CHAPTER 5

# Using the Startup Wizard

This chapter describes the Startup wizard and how to use it to configure your sensor. It contains the following sections:

## Startup Wizard Introduction Window

**Note** You must be administrator to configure basic sensor settings in the Startup wizard.

Because the IME cannot communicate with an unconfigured sensor, you must log in to the sensor CLI and run the **setup** command to configure communication parameters. You can set all communication parameters by using the **setup** command. You can use the Startup Wizard to modify a sensor that has already been configured, but you cannot use the Startup Wizard for initializing a new, unconfigured sensor. You must use the **setup** command for that. Because until you initialize the sensor with the **setup** command, the IME cannot connect to the sensor.

The Startup Wizard leads you through the steps needed to configure the sensor to inspect, respond to, and report on traffic. You can configure basic sensor network settings, set the sensor time, associate signature policies with threat profiles, configure interfaces, create policies, assign policies and interfaces to the virtual sensor, configure the sensor to automatically download signature and signature engine updates from Cisco.com, and save your changes to the sensor.

You can use the Startup Wizard on all IPS platforms. If a feature is not available on a certain platform, you will not see that configuration window.

**Note** VLAN groups are not supported in the Startup Wizard.

The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the following features of the Setup Wizard—Inline VLAN pairs, inline interface pairs, VLAN groups, setting the time, or interface configuration (you must configure interfaces on the adaptive security appliance).

**Note** The ASA IPS modules get their time settings from the adaptive security appliance in which they are installed.

#### For More Information

You must initialize the sensor before you can choose **Configuration >** ***sensor_name*** **> Sensor Setup** in IME to further configure the sensor. For the procedure for using the **setup** command to initialize the sensor, see Basic Sensor Setup, page 24-4.

# Setting up the Sensor

This section describes how to set up the sensor, and contains the following topics:

- Sensor Setup Window, page 5-2
- Add and Edit ACL Entry Dialog Boxes, page 5-3
- Configure Summertime Dialog Box, page 5-4
- Configuring Sensor Settings, page 5-5

## Sensor Setup Window

In the two Sensor Setup window, you can configure the sensor for basic operation. Most of the fields will already be populated because you assigned the values during initialization. But you can change them here if needed.

#### Field Definitions

The following fields are found in the Sensor Setup window:

- Network Settings—Lets you set the network settings of the sensor:
  - Host Name—Specifies the name of the sensor. The hostname can be a string of 1 to 64 characters that matches the pattern ^[A-Za-z0-9_/-]+$. The default is sensor. You receive an error message if the name contains a space or exceeds 64 alphanumeric characters.
  - IP Address—Specifies the IP address of the sensor. The default is 192.168.1.2.
  - Subnet Mask—Specifies the mask corresponding to the IP address. The default is 255.255.255.0.
  - Gateway—Specifies the default gateway address. The default is 192.168.1.1.
  - HTTP Proxy Server—Lets you enter an HTTP proxy server IP address. You may need proxy servers to download global correlation updates if customer networks use proxy in their networks.
  - HTTP Proxy Port—Lets you enter the port number for the HTTP proxy server.
  - DNS Primary—Lets you enter the primary DNS server IP address.

**Caution** For automatic and global correlation updates to function, you must have either a DNS server or an HTTP proxy server configured at all times.

**Caution** DNS resolution is supported only for accessing the automatic update and global correlation update server.

- Allowed hosts/networks that can access the sensor—Lets you add ACLs:
  - Network—Specifies the IP address of the network you want to add to the access list.
  - Mask—Specifies the netmask of the network you want to add to the access list.

    **Note** If you change the sensor ACL entries, the IME may lose connection to the sensor when the changes are applied.
- Network Participation—Lets you chose to participate in sending data to the SensorBase Network and at which level you want to participate:
  - Off—No data is contributed to the SensorBase Network.
  - Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
  - Full—All data is contributed to the SensorBase Network.

