CSM 3.x: Add IDS Sensors and Modules to Security Manager Inventory

Document ID: 91671

Contents

Introduction

This document provides information on how to add Intrusion Detection System (IDS) sensors and modules (includes IDSM on Catalyst 6500 switches, NM−CIDS on routers and AIP−SSM on ASA) in the Cisco Security Manager (CSM).

Note: CSM 3.2 does not support IPS 6.2. It is supported in CSM 3.3.

Prerequisites

Requirements

This document assumes that CSM and IDS devices are installed and work properly.

Components Used

The information in this document is based on the CSM 3.0.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Add Devices to the Security Manager Inventory

When you add a device to Security Manager, you bring in a range of identifying information for the device, such as its DNS name and IP address. After you add the device, it appears in the Security Manager device inventory. You can manage a device in Security Manager only after you add it to the inventory.

You can add devices to the Security Manager inventory with these methods:

- Add a device from the network.
- Add a new device that is not yet on the network
- Add one or more devices from the Device and Credentials Repository (DCR).
- Add one or more devices from a configuration file.

Note: This document focuses on the method: Add a new device that is not yet on the network.

Steps to Add the IDS Sensor and Modules

Use the Add New Device option in order to add a single device to the Security Manager inventory. You can use this option for pre–provisioning. You can create the device in the system, assign policies to the device, and generate configuration files before you receive the device hardware.

When you receive the device hardware, you must prepare the devices to be managed by Security Manager. Refer to Preparing the Devices for Security Manager to Manage for more information.

This procedure shows how to add a new IDS sensor and modules:

1. Click the **Device View** button in the toolbar.

   The Devices page appears.
2. Click the **Add** button in the Device selector.

   The New Device – Choose Method page appears with four options.
3. Choose **Add New Device**, then click **Next**.

   The New Device – Device Information page appears.
4. Enter the device information in the appropriate fields.

   See the Providing Device Information New Device section for more information.
5. Click **Finish**.

   The system performs device validation tasks:

   ♦ If the data is incorrect, the system generates error messages and displays the page on which the error occurs with a red error icon that corresponds to it.
   ♦ If the data is correct, the device is added to the inventory and it appears in the Device selector.

Providing Device Information New Device

Complete these steps:

1. Select the device type for the new device:

   a. Select the top–level device type folder in order to display the supported device families.
   b. Select the device family folder in order to display the supported device types.

      a. Select **Cisco Interfaces and Modules > Cisco Network Modules** in order to add the **Cisco IDS Access Router Network Module**. Likewise, select **Cisco Interfaces and Modules > Cisco Services Modules** in order to add the AIP–SSM and IDSM modules shown.

b. Select **Security and VPN > Cisco IPS 4200 Series Sensors** in order to add the Cisco IDS 4210 Sensor to the CSM inventory.
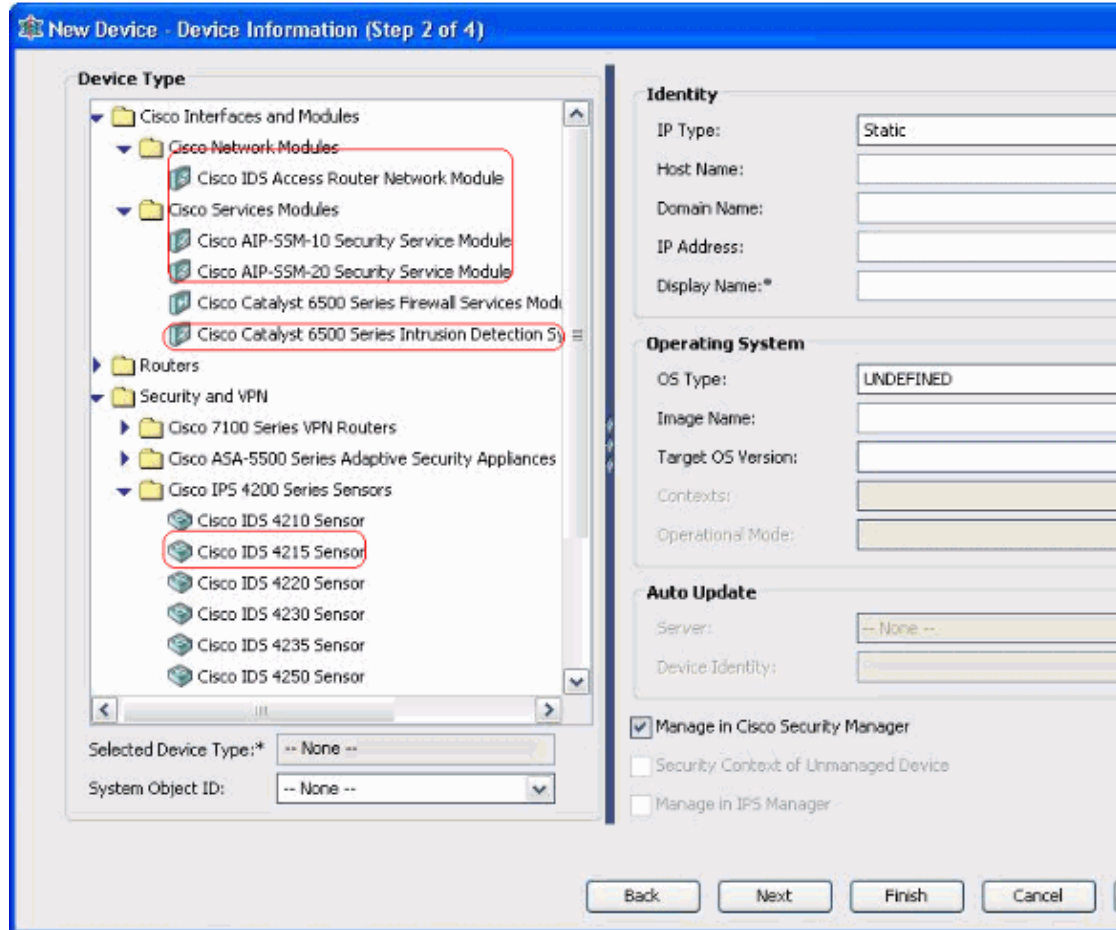
c. Select the device type.

