CHAPTER 11

Maintaining the Sensor

This chapter describes how to maintain the sensor by automatically updating the sensor with the most recent software, or updating it immediately, restoring the factory defaults, and shutting down the sensor. You can also generate information for troubleshooting purposes and to use if you need to contact TAC. This chapter contains the following sections:

Updating the Sensor Automatically

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

Auto Update Pane

Note You must be administrator to view the Auto Update pane and to configure automatic updates

You can configure automatic service pack and signature updates, so that when service pack or signature updates are loaded on a central FTP or SCP server, they are downloaded and applied to your sensor.

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.

Note The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server.

Caution After you download an update from Cisco.com, you must take steps to ensure the integrity of the downloaded file while it resides on your FTP or SCP server.

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.

Auto Update Pane Field Definitions

The following fields are found in the Auto Update pane:

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

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

Note The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server.

To configure automatic updates, follow these steps:

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

Step 2 Choose **Configuration > Auto Update**.

Step 3 To enable automatic updates, check the **Enable Auto Update** check box.

Step 4 In the IP Address field, enter the IP address of the remote server where you have downloaded and stored updates.

Step 5 To identify the protocol used to connect to the remote server, from the File Copy Protocol drop-down list, choose either FTP or SCP.

Step 6 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.

Step 7 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.

Step 8 In the Password field, enter the username password on the remote server. A valid value for the password is 1 to 2047 characters.

Step 9 In the Confirm Password field, enter the password to confirm it.

Step 10 For hourly updates, check the **Hourly** check box, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.

b. 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.

Step 11 For weekly updates, check the **Daily** check box, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.

b. 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 12 Click **Apply** to save your changes.

Restoring the Defaults

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

You can restore the default configuration to your sensor.

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.**

Field Definitions

The following buttons are found in the Restore Defaults pane:

- Restore Defaults—Opens the Restore Defaults dialog box. In this dialog box, you can begin the restore defaults process. This process returns the sensor configuration to the default settings and immediately terminates connection to the sensor.
- OK—Starts the restore defaults process.
- Cancel—Closes the Restore Defaults dialog box and returns you to the Restore Defaults pane without performing the restore defaults process.

Restoring the Defaults

To restore the default configuration, follow these steps:

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

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

Step 3 To restore the default configuration, click **Restore Configuration Defaults**. The Restore Defaults dialog box appears.

Step 4 To begin the restore defaults process, click **Yes**.

Note Restoring defaults resets the IP address, netmask, default gateway, and access list. The password, and time will not be reset. Manual and automatic blocks also remain in effect.

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.

Field Definitions

The following button is found in the Reboot Sensor pane:

- Reboot Sensor—Opens the Reboot Sensor dialog box. In this dialog box, you can begin the process that shuts down and restarts the sensor.

Rebooting the Sensor

To reboot the sensor, follow these steps:

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

Step 2 Choose **Configuration > Reboot**, 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.

Field Definitions

The following button is found in the Shut Down Sensor pane:

- Shut Down Sensor—Opens the Shut Down Sensor dialog box. In this dialog box, you can begin the process that shuts down the sensor.

Shutting Down the Sensor

To shut down the sensor, follow these steps:

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

Step 2 Choose **Configuration > Shut Down Sensor**.

Step 3 Click **Shut Down Sensor**, and then 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.

Updating the Sensor

This section describes how to update the sensor with the most current software, and contains the following topics:

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 The sensor cannot download service pack and signature updates from Cisco.com. 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 The sensor cannot download service pack and signature updates from Cisco.com. 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 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.

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

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.

Generating a Diagnostics Report

Note You must be administrator to run diagnostics.

You can obtain diagnostics information on your sensors for troubleshooting purposes. The diagnostics report contains internal system information, such as logs, status, configuration, and so forth, that is intended for TAC to use when troubleshooting the sensor. You can view the report in the Diagnostics Report pane or you can click **Save** and save it to the hard-disk drive.

Note Generating a diagnostics report can take a few minutes.

Field Definitions

The following buttons are found in the Diagnostics Report pane:

- Save—Opens the Save As dialog box so you can save a copy of the diagnostics report to your hard-disk drive.
- Generate Report—Starts the diagnostics process. This process can take several minutes to complete. After the process is complete, a report is generated and the display is refreshed with the updated report.

Generating a Diagnostics Report

Caution After you start the diagnostics process, do not click any other options in IDM or leave the Diagnostics pane. This process must be completed before you can perform any other tasks for the sensor.

To run diagnostics, follow these steps:

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

Step 2 Choose **Monitoring > Support Information > Diagnostics Report**.

Step 3 Click **Generate New Report**.

Note The diagnostics process can take some time to complete. When the process has finished running, the display is refreshed with the updated results.

Step 4 To save this report as a file, click **Save**. The **Save As** dialog box opens and you can save the report to your hard-disk drive.

Viewing Statistics

Note Administrators, operators, and viewers can view system statistics.

The Statistics pane shows statistics for the following categories:

- Analysis Engine
- Anomaly Detection
- Event Server
- Event Store
- External Product Interface
- Host
- Interface Configuration
- Logger
- Attack Response Controller (formerly known as Network Access Controller)

- Notification
- OS Identification
- Transaction Server
- Virtual Sensor
- Web Server

Field Definitions

The following button is found in the Statistics pane:

- Refresh—Displays the most recent information about the sensor applications, including the Web Server, Transaction Source, Transaction Server, Network Access Controller (known as Attack Response Controller in IPS 5.1 but still listed as Network Access Controller in the statistics), Logger, Host, Event Store, Event Server, Analysis Engine, Interface Configuration, and Authentication.

Viewing Statistics

To show statistics for your sensor, follow these steps:

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

Step 2 Choose **Monitoring > Support Information > Statistics**.

Step 3 To update statistics as they change, click **Refresh**.

Viewing System Information

Note You must be administrator or operator to view system information. Viewers can see all system information except for how long the sensor has been running and the disk usage.

The System Information pane displays following information:

- TAC contact information
- Platform information
- Booted partition
- Software version
- Status of applications
- Upgrades installed
- PEP information
- Memory usage
- Disk usage

Field Definitions

The following button is found in the System Information pane:

- Refresh—Displays the most recent information about the sensor, including the software version and PEP information.

Viewing System Information

To view system information, follow these steps:

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

Step 2 Choose **Monitoring > Support Information > System Information**. The System Information pane displays information about the system.

Step 3 Click **Refresh**. The pane refreshes and displays new information.