## Add and Edit ACL Entry Dialog Boxes

You can configure the list of hosts or networks that you want to have access to your sensor. The following hosts must have an entry in the access list:

- Hosts that need to Telnet to your sensor.
- Hosts that need to use SSH with your sensor.
- Hosts, such as the IDM and the ASDM, that need to access your sensor from a web browser.
- Management stations, such as the CSM, that need access to your sensor.
- If your sensor is a master blocking sensor, the IP addresses of the blocking forwarding sensors must have an entry in the list.

### Field Definitions

The following fields are found in the Add and Edit ACL Entry dialog boxes:

- IP Address—Specifies the IP address of the host or network you want to have access to your sensor.
- Network Mask—Specifies the network mask of the host or network you want to have access to your sensor. The netmask for a single host is 32.

## Sensor Setup Wind

In the two Sensor Setup windows, you can configure the sensor for basic operation. Most of the fields will already be populated because you assigned the values during initialization. But you can change them here if needed.

### Field Definitions

- Current Sensor Date and Time—Sets the time and date for appliances that are not configured with an NTP server:
  - Date—Specifies the sensor local date. When you update the time and date, click **Apply Date/Time to Sensor** to have it go in to effect.
  - Apply Date/Time to Sensor—Immediately updates the time and date on the sensor.

  **Note** If you cancel the Startup Wizard, the date and time changes remain.

- Time Zone—Sets the zone name and UTC offset:
  - Zone Name—Specifies the local time zone when summertime is not in effect. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
  - Offset—Specifies the local time zone offset in minutes. The default is 0. If you select a predefined time zone this field is populated automatically.

  **Note** Changing the time zone offset requires the sensor to reboot.

- NTP Server—Lets you configure the sensor to use an NTP server as its time source:
  - IP Address—Specifies the IP address of the NTP server if you use this to set time on the sensor.
  - Authenticated NTP—Lets you use authenticated NTP, which requires a key and key ID.
  - Key—Specifies the NTP MD5 key type.
  - Key ID—Specifies the ID of the key (1 to 65535) used to authenticate on the NTP server. You receive an error message if the key ID is out of range.

  **Note** We recommend that you use an NTP server as the sensor time source.

- Summertime—Lets you configure the summer mode:
  - Enable Summertime—Check to enable summertime mode. The default is disabled.
  - Configure Summertime—Click to configure summertime settings.

## Configure Summertime Dialog Box

**Note** You must be administrator to configure time settings.

The following fields are found in the Configure Summertime dialog box:

- Summer Zone Name—Specifies the summertime zone name. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
- Offset—Specifies the number of minutes to add during summertime. The default is 60. If you choose a predefined time zone, this field is populated automatically.

  **Note** Changing the time zone offset requires the sensor to reboot.

- Start Time—Specifies the summertime start time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- End Time—Specifies the summertime end time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- Summertime Duration—Lets you set whether the duration is recurring or a single date:
  - Recurring—Specifies the duration is in recurring mode.
  - Date—Specifies the duration is in nonrecurring mode.
  - Start—Specifies the start week, day, and month setting.
  - End—Specifies the end week, day, and month setting.

## Configuring Sensor Settings

To configure sensor settings in the Startup Wizard, follow these steps:

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

**Step 2** Choose **Configuration >** ***sensor_name*** **> Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next**.

**Step 3** In the Host Name field, enter the sensor name.

**Step 4** In the IP Address field, enter the sensor IP address.

**Step 5** In the Subnet Mask field, enter the network mask address.

**Step 6** In the Gateway field, enter the default gateway address.

**Note** If you change the sensor network settings, the IME loses connection to the sensor when the changes are applied.

**Step 7** To configure either an HTTP proxy server or a DNS server to support automatic updates and global correlation, enter the HTTP proxy server IP address in the HTTP Proxy Server field and the port number in the HTTP Proxy Port field, or enter the DNS server IP address in the DNS Primary field. If you do not want to turn on global correlation, click **OK** on the following Warning dialog box:

```
Global correlation requires either an HTTP proxy server or at least one DNS server.
```

If you are using a DNS server, you must configure at least one DNS server and it must be reachable for automatic updates and global correlation updates to be successful. You can configure other DNS servers as backup servers. DNS queries are sent to the first server in the list. If it is unreachable, DNS queries are sent to the next configured DNS server.

