CHAPTER 16

Managing the Sensor

This chapter describes how to manage your sensor, for example, how to set passwords, obtain and install license keys, set up IP logging variables, update your sensor with the latest software, restore sensor defaults, reboot the sensor, and shut down the sensor. It contains the following sections:

- Configuring Passwords, page 16-1
- Recovering the Password, page 16-3
- Configuring Licensing, page 16-12
- Configuring Sensor Health, page 16-16
- Configuring IP Logging Variables, page 16-17
- Configuring Automatic Update, page 16-18
- Manually Updating the Sensor, page 16-22
- Restoring Defaults, page 16-24
- Rebooting the Sensor, page 16-25
- Shutting Down the Sensor, page 16-25

Configuring Passwords

This section describes how to set up passwords for users on the sensor, and contains the following topics:

- Password Pane, page 16-2
- Passwords Pane Field Definitions, page 16-2
- Configuring Password Requirements, page 16-2

Password Pane

As sensor administrator, you can configure how passwords are created in the Passwords pane. All user-created passwords must conform to the policy that you set in the Passwords pane.

Passwords Pane Field Definitions

Caution If the password policy includes minimum numbers of character sets, such as upper case or number characters, the sum of the minimum number of required character sets cannot exceed the minimum password size. For example, you cannot set a minimum password size of eight and also require that passwords must contain at least five lowercase and five uppercase characters.

The following fields are found in the Passwords pane:

- Attempt Limit—Lets you lock accounts so that users cannot keep trying to log in after a certain number of failed attempts. The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.
- Size Range—Range you specify for the minimum and maximum allowed size for a password. The valid range is 6 to 64 characters.
- Minimum Digit Characters—Minimum number of numeric digits that you specify must be in a password.
- Minimum Upper Case Characters—Maximum number of upper-case alphabet characters that you specify must be in a password.
- Minimum Lower Case Characters—Minimum number of lower-case alphabet characters that you specify must be in a password.
- Minimum Other Characters—Minimum number of non-alphanumeric printable characters that you specify must be in a password.
- Number of Historical Passwords—Number of historical passwords you want the sensor to remember for each account. Any attempt to change the password of an account fails if the new password matches any of the remembered passwords. When this value is 0, no previous passwords are remembered.

Configuring Password Requirements

To configure password requirements, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Passwords**.

Step 3 In the Attempt Limit field, enter how many attempts a user has to enter the correct password.

Note The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.

Step 4 In the Size Range field, enter how long the password can be. The valid range is 6 to 64.

Step 5 In the Minimum Digit Characters field, enter the minimum number of numeric digits a password can have.

Step 6 In the Minimum Upper Case Characters field, enter the least number of upper case characters the password can have.

Step 7 In the Minimum Lower Case Characters field, enter the least number of lower case characters the password can have.

Caution If the password policy includes minimum numbers of character sets, such as upper case or number characters, the sum of the minimum number of required character sets cannot exceed the minimum password size. For example, you cannot set a minimum password size of eight and also require that passwords must contain at least five lowercase and five uppercase characters.

Step 8 In the Minimum Other Characters field, enter the least number of other characters the password can have.

Step 9 In the Number of Historical Passwords field, enter the number of historical passwords you want the sensor to remember for each account.

Tip To discard your changes, click **Reset**.

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Recovering the Password

For most IPS platforms, you can now recover the password on the sensor rather than using the service account or reimaging the sensor. This section describes how to recover the password on the various platforms, and contains the following topics:

- Understanding Password Recovery, page 16-3
- Recovering the Appliance Password, page 16-4
- Recovering the AIM IPS Password, page 16-6
- Recovering the AIP SSM Password, page 16-6
- Recovering the IDSM2 Password, page 16-9
- Recovering the NME IPS Password, page 16-9
- Disabling Password Recovery, page 16-10
- Troubleshooting Password Recovery, page 16-11
- Verifying the State of Password Recovery, page 16-11

Understanding Password Recovery

Password recovery implementations vary according to IPS platform requirements. Password recovery is implemented only for the cisco administrative account and is enabled by default. The IPS administrator can then recover user passwords for other accounts using the CLI. The cisco user password reverts to **cisco** and must be changed after the next login.

Note Administrators may need to disable the password recovery feature for security reasons.

Table 16-1 lists the password recovery methods according to platform.

