** To refresh the Progress Viewer table, click **Refresh**.**Step 5** To refresh the page automatically, select the **Enable Refresh Rate** check box and select a time interval from the drop-down list.

## Viewing Device Statistics

You can view statistical information for the devices in your IPS MC installation. The statistical information is not updated in real time; instead, it displays a snapshot of the device component at the time the information is requested.

To display statistics for a device, follow these steps:

- 
- Step 1** Select **Devices > Statistics**.
- Step 2** In the Object Selector, select the device for which you want to view statistics. The components of the device that you selected are listed under the heading **Select Component to View**.
- Step 3** Select a device component from the **Select Component to View** list. You can select statistics from the following components:
- Analysis Engine
  - Authentication
  - Denied Attackers
  - Event Server
  - Event Store
  - Host
  - Interface (5.x devices only)
  - Logger
  - Network Access Controller
  - Notification
  - SDEE Server
  - Transaction Server
  - Transaction Source
  - Version/License
  - Virtual Sensor
  - Web Server
- Step 4** Click **View**.
- The report appears in a new browser window.
-

# Managing SSL Certificates

The IPS MC uses SSL certificates to secure and authenticate sensors, thereby ensuring secure communication across your network. This applies to all sensor communications, such as import, re-import, deploy, signature update, query sensor version, query interfaces, and health and welfare.

The IPS MC monitors certificate information and logs messages when the certificate changes for any reason. Beginning with IPS MC version 2.2, you can choose to drop the connection between the sensor and the IPS MC server if the certificate changes. You can easily see whether a connection to a sensor has been rejected because of a bad certificate.

You can also query, view, and set the certificate fingerprint for a particular sensor. For more information see [SSL VPN Security](#) on CCO.

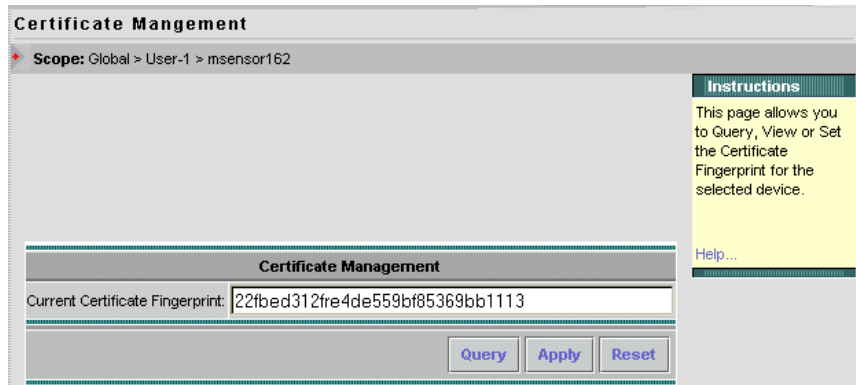
The following field is found on the Certificate Management page:

- **Current Certificate Fingerprint**—a hexadecimal representation of the SSL fingerprint for a particular sensor.

To manage SSL certificates, follow these steps:

- 
- Step 1** Select **Devices > Certificate Management**.
  - Step 2** Click the **Object Selector** handle.
  - Step 3** In the Object Selector, select a sensor for which you want to manage an SSL certificate.

The Object Selector closes and the Certificate Management page appears with its scope set to the sensor you selected.



- Step 4** In the Certificate Management page, click one of the following:
- **Query**—Contacts the sensor and return the certificate fingerprint. You may then click **Apply** to save the information to the IPS MC database.
  - **Apply**—Saves the certificate fingerprint entered in the Current Certificate Fingerprint text field to the IPS MC database.
  - **Reset**—Retrieves the certificate fingerprint from the IPS MC database and displays it in the Current Certificate Fingerprint text field.