**Caution** For automatic and global correlation updates to function, you must have either a DNS server or an HTTP proxy server configured at all times.

**Caution** DNS resolution is supported only for accessing the automatic update or global threat correlation update server.

**Step 8** To configure the hosts and networks that are allowed to access the sensor, click **Add**:

a. In the IP Address field, enter the IP address of the host you want to have access to the sensor.

b. In the Network Mask field, enter the network mask address of the host you want to have access to the sensor.

c. Click **OK**.

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

**Step 9** To enable network participation, select the degree of network participation that you want:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network.

**Note** The default is Off. If you chose Partial or Full, you must agree to the Network Participation Disclaimer.

**Tip** To discard your changes and close the Sensor Setup window, click **Cancel**.

**Step 10** Click **Next** to continue to the next Setup window.

**Step 11** Under Current Sensor Date and Time, select the current date and time from the drop-down calendar, and then click **OK**, and then click **Apply Date/Time to Sensor**. Date and time indicate the date and time on the local host.

**Caution** If you accidentally specify the incorrect time, stored events have the wrong time stamp. You must clear the events.

**Note** If you cancel the Startup Wizard, the date and time changes remain.

**Note** You cannot change the date or time on IPS modules or if you have configured NTP.

**Step 12** Under Time Zone, configure the time zone and offset:

**a.** In the Zone Name field, choose a time zone from the drop- down list, or enter one that you have created. This is the time zone to be displayed when summertime hours are not in effect.

**b.** In the Offset field, enter the offset in minutes from UTC. If you choose a predefined time zone name, this field is automatically populated.

**Note** Changing the time zone offset requires the sensor to reboot.

**Step 13** If you are using NTP synchronization, under NTP Server enter the following:

- The IP address of the NTP server in the IP Address field.
- If using authenticated NTP, check the **Authenticated NTP** check box, and then enter the key of the NTP server in the Key field, and the key ID of the NTP server in the Key ID field.

**Note** If you define an NTP server, the sensor time is set by the NTP server. The CLI **clock set** command produces an error, but time zone and daylight saving time parameters are valid.

**Step 14** To enable daylight saving time, check the **Enable Summertime** check box, and then click **Configure Summertime**.

**Step 15** Choose the Summer Zone Name from the drop-down list or enter one that you have created. This is the name to be displayed when daylight saving time is in effect.

**Step 16** In the Offset field, enter the number of minutes to add during summertime. If you choose a predefined summer zone name, this field is automatically populated.

**Step 17** In the Start Time field, enter the time to apply summertime settings.

**Step 18** In the End Time field, enter the time to remove summertime settings.

**Step 19** Under Summertime Duration, choose whether summertime settings will occur on specified days each year (recurring) or whether they will start and end on specific dates (date):

**a.** Recurring—Choose the Start and End times from the drop-down lists. The default is the second Sunday in March and the first Sunday in November.

**b.** Date—Choose the Start and End time from the drop-down lists. The default is January 1 for the start and end time.

**Step 20** Click **OK**.

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

**Step 21** Click **Next** to continue through the Startup Wizard.

**Note** Changing the network settings may disrupt your connection to the sensor and force you to reconnect with the new address.

# Configuring Interfaces

**Note** You cannot use the Startup Wizard to configure interfaces and virtual sensors for the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP.

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

- Interface Summary Window, page 5-8
- Restore Defaults to an Interface Dialog Box, page 5-9
- Traffic Inspection Mode Window, page 5-9
- Interface Selection Window, page 5-10
- Inline Interface Pair Window, page 5-10
- Inline VLAN Pairs Window, page 5-10
- Add and Edit Inline VLAN Pair Entry Dialog Boxes, page 5-11
- Configuring Inline VLAN Pairs, page 5-11

## Interface Summary Window

The Interface Summary window displays the existing interface configuration settings. If an interface is not assigned to a virtual sensor, the Assigned Virtual Sensor column reads “None” and the Details column reads “Backplane” for platforms that have backplane interfaces. The details column reads “Promiscuous” for all other platforms. An interface can be either physical or logical. A physical interface can also be part of a logical interface and can be further subdivided.