Table 16-1 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4200 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
AIM IPS NME IPS	Router IPS modules	Bootloader command
AIP SSM	ASA 5500 series adaptive security appliance modules	adaptive security appliance CLI command
IDSM2	Switch IPS module	Password recovery image file

Recovering the Appliance Password

There are two ways to recover the password for appliances—using the GRUB menu or ROMMON. This section describes how to recover the password on appliances, and contains the following topics:

- Using the GRUB Menu, page 16-4
- Using ROMMON, page 16-5

Using the GRUB Menu

For the 4200 series appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

Note You must have a terminal server or direct serial connection to the appliance to use the GRUB menu to recover the password.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance to see the GRUB menu.

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
-------------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
-------------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **`2: Cisco IPS Clear Password (cisco)`**.

The password is reset to **cisco**. You can change the password the next time you log in to the CLI.

Using ROMMON

For the IPS 4240 and the IPS 4255 you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

To recover the password using the ROMMON CLI, follow these steps:

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection).

The boot code either pauses for 10 seconds or displays something similar to one of the following:

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

Step 3 Enter the following commands to reset the password.

```
confreg 0x7
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS 4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Recovering the AIM IPS Password

To recover the password for the AIM IPS, use the **clear password** command. You must have console access to the AIM IPS and administrative access to the router.

To recover the password for the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

Step 4 Session in to the AIM IPS.

```
router# service-module ids-sensor slot/port session
```

Example

```
router# service-module ids-sensor 0/0 session
```

Step 5 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 6 Reset the AIM IPS from the router console.

```
router# service-module ids-sensor 0/0 reset
```

Step 7 Press **Enter** to return to the router console.

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

```
ServicesEngine boot-loader# clear password
```

The AIM IPS reboots. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Recovering the AIP SSM Password

You can reset the password to the default (**cisco**) for the AIP SSM using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Note To reset the password, you must have ASA 7.2.2 or later.

Use the **hw-module module** *slot_number* **password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

Resetting the Password Using the CLI

To reset the password on the AIP SSM, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command to verify the module slot number:

```
asa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5510 Adaptive Security Appliance         ASA5510            JMX1135L097
  1 ASA 5500 Series Security Services Module-40  ASA-SSM-40         JAF1214AMRL

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 001b.d5e8.e0c8 to 001b.d5e8.e0cc  2.0          1.0(11)2     8.4(3)
  1 001e.f737.205f to 001e.f737.205f  1.0          1.0(14)5     7.0(7)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- -------------------------
  1 IPS                            Up               7.0(7)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

Step 2 Reset the password for module 1.

```
asa# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm]
```

Step 3 Press **Enter** to confirm.

```
Password-Reset issued for slot 1.
```

Step 4 Verify the status of the module. Once the status reads Up, you can session to the AIP SSM.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5500 Series Security Services Module-40  ASA-SSM-40         JAF1214AMRL

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 001e.f737.205f to 001e.f737.205f  1.0          1.0(14)5     7.0(7)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- -------------------------
  1 IPS                            Up               7.0(7)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Step 5 Session to the AIP SSM.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 6 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
```

```
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 7 Enter your new password twice.

```
New password: new password
Retype new password: new password

***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.
aip_ssm#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Recovering the NME IPS Password

To recover the password for the NME IPS, use the **clear password** command. You must have console access to the NME IPS and administrative access to the router. To recover the password for the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

Step 4 Session in to the NME IPS.

```
router# service-module ids-sensor slot/port session
```

Example

```
router# service-module ids-sensor 1/0 session
```

Step 5 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 6 Reset the NME IPS from the router console.

```
router# service-module ids-sensor 1/0 reset
```

Step 7 Press **Enter** to return to the router console.

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

```
ServicesEngine boot-loader# clear password
```

The NME IPS reboots. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Recovering the IDSM2 Password

To recover the password for the IDSM2, you must install a special password recovery image file. This installation only resets the password, all other configuration remains intact. The password recovery image is version-dependent and can be found on the Cisco Download Software site. For IPS 6.*x*, download WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz. For IPS 7.*x*, download WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz.

FTP is the only supported protocol for image installations, so make sure you put the password recovery image file on an FTP server that is accessible to the switch. You must have administrative access to the Cisco 6500 series switch to recover the password on the IDSM2.

During the password recovery image installation, the following message appears:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

This message is in error. Installing the password recovery image does not remove any configuration, it only resets the login account.

Once you have downloaded the password recovery image file, follow the instructions to install the system image file but substitute the password recovery image file for the system image file. The IDSM2 should reboot into the primary partition after installing the recovery image file. If it does not, enter the following command from the switch:

```
hw-module module module_number reset hdd:1
```

Note The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

For More Information

- For the procedure for installing system images on the IDSM2, see Installing the IDSM2 System Image, page 21-27.
- For more information on downloading Cisco IPS software, see Obtaining Cisco IPS Software, page 20-1.

Disabling Password Recovery

Caution If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimage your sensor.

Password recovery is enabled by default. You can disable password recovery through the CLI or the IDM.

Disabling Password Recovery Using the CLI

To disable password recovery in the CLI, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

```
sensor(config)# service host
```

Step 4 Disable password recovery.

```
sensor(config-hos)# password-recovery disallowed
```

Disabling Password Recovery Using the IDM

To disable password recovery in the IDM, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration >Sensor Setup > Network**.

Step 3 To disable password recovery, uncheck the **Allow Password Recovery** check box.

Troubleshooting Password Recovery

When you troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If you attempt password recovery, it always appears to succeed. If it has been disabled, the password is not reset to **`cisco`**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as the AIM IPS and the NME IPS bootloader, ROMMON, and the maintenance partition for the IDSM2, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.
- When performing password recovery on the IDSM2, you see the following message: `Upgrading will wipe out the contents on the storage media`. You can ignore this message. Only the password is reset when you use the specified password recovery image.

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled. To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

Step 3 Verify the state of password recovery by using the **include** keyword to show settings in a filtered output.

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

Configuring Licensing

This section describes how to obtain and install the license key, and contains the following topics:

- Licensing Pane, page 16-12
- Understanding Licensing, page 16-12
- Service Programs for IPS Products, page 16-13
- Licensing Pane Field Definitions, page 16-14
- Obtaining and Installing the License Key, page 16-14
- Uninstalling the License Key, page 16-15

Licensing Pane

Note You must be administrator to view license information in the Licensing pane and to install the sensor license key.

In the Licensing pane, you can obtain and install the sensor license key. The Licensing pane displays the status of the current license.

Understanding Licensing

Although the sensor functions without the license key, you must have a license key to obtain signature updates and use the global correlation features. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract—Contact your reseller, Cisco service or product sales to purchase a contract.
- Your IPS device serial number—To find the IPS device serial number in the IDM, choose **Configuration > Sensor Management > Licensing**., or in the CLI use the **show version** command.
- Valid Cisco.com username and password

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to http://www.cisco.com/go/license and click **IPS Signature Subscription Service** to apply for a license key.

You can view the status of the license key in these places:

- The IDM Home window Licensing section on the Health tab
- The IDM Licensing pane (**Configuration > Licensing**)
- The License Notice at CLI login

Whenever you start the IDM or the CLI, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use the IDM and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key to the computer that the IDM is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

When you purchase an ASA 5500 series adaptive security appliance product that does not contain IPS, you must purchase a SMARTnet contract.

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

When you purchase an ASA 5500 series adaptive security appliance product that ships with AIP SSM installed, or if you purchase it to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract.

Note Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

For example, if you purchase an ASA 5510 and then later want to add IPS and purchase an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract. After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key.

Caution If you ever send your product for RMA, the serial number changes. You must then get a new license key for the new serial number.

Licensing Pane Field Definitions

The following fields are found in the Licensing pane:

- Current License—Provides the status of the current license:
  - License Status—Current license status of the sensor.
  - Expiration Date—Date when the license key expires (or has expired). If the key is invalid, no date is displayed.
  - Serial Number—Serial number of the sensor.
  - Product ID—The product ID of your sensor.
- Update License—Specifies from where to obtain the new license key:
  - Cisco.com—Contacts the license server at Cisco.com for a license key.
  - License File—Specifies that a license file be used.
  - Local File Path—Indicates where the local file is that contains the license key.

Obtaining and Installing the License Key

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

To obtain and install the license key, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Licensing**. The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.

Step 3 Obtain a license key by doing one of the following:

- Click the **Cisco.com** radio button to obtain the license from Cisco.com. The IDM contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.
- Click the **License File** radio button to use a license file. To use this option, you must apply for a license key at this URL: www.cisco.com/go/license. The license key is sent to you in e-mail and you save it to a drive that the IDM can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

Step 4 Click **Update License**, and in the Licensing dialog box, click **Yes** to continue. The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.

Step 5 Click **OK**.

Step 6 Go to www.cisco.com/go/license.

Step 7 Fill in the required fields. Your license key will be sent to the e-mail address you specified.

Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 8 Save the license key to a hard-disk drive or a network drive that the client running the IDM can access.

Step 9 Log in to the IDM.

Step 10 Choose **Configuration > Sensor Management > Licensing**.

Step 11 Under Update License, click the **License File** radio button.

Step 12 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 13 Browse to the license file and click **Open**.

Step 14 Click **Update License**.

Uninstalling the License Key

Use the **erase license-key** command to uninstall the license key on your sensor. This allows you to delete an installed license key from a sensor without restarting the sensor or logging into the sensor using the service account.

To uninstall the license key, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Uninstall the license key on the sensor.