Note: After you add a device, you cannot change the device type.

System object IDs for that device type are displayed in the SysObjectId field. The first system object ID is selected by default. You can select another one if needed.

2. Enter the device identity information, such as the IP type (static or dynamic), hostname, domain name, IP address, and display name.

3. Enter the device operating system information, such as OS type, image name, target OS version, contexts, and operational mode.

4. The Auto Update or CNS−Configuration Engine field appears, which depends on the device type you select:

   ♦ Auto Update Displayed for PIX Firewall and ASA devices.
   ♦ CNS−Configuration Engine Displayed for Cisco IOS® routers.
   Note: This field is not active for Catalyst 6500/7600 and FWSM devices.

5. Complete these steps:

   ♦ Auto Update Click the arrow to display a list of servers. Select the server that is managing the device. If the server does not appear in the list, complete these steps:

      a. Click the arrow, then select + **Add Server**... The Server Properties dialog box appears.
      b. Enter the information in the required fields.

c. Click **OK**. The new server is added to the list of available servers.

♦ CNS–Configuration Engine Different information is displayed, which depends on whether you select static or dynamic IP type:

Static Click the arrow to display a list of Configuration Engines. Select the Configuration Engine that is managing the device. If the Configuration Engine does not appear in the list, complete these steps:

  a. Click the arrow, then select + **Add Configuration Engine**... The Configuration Engine Properties dialog box appears.
  b. Enter the information in the required fields.
  c. Click **OK**. The new Configuration Engine is added to the list of available Configuration Engines.

♦ **Dynamic** Click the arrow to display a list of servers. Select the server that is managing the device. If the server does not appear in the list, complete these steps:

  a. Click the arrow, then select + **Add Server**... The Server Properties dialog box appears.
  b. Enter the information in the required field.
  c. Click **OK**. The new server is added to the list of available servers.

6. Complete these steps:

  ♦ In order to manage the device in Security Manager, check the **Manage in Cisco Security Manager** check box. This is the default.
  ♦ If the only function of the device you are adding is to serve as a VPN end point, uncheck the **Manage in Cisco Security Manager** check box.

    Security Manager will not manage configurations or upload or download configurations on this device.

7. Check the Security Context of Unmanaged Device check box in order to manage a security context, whose parent device (PIX Firewall, ASA, or FWSM) is not managed by Security Manager.

  You can partition a PIX Firewall, ASA, or FWSM into multiple security firewalls, also known as security contexts. Each context is an independent system, with its own configuration and policies. You can manage these standalone contexts in Security Manager, even though the parent (PIX Firewall, ASA, or FWSM) is not managed by Security Manager.

  Note: This field is active only if the device you selected in the Device selector is a firewall device, such as PIX Firewall, ASA, or FWSM, that supports security context.

8. Check the **Manage in IPS Manager** check box in order to manage a Cisco IOS router in IPS Manager.

  This field is active only if you selected a Cisco IOS router from the Device selector.

  Note: IPS Manager can manage the IPS features only on a Cisco IOS router that has IPS capabilities. For more information, see the IPS documentation.

  If you check the Manage in IPS Manager check box, you must check the Manage in Cisco Security Manager check box also.

  If the selected device is IDS, this field is not active. However, the check box is checked because IPS Manager manages IDS sensors.

If the selected device is PIX Firewall, ASA, or FWSM, this field is not active because IPS Manager does not manage these device types.

9. Click **Finish**.

The system performs device validation tasks:

♦ If the data you entered is incorrect, the system generates error messages and displays the page where the error occurs.
♦ If the data you entered is correct, the device is added to the inventory and it appears in the Device selector.

Troubleshoot

Use this section to troubleshoot your configuration.

Error Messages

When you add IPS to CSM, the `Invalid device: Could not deduce the SysObjId for the platform type` error message appears.

Solution

Complete these steps in order to resolve this error message.

1. Stop the CSM Daemon service in Windows, and then choose **Program Files > CSCOpx > MDC > athena > config > Directory**, where you can find `VMS-SysObjID.xml`.
2. On the CSM system, replace the original VMS–SysObjID.xml file located by default in `C:\Program Files\CSCOpx\MDC\athena\config\directory` with the latest `VMS-SysObjID.xml` file.
3. Restart the CSM Daemon Manager service (CRMDmgtd), and re−try to add or discover the affected device(s) again.

Related Information

- **Cisco Security Manager Support Page**
- **Cisco Intrusion Detection System Support Page**
- **Technical Support & Documentation − Cisco Systems**