**Note** The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) all have backplane interfaces.

**Note** You can configure one physical or logical interface during each Startup Wizard session. To configure multiple interfaces, run Startup Wizard multiple times.

You can specify interface configuration in one of five types:

- Promiscuous
- Promiscuous VLAN group (a subinterface)
- Inline interface pair
- Inline interface pair VLAN group (a subinterface)
- Inline VLAN pair (a subinterface)

**Note** VLAN groups are not supported in the Startup Wizard.

**Caution** You can configure any single physical interface to run in promiscuous mode, inline pair mode, or inline VLAN pair mode, but you cannot configure an interface in a combination of these modes.

You can click **Finish** to exit the Startup Wizard on this window and commit your changes, or you can continue to configure interfaces and virtual sensors.

### Field Definitions

The following fields are found in the Interface Summary window:

- Name—Displays the name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
- Details—Tells you whether the interface is promiscuous, inline, or backplane and whether there are VLAN pairs.
- Assigned Virtual Sensor—Tells you whether the interface or interface pair has been assigned to a virtual sensor.
- Enabled—Tells you whether this interface is enabled or disabled.
- Description—Displays your description of the interface.

## Restore Defaults to an Interface Dialog Box

The Restore Default Interface dialog box displays all of the interfaces that are configured or assigned to a virtual sensor. You can select any of the interfaces to be restored. If the selected interface is assigned to a virtual sensor, it is unassigned. If you select an inline interface pair, both physical interfaces are restored to the default and the logical interface is deleted. You cannot select and restore defaults to an inline VLAN pair or VLAN group.

**Caution** You can only restore defaults to physical interfaces and inline interface pairs.

## Traffic Inspection Mode Window

The Traffic Inspection Mode window lets you configure the sensor interfaces as promiscuous, inline interface, or inline VLAN pair mode. If the sensor only has one physical interface, the Inline Interface Pair Mode radio button is disabled. If the sensor does not support inline VLAN pair mode, that option is also disabled.

The following radio buttons are found on the Traffic Inspection Mode window:

- (Keep existing interface configuration)—No changes are made to the interface configuration of the sensor.
- Promiscuous—The sensor is not in the data path of the inspected packets. The sensor cannot modify or drop packets.
- Inline Interface Pair—The sensor is in the data path of the inspected packets. The sensor can modify or drop inspected packets. For inline interface inspection, you must pair two physical interfaces together.

- Inline VLAN Pair—The sensor is in the data path of the inspected packets. The sensor can modify or drop inspected packets. For inline VLAN inspection, you must have one physical interface and an even number of VLANs and the interface must be connected to a trunk port.

## Interface Selection Window

On the Interface Selection window, you can choose which interface you want to configure.

**Note** You can configure one physical or logical interface during each Startup Wizard session. To configure multiple interfaces, run Startup Wizard multiple times.

## Inline Interface Pair Window

In the Inline Interface Pair window, you can assign an interface name for two unique interfaces. If your sensor supports hardware bypass, an icon identifies that. If you pair a hardware bypass interface with an interface that does not support hardware bypass, you receive a warning message indicating that hardware bypass is not available.

**Note** Hardware bypass interfaces allow packet flow to continue even if power is disrupted.

### Field Definitions

The following fields are found on the Inline Interface Pair window:

- Inline Interface Name—Lets you assign a name to this inline interface pair.
- First Interface of Pair—Lets you assign the first interface of this pair.
- Second Interface of Pair—Lets you assign the other interface of this pair.

## Inline VLAN Pairs Window

**Note** For the IPS 4500, series sensors the maximum number of inline VLAN pairs you can create system-wide is 150. On all other platforms, the limit is 255 per interface.