```
sensor# erase license-key
Warning: Executing this command will remove the license key installed on the sensor.

You must have a valid license key installed on the sensor to apply the Signature Updates
and use the Global Correlation features.

Continue? []: yes
sensor#
```

Step 3 Verify the sensor key has been uninstalled.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(7)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S615.0                  2012-01-03
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS-4260-K9
Serial Number:          AZBW5470014
No license present
Sensor up-time is 5 days.
```

```
Using 1887371264 out of 4100345856 bytes of available memory (46% usage) system is using
18.2M out of 38.5M bytes of available disk space (47% usage) application-data is using
48.0M out of 166.8M bytes of available disk space (30% usage) boot is using 46.1M out of
69.5M bytes of available disk space (70% usage) application-log is using 494.0M out of
513.0M bytes of available disk space (96% usage)


MainApp            B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
AnalysisEngine     B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
CollaborationApp   B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
CLI              B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600

Upgrade History:

  IPS-K9-7.0-7-E4   05:05:07 UTC Mon Jan 16 2012

Recovery Partition Version 1.1 - 7.0(7)E4

Host Certificate Valid from: 17-Jan-2012 to 17-Jan-2014
```

Configuring Sensor Health

This section describes how to configure sensor health metrics, and contains the following topics:

- Sensor Health Pane, page 16-16
- Sensor Health Pane Field Definitions, page 16-17

Sensor Health Pane

Note You must be administrator to configure sensor health metrics.

In the Sensor Health pane, you can configure the metrics that are used to determine the health and network security status of the IPS. The results show up in the Home pane in the various gadgets.

If you do not select a metric by checking the check box, it does not show up in the health and network security status results. You can accept the default configuration or edit the values.

The overall health is set to the most critical settings of any of the metrics. For instance, if all the selected metrics are green except for one that is red, the overall health becomes red. The IPS produces a health and security status event when the overall health status of the IPS changes.

The security status of the sensor is determined for each virtual sensor using the threat ratings of events detected by the virtual sensors. The security status of the virtual sensor is raised when the virtual sensor detects an event with a threat rating that exceeds the threshold for that virtual sensor. Once a threshold has been exceeded, the security status remains at a critical level until the configured amount of time has passed with no more events being detected at the higher level.

Sensor Health Pane Field Definitions

The following fields are found in the Sensor Health pane:

- Inspection Load—Lets you set a threshold for inspection load and whether this metric is applied to the overall sensor health rating.
- Missed Packet—Lets you set a threshold percentage for missed packets and whether this metric is applied to the overall sensor health rating.
- Memory Usage—Lets you set a threshold percentage for memory usage and whether this metric is applied to the overall sensor health rating.
- Signature Update—Lets you set a threshold for when the last signature update was applied and whether this metric is applied to the overall sensor health rating.
- License Expiration—Lets you set a threshold for when the license expires and whether this metric is applied to the overall sensor health rating.
- Event Retrieval—Lets you set a threshold for when the last event was retrieved and whether this metric is applied to the overall sensor health rating.

  Note The event retrieval metric keeps track of when the last event was retrieved by an external monitoring application such as IME. Disable Event Retrieval if you are not doing external event monitoring.