If you checked the Inline VLAN Pair Mode radio button in the Interface Inspection Mode window, you can configure inline VLAN pairs on the Inline VLAN Pairs window. If you have already configured inline VLAN pairs, they appear in the table, and you can edit or delete them.

**Note** You cannot create an inline VLAN pair for an interface that has already been paired with another interface or for an interface that is in promiscuous mode and assigned to a virtual sensor.

To create an inline VLAN pair for an interface that is in promiscuous mode, you must remove the interface from the virtual sensor and then create the inline VLAN pair. You can only pair interfaces that are available.

**Note** If your sensor does not support inline VLAN pairs, the Inline VLAN Pairs window is not displayed. The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

### Field Definitions

The following fields are found in the Inline VLAN Pairs window:

- Subinterface Number—Displays the subinterface number of the inline VLAN pair. The value is 1 to 255.
- VLAN A—Displays the VLAN number for the first VLAN. The value is 1 to 4095.
- VLAN B—Displays the VLAN number for the second VLAN. The value is 1 to 4095.
- Interface—Displays the name of the inline VLAN pair.
- Virtual Sensor—Displays the name of the virtual sensor for this inline VLAN pair.
- Description—Displays your description of the inline VLAN pair.

## Add and Edit Inline VLAN Pair Entry Dialog Boxes

**Note** You cannot pair a VLAN with itself.

**Note** The subinterface number and the VLAN numbers should be unique to each physical interface.

The following fields are found in the Add and Edit Inline VLAN Pair Entry dialog boxes:

- Subinterface Number—Lets you assign a subinterface number. You can assign a number from 1 to 255.
- VLAN A—Lets you specify the first VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- VLAN B—Lets you specify the other VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- Description—Lets you add a description of this inline VLAN pair.

## Configuring Inline VLAN Pairs

To configure inline VLAN pairs in the Startup Wizard, follow these steps:

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

**Step 2** Choose **Configuration >** ***sensor_name*** **> Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next**. until you get to the Traffic Inspection Mode window.

**Step 3** Click the **Inline VLAN Pair Mode** radio button, click **Next,** and then click **Add**.

**Step 4** In the Subinterface Number field, enter a subinterface number (1 to 255) for the inline VLAN pair.

**Step 5** In the VLAN 1 field, specify the first VLAN (1 to 4095) for this inline VLAN pair.

**Step 6** In the VLAN 2 field, specify the other VLAN (1 to 4095) for this inline VLAN pair.

**Step 7** In the Description field, add a description of the inline VLAN pair if desired.

**Tip** To discard your changes and close the Add Inline VLAN Pair dialog box, click **Cancel**.

**Step 8** Click **OK**. The new inline VLAN pair appears in the list in the Inline VLAN Pairs window.

**Step 9** To edit an inline VLAN pair, select it, and click **Edit**.

**Step 10** You can change the subinterface number, the VLAN numbers, or edit the description.

**Tip** To discard your changes and close the Edit Inline VLAN Pair dialog box, click **Cancel**.

**Step 11** Click **OK**. The edited VLAN pair appears in the list in the Inline VLAN Pairs window.

**Step 12** To delete a VLAN pair, select it, and click **Delete**. The VLAN pair no longer appears in the list in the Inline VLAN Pairs window.

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

**Step 13** Click **Apply** to apply your changes and save the revised configuration.

# Configuring Virtual Sensors

This section describes how to configure virtual sensors, and contains the following topics:

- Virtual Sensors Window, page 5-12
- Add Virtual Sensor Dialog Box, page 5-13
- Adding a Virtual Sensor, page 5-14

## Virtual Sensors Window

The Virtual Sensors window of the Startup Wizard shows the interfaces and security policies that have been assigned to the virtual sensors. You can assign the default block policy and select a risk category for that virtual sensor.

If you have a sensor that supports multiple virtual sensors, after you have configured interfaces, you assign them to a virtual sensor in the Virtual Sensors window of the Startup Wizard. By default, the interface is assigned to virtual sensor vs0. You can assign the interface to any existing virtual sensor or you can create a new virtual sensor. To create a virtual sensor, click **Create a Virtual Sensor**. The Add Virtual Sensor dialog box appears and you can configure a virtual sensor.

**Note** The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not have configurable interfaces; therefore, you must use the default virtual sensor. You cannot create a new virtual sensor using the Startup Wizard and you will not see the fields for creating a new virtual sensor.

### Field Definitions

The following fields are found in the Virtual Sensors window:

- IPS Policy Summary—Displays the assigned interfaces with assigned policies:
  - Name—Displays the name of the virtual sensor. The default virtual sensor is vs0.
  - Interfaces—Lists the interfaces that you want to assign to a virtual sensor.
  - Signature Policy—Displays the name and threat profile of the signature policy. The default signature policy is sig0. The default threat profile is None.
  - Event Action Policy—Displays the name of the event action policy. The default event action policy is rules0.
  - Anomaly Detection Policy—Displays the name of the anomaly detection policy. The default anomaly detection policy is ad0.

    **Note** Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

  - Description—Displays the description of the virtual sensor.
- Virtual Sensor Assignments—Lets you assign interfaces and create a virtual sensor for appliances; for modules, the default virtual sensor, vs0, is already assigned.
  - Interface(s)—Lists the available interfaces.
  - Assign Interface to Virtual Sensor—Lists the available virtual sensors. The default sensor is vs0.
  - Create a Virtual Sensor—Displays the Add Virtual Sensor dialog where you can create a virtual sensor with new signature, event action rules, and anomaly detection policies, or you can use the default policies.
- Default Block Policy—Lets you select a risk category for this virtual sensor:
  - Select Virtual Sensor—Lets you choose a virtual sensor to apply the default block policy to. If your sensor does not support virtualization, you will see only vs0 (the default virtual sensor) as a choice.
  - Select a Risk Category—Displays the default risk category used in the deny event action override. Alerts with a risk rating of 90-100 are denied by default. If you do not want to use the default risk category, you can edit the HIGHRISK risk category, or create a new risk category in **Configuration >** ***sensor_name*** **> Policies > IPS Policies > Event Action Rules > rules0 > Risk Category**.

## Add Virtual Sensor Dialog Box

In the Add Virtual Sensor dialog box, you can create a new signature policy, event action rules policy, and anomaly detection policy, but you cannot configure them. You create the new policy by cloning the default policy. To configure the new policy:

- For new signature policies, choose **Configuration >** ***sensor_name*** **> Policies > Signature Definitions >** ***NewSigPolicy*** **> Active Signatures**.
- For new event action rules policies, choose **Configuration >** ***sensor_name*** **> Policies > Event Action Rules >** ***NewRulesPolicy***.

- For new anomaly detection policies, choose **Configuration >** ***sensor_name*** **> Policies > Anomaly Detections >** ***NewADPolicy***.

  **Note** Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

### Field Definitions

The following fields are found in the Add Virtual Sensor dialog box:

- Virtual Sensor name—Lets you assign a name to the virtual sensor.
- Description—Lets you add a description of the virtual sensor.
- Assign a Signature Policy—Lets you assign a signature policy:
  - Assign a Signature Policy—Lets you assign a signature policy that has already been created.
  - Create a Signature Policy—Lets you create a new signature policy.
- Assign an Event Action Rules Policy—Lets you assign an event action rules policy:
  - Assign an Event Action Rules Policy—Lets you assign an event action rules policy that has already been created.
  - Create an Event Action Rules Policy—Lets you create a new event action rules policy.
- Assign an Anomaly Detection Policy—Lets you assign an anomaly detection policy:
  - Assign an Anomaly Detection Policy—Lets you assign an anomaly detection policy that has already been created.
  - Create an Anomaly Detection Policy—Lets you create a new anomaly detection policy.