- Network Participation—Lets you choose whether the network participation health metrics contribute to the overall sensor health rating.
- Global Correlation—Let you choose whether the global correlation health metrics contribute to the overall sensor health rating.
- Application Failure—Lets you choose to have an application failure applied to the overall sensor health rating.
- IPS in Bypass Mode—Let you choose to know if bypass mode is active and have that apply to the overall sensor health rating.
- One or More Active Interfaces Down—Lets you choose to know if one or more enabled interfaces are down and have that apply to the overall sensor health rating.
- Yellow Threshold—Lets you set the lowest threshold in percentage, days, seconds, or failures for yellow.
- Red Threshold—Lets you set the lowest threshold in percentage, days, seconds, or failures for red.

Configuring IP Logging Variables

Note You must be administrator to configure the IP logging variable.

You can configure the IP logging variable, Maximum Open IP Log Files, which applies to the general operation of the sensor.

Field Definitions

The following field is found in the Global Variables pane:

- Maximum Open IP Log Files—Maximum number of concurrently open IP log files. The valid range is from 20 to 100. The default is 20.

Configuring Automatic Update

This section describes how to configure your sensor for automatic software updates, and contains the following topics:

- Auto/Cisco.com Update Pane, page 16-18
- Supported FTP and HTTP Servers, page 16-19
- UNIX-Style Directory Listings, page 16-19
- Signature Updates and Installation Time, page 16-19
- Auto/Cisco.com Update Pane Field Definitions, page 16-20
- Configuring Auto Update, page 16-21

Auto/Cisco.com Update Pane

Note You must be administrator to view the Auto/Cisco.com Update pane and to configure automatic updates.

You can configure the sensor to automatically download signature and signature engine updates from Cisco.com and from a local server. When you enable automatic updates, the sensor logs in to Cisco.com and checks for signature and signature engine updates. When an update is available, the sensor downloads the update and installs it. You must have a Cisco.com user account with cryptographic privileges to download Cisco IPS signature and signature engine updates from Cisco.com. The first time you download Cisco software you set up an account with cryptographic privileges.

Caution Automatic updates do not work with Windows FTP servers configured with DOS-style paths. Make sure the server configuration has the UNIX-style path option enabled rather than DOS-style paths.

Caution The sensor does not support communication with Cisco.com through nontransparent proxy servers.

Caution In IPS 7.0(8)E4 the default value of the Cisco server IP address has been changed from 198.133.219.25 to 72.163.4.161 in the Auto Update URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new IP address.

Supported FTP and HTTP Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- CMS - Apache Server (Tomcat)
- CMS - Apache Server (JRun)

UNIX-Style Directory Listings

To configure Auto Update using an FTP server, the FTP server must provide directory listing responses in UNIX style. MS-DOS style directory listing is not supported by the sensor Auto Update feature.

Note If the server supplies MS-DOS style directory listings, the sensor cannot parse the directory listing and does not know that there is a new update available.

To change Microsoft IIS to use UNIX-style directory listings, follow these steps:

Step 1 Choose **Start > Program Files > Administrative Tools**.

Step 2 Click the **Home Directory** tab.

Step 3 Click the **UNIX directory listings style** radio button.

Signature Updates and Installation Time

There is a short period of time that traffic is not inspected while you are performing signature updates. However, traffic continues to flow if you have bypass enabled.

When a signature update adds or modifies signatures that contain regular expressions, the regular expression cache tables used by SensorApp have to be recompiled. The amount of recompile time varies by platform, number of signatures modified and/or added, and type of signatures modified and/or added.

If a signature update only adds one or two new signatures on a high-end platform, for example, IPS 4255 or IPS 4260, the recompile can be as fast as a few seconds.

The recompile takes several minutes and even up to a half hour under the following conditions:

- When a signature update adds a large number of signatures, for example, when you are skipping several signature levels to install a newer one, for example, installing S258 on top of S240.
- When a signature update modifies a large number of signatures, for example when a large number of older signatures is disabled and/or retired.

During the recompile, SensorApp stops monitoring packets. The interface driver detects this when the packet buffers begin filling up on the way to SensorApp and the driver stops receiving packets from SensorApp. If the sensor is in inline mode, the driver either turns on bypass if the bypass option is set to Auto, or brings down the interface links if bypass is set to Off.

Note Some packets can be dropped before the bypass setting begins operating. Once SensorApp completes the recompile of the regular expression cache files, SensorApp reconnects to the driver and begins monitoring again, and the driver begins passing packets to SensorApp for analysis, and if necessary, also brings the interface links back up.

Auto/Cisco.com Update Pane Field Definitions

The following fields are found in the Auto/Cisco.com Update pane:

- Enable Auto Update From a Remote Server—Lets the sensor install updates stored on a remote server.

  Note If Enable Auto Update From a Remote Server is not checked, all fields are disabled and cleared. You cannot toggle this on or off without losing all other settings.

- Remote Server Access—Lets you specify the following options:
  - IP Address—Identifies the IP address of the remote server.
  - File Copy Protocol—Specifies whether to use FTP or SCP.
  - Directory—Identifies the path to the update on the remote server.
  - Username—Identifies the username corresponding to the user account on the remote server.
  - Password—Identifies the password for the user account on the remote server.
  - Confirm Password—Confirms the password by forcing you to retype the remote server password.
- Enable Signature and Engine Updates from Cisco.com—Lets the sensor go to Cisco.com to download signature and engine updates.
- Cisco.com Access
  - Username—Identifies the username corresponding to the user account on Cisco.com.
  - Cisco.com URL—Automatically populated with the correct URL when you check the **Enable Signature and Engine Updates from Cisco.com** check box.
  - Password—Identifies the password for the user account on Cisco.com.
  - Confirm Password—Confirms the password by forcing you to retype the Cisco.com password.
- Schedule—Lets you specify the following options:
  - Start Time—Identifies the time to start the update process. This is the time when the sensor will contact the remote server and search for an available update.
  - Frequency—Specifies whether to perform updates on an hourly or weekly basis.
  - Hourly—Specifies to check for an update every n hours.
  - Daily—Specifies the days of the week to perform the updates.

Configuring Auto Update

To configure automatic updates from a remote server or Cisco.com, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Auto/Cisco.com Update**.

Step 3 To enable automatic updates from a remote server, check the **Enable Auto Update from a Remote Server** check box.

a. In the IP Address field, enter the IP address of the remote server where you have downloaded and stored updates.

b. To identify the protocol used to connect to the remote server, from the File Copy Protocol drop-down list, choose either FTP or SCP.

c. In the Directory field, enter the path to the directory on the remote server where the updates are located. A valid value for the path is 1 to 128 characters.

d. In the Username field, enter the username to use when logging in to the remote server. A valid value for the username is 1 to 2047 characters.

e. In the Password field, enter the username password on the remote server. A valid value for the password is 1 to 2047 characters.

f. In the Confirm Password field, enter the password to confirm it.

g. For hourly updates, check the **Hourly** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
- In the Every_hours field, enter the hour interval at which you want every update to occur. The valid value is 1 to 8760.

  For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates. The sensor determines the most recent update that can be installed and installs that file.

h. For weekly updates, check the **Daily** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
- In the Days field, check the day(s) you want the sensor to check for and download available updates.

Step 4 To enable signature and engine updates from Cisco.com, check the **Enable Signature and Engine Updates from Cisco.com** check box.

a. In the Username field, enter the username to use when logging in to Cisco.com. A valid value for the username is 1 to 2047 characters.

b. In the Password field, enter the username password for Cisco.com. A valid value for the password is 1 to 2047 characters.

c. In the Confirm Password field, enter the password to confirm it.

d. For hourly updates, check the **Hourly** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
- In the Every_hours field, enter the hour interval at which you want every update to occur. The valid value is 1 to 8760.

For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates. The sensor determines the most recent update that can be installed and installs that file.

e. For weekly updates, check the **Daily** check box, and follow these steps:
   - In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
   - In the Days field, check the day(s) you want the sensor to check for and download available updates.

Tip To discard your changes, click **Reset**.

Step 5 Click **Apply** to save your changes.

Manually Updating the Sensor

This section describes how to manually update the sensor, and contains the following topics:

- Update Sensor Pane, page 16-22
- Update Sensor Pane Field Definitions, page 16-22
- Updating the Sensor, page 16-23

Update Sensor Pane

Note You must be administrator to view the Update Sensor pane and to update the sensor with service packs and signature updates.

In the Update Sensor pane, you can immediately apply service pack and signature updates.