    **Note** Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

## Adding a Virtual Sensor

To add a virtual sensor using the Startup Wizard, follow these steps:

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

**Step 2** Choose **Configuration >** ***sensor_name*** **> Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next** until you get to the Virtual Sensors window.

**Step 3** Click **Create a Virtual Sensor**.

**Step 4** In the Virtual Sensor name field, enter the virtual sensor name.

**Step 5** In the Description field, enter a description that will help you identify this virtual sensor.

**Step 6** Assign a signature policy by doing one of the following:

**a.** Click the **Assign a Signature Policy** radio button and chose a signature policy from the drop-down list.

**b.** Click the **Create a Signature Policy** radio button and enter a name for the signature policy in the field.

**Note** To configure the new signature policy, choose **Configuration >** ***sensor_name*** **>Policies > IPS Policies > Signature Definitions >** ***NewSigPolicy*** **> Active Signatures**.

**Step 7** Assign an event action rules policy by doing one of the following:

**a.** Click the **Assign an Event Action Rules Policy** radio button and chose an event action rules policy from the drop-down list.

**b.** Click the **Create an Event Action Rules Policy** radio button and enter a name for the event action rules policy in the field.

**Note** To configure the new event action rules policy, choose **Configuration >** ***sensor_name*** **>Policies > Event Action Rules >** ***NewRulesPolicy***.

**Step 8** Assign an anomaly detection policy by doing one of the following:

**a.** Click the **Assign an Anomaly Detection Policy** radio button and chose an anomaly detection policy from the drop-down list.

**b.** Click the **Create an Anomaly Detection Policy** radio button and enter a name for the anomaly detection policy in the field.

**Note** Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

**Note** To configure the new anomaly detection policy, click **Configuration >** ***sensor_name*** **> Policies > IPS Policies > Anomaly Detections >** ***NewADPolicy***.

**Step 9** Click **Finish**, and then in the Confirm Configuration Changes dialog box, click **Yes** to save your changes.

# Applying Signature Threat Profiles

**Note** You must be administrator or operator to configure signature threat profiles.

**Note** Signature threat profiles are supported on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP.

In the Signatures window, the threat profiles (specific signature templates) that have been applied to individual signature policies are displayed and you can change threat profiles by clicking the existing threat profile and choosing another. A signature threat profile is a predefined signature template that includes customized tunings. These tunings adjust the signature coverage and response actions to enable the sensor to make better choices in various deployment and threat scenarios. You can apply a signature threat profile to one or more signature policies.

You can dynamically upgrade threat profiles through signature upgrades. You can see a description of the template when you select it. Threat profiles may tune several signatures and when these signature policies are assigned to virtual sensors, depending on the signatures turned ON in the threat profile, there may be increased usage of the resources of the sensor. Furthermore, based on the traffic pattern of your network, these signatures may be further tuned.

Once you apply a signature template to a signature policy, you can make modifications to the signature policy, such as retiring a signature to eliminate a false positive. Your changes are NOT overwritten during signature updates or sensor software upgrades.

The following threat profiles are part of the signature upgrades:

- Supervisory Control and Data Acquisition (SCADA)—In addition to signatures in the default set, the SCADA signature template includes specialized signatures for general SCADA protocol detections and specific identifiers that address tools and environments common to most device controlled environments. Use this template if the Cisco IPS is primarily used for protecting Industrial Control Systems (ICS).

**Caution** You must purchase a SCADA signature license to use the SCADA threat profile. For more information refer to the following URL: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/ips_industrial_control_protection.pdf

- Edge—In addition to signatures in the default set, the Internet Edge signature template includes additional signatures that provide broader protection for desktop operating systems, web browsers, web technologies, and common desktop applications. Use this template if the Cisco IPS is primarily used for securing an Internet connection.
- Web Applications—In addition to signatures in the default set, the Web Applications signature template includes additional signatures that provide broader protection for web servers, web development tools and frameworks, content management systems, load balancers, and databases. Use this template if the Cisco IPS is primarily used for protecting web server farms.
- Data Center—In addition to signatures in the default set, the Data Center signature template includes additional signatures that provide broader protection for server operating systems, web servers, application servers, databases, content management systems, messaging servers, and virtualization systems. Use this template if the Cisco IPS is primarily used for protecting data centers.

### Field Definitions

The following fields are found on the Signatures window of the Startup Wizard:

- Policy Name—Displays the names of the signature policies.

  You create and configure signature policies at **Configuration > Policies > Signature Definitions > Add**. Those signature policies are displayed here.
- Threat Profile—Displays the threat profile that has been applied:
  - SCADA—Default signature set plus SCADA-specific signatures, that is, signatures for protecting Industrial Control Systems (ICS).

**Caution** You must purchase a SCADA signature license to use the SCADA threat profile. For more information refer to the following URL: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/ips_industrial_control_protection.pdf

- Edge—Default signature set plus signatures that help in securing an Internet connection.
- Web_Applications—Default signature set plus signatures for protecting web server farms.
- Data_Center—Default signature set plus signatures for protecting data centers.

### Applying Signature Threat Profiles

To apply signature threat profiles to signature policies using the Startup Wizard, follow these steps:

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

**Step 2** Choose **Configuration >** ***sensor_name*** **> Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next** until you get to the Signatures window.

**Step 3** Under IPS Signature Policies, from the Policy Name list, select the signature policy to which you want to apply a signature threat profile.

**Step 4** Under Threat Profile, click the down arrow next to the threat profile to display the drop-down list, and select one of the following signature templates:

- SCADA—Default signature set plus SCADA-specific signatures, that is, signatures for protecting Industrial Control Systems (ICS).

**Caution** You must purchase a SCADA signature license to use the SCADA threat profile. For more information refer to the following URL:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/ips_industrial_control_protection.pdf

- Edge—Default signature set plus signatures that help in securing an Internet connection.
- Web_Applications—Default signature set plus signatures for protecting web server farms.
- Data_Center—Default signature set plus signatures for protecting data centers.

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

**Step 5** Click **Next** to continue with the Startup Wizard, or click **Finish** to exit, and then click **Yes** to save your changes.

# Configuring Auto Update

You can configure the sensor to automatically download signature and signature engine updates from Cisco.com. 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** The sensor does not support communication with Cisco.com through nontransparent proxy servers.

**Note** Automatic update requires either an HTTP proxy server or at least one DNS server to function.

### Field Definitions

The following fields are found on the Auto Update window of the Startup Wizard:

- Enable Signature and Engine Updates from Cisco.com—Lets the sensor go to Cisco.com to download signature and engine updates and install them on the sensor.

  **Note** You must check the **Enable Signature and Engine Updates from Cisco.com** check box to enable the fields.

- Cisco.com Access—Lets you specify the following options for the Cisco.com server:
  - Username—Specifies the username corresponding to the user account on Cisco.com.
  - Password—Specifies 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 daily start time:
  - Start Time—Specifies the time to start the update process in 24-hour clock time. This is the time when the sensor will contact Cisco.com and download any new updates.

### Configuring Auto Update

**Note** Automatic update requires either an HTTP proxy server or at least one DNS server to function. Make sure that you have a server configured on Configuration > Startup Wizard > Sensor Setup (Step 2 of ...).

To configure automatic updates from Cisco.com, follow these steps:

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

**Step 2** Choose **Configuration >** ***sensor_name*** **> Sensor Setup > Startup Wizard > Auto Update**.

**Step 3** 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. In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss using the 24-hour clock. The updates occur daily.

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

**Step 4** Click **Finish** to save your changes.

### For More Information

- For the procedure for obtaining software and an account with cryptographic privileges, see Obtaining Cisco IPS Software, page 25-1.
- For a list of the supported FTP and HTTP servers, see Supported FTP and HTTP Servers, page 19-21.
- To configure UNIX-style directory listings for downloading automatic updates, see UNIX-Style Directory Listings, page 19-21.
- For information about the time is takes to install signature updates, see Signature Updates and Installation Time, page 19-21.