Note To manually update the sensor, you must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

Update Sensor Pane Field Definitions

The following fields are found in the Update Sensor pane:

- Update is located on a remote server and is accessible by the sensor—Lets you specify the following options:
  - URL—Identifies the type of server where the update is located. Specify whether to use FTP, HTTP, HTTPS, or SCP.
  - ://—Identifies the path to the update on the remote server.
  - Username—Identifies the username corresponding to the user account on the remote server.

  - Password—Identifies the password for the user account on the remote server.
- Update is located on this client—Lets you specify the following options:
  - Local File Path—Identifies the path to the update file on this local client.
  - Browse Local—Opens the Browse dialog box for the file system on this local client. From this dialog box, you can navigate to the update file.

Updating the Sensor

Note To manually update the sensor, you must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

To immediately apply a service pack and signature update, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Update Sensor**.

Step 3 To pull an update down from a remote server and install it on the sensor, follow these steps:

a. Check the **Update is located on a remote server and is accessible by the sensor** check box.

b. In the URL field, enter the URL where the update can be found.

The following URL types are supported:

- FTP:—Source URL for an FTP network server.

  The syntax for this prefix is the following:

  `ftp://location/relative_directory/filename`

  or

  `ftp://location//absolute_directory/filename`

- HTTPS:—Source URL for a web server.

  The syntax for this prefix is the following:

  `https://location/directory/filename`

  Note Before using the HTTPS protocol, set up a TLS trusted host.

- SCP:—Source URL for a SCP network server.

  The syntax for this prefix is the following:

  `scp://location/relative_directory/filename`

  or

  `scp://location/absolute_directory/filename`

- HTTP:—Source URL for a web server.

  The syntax for this prefix is the following:

  `http://location/directory/filename`

The following example shows the FTP protocol:

`ftp://user@ip_address/UPDATES/file_name.rpm.pkg`

Note You must have already downloaded the update from Cisco.com and put it on the FTP server.

c. In the Username field, enter the username for an account on the remote server.

d. In the Password field, enter the password associated with this account on the remote server.

Step 4 To push from the local client and install it on the sensor, follow these steps:

a. Check the **Update is located on this client** check box.

b. Specify the path to the update file on the local client or click **Browse Local** to navigate through the files on the local client.

Step 5 Click **Update Sensor**. The Update Sensor dialog box tells you that if you want to update, you will lose your connection to the sensor and you must log in again.

Step 6 Click **OK** to update the sensor.

Note The IDM and CLI connections are lost during the following updates: service pack, minor, major, and engineering patch. If you are applying one of these updates, the installer restarts the IPS applications. A reboot of the sensor is possible. You do not lose the connection when applying signature updates and you do not need to reboot the system.

Tip To discard your changes and close the dialog box, click **Cancel**.

Restoring Defaults

Note You must be administrator to view the Restore Defaults pane and to restore the sensor defaults.

Warning **Restoring the defaults removes the current application settings and restores the default settings. Your network settings also return to the defaults and you immediately lose connection to the sensor.**

You can restore the default configuration to your sensor. To restore the default configuration, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Restore Defaults**.

Step 3 To restore the default configuration, click **Restore Defaults**.

Step 4 In the Restore Defaults dialog box, click **OK**.

Note Restoring defaults resets the IP address, netmask, default gateway, and access list. The password and time are not reset. Manual and automatic blocks also remain in effect. You must manually reboot your sensor.

Rebooting the Sensor

Note You must be administrator to see the Reboot Sensor pane and to reboot the sensor.

You can shut down and restart the sensor from the Reboot Sensor pane. To reboot the sensor, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Reboot Sensor**, and then click **Reboot Sensor**.

Step 3 To shut down and restart the sensor, click **OK**. The sensor applications shut down and then the sensor reboots. After the reboot, you must log back in.

Note There is a 30-second delay during which users who are logged in to the CLI are notified that the sensor applications are going to shut down.

Shutting Down the Sensor

Note You must be administrator to view the Shut Down Sensor pane and to shut down the sensor.

You can shut down the IPS applications and then put the sensor in a state in which it is safe to power it off. To shut down the sensor, follow these steps:

Step 1 Log in to the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > Sensor Management > Shut Down Sensor**, and then click **Shut Down Sensor**.

Step 3 In the Shut Down Sensor dialog box, click **OK**. The sensor applications shut down and any open connections to the sensor are closed.

Note There is a 30-second delay during which users who are logged in to the CLI are notified that the sensor applications are going to shut down.