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

Because IME cannot communicate with an unconfigured sensor, you must log in to the sensor CLI and run the **setup** command to configure communication parameters. The AIP SSM is an exception. You can initialize it from ASDM.

You can use the Startup Wizard to set up a sensor and to modify a sensor that has already been configured. You cannot use it for initializing a new, unconfigured sensor. You must use the **setup** command for that. Until you initialize the sensor with the **setup** command, 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 settings, configure interfaces, create virtual sensors, 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 cannot see that configuration window.

Note VLAN groups are not supported in the Startup Wizard.

The IPS modules do not support the following features:

- AIM IPS and NME IPS—Inline interface pairs, VLAN groups, virtualization, or setting the time.
- AIP SSM—Inline VLAN pairs, inline interface pairs, VLAN groups, setting the time, or interface configuration (you must configure interfaces on the adaptive security appliance).

- IDSM2—VLAN groups for inline interface pairs or setting the time.

Note The IPS modules get their time settings from the router, switch, or adaptive security appliance in which they are installed.

For More Information

- For the procedure for using the **setup** command to initialize the sensor, see Chapter 23, "Initializing the Sensor."
- For detailed information on interface configuration restrictions, see Interface Configuration Restrictions, page 7-8.

Setting up the Sensor

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

Sensor Setup Window

In the 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:

- Host Name—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—IP address of the sensor. The default is 192.168.1.2.
- Subnet Mask—Mask corresponding to the IP address. The default is 255.255.255.0.
- Gateway—Default gateway address. The default is 192.168.1.1.
- HTTP Proxy Server—Lets you enter a 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 proxy server.
- DNS Primary—Lets you enter the primary DNS server IP address.
- DNS Secondary—Lets you enter the secondary DNS server IP address.

- DNS Tertiary—Lets you enter tertiary DNS server IP address.

  If you are using a DNS server, you must configure at least one DNS server and it must be reachable for 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 global correlation 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 global correlation update server.

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

  Note If you change the sensor ACL entries, IME may lose connection to the sensor when the changes are applied.

- Current Sensor Date and Time—Sets the time and date for appliances that are not configured with an NTP server.
  - Date—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—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—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—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—NTP MD5 key type.
  - Key ID—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.

- Summertime
  - Enable Summertime—Check to enable summertime mode. The default is disabled.
  - Configure Summertime—Click to configure summertime settings.

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 IDM and ASDM, that need to access your sensor from a web browser.
- Management stations, such as 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—The IP address of the host or network you want to have access to your sensor.
- Network Mask—The network mask of the host or network you want to have access to your sensor.

  The netmask for a single host is 32.

Configure Summertime Dialog Box

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

- Summer Zone Name—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—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—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—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—Duration is in recurring mode.
  - Date—Duration is in nonrecurring mode.
  - Start—Start week, day, and month setting.
  - End—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 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, IME loses connection to the sensor when the changes are applied.

Step 7 To configure either an HTTP proxy server or at least one DNS server to support 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 are using a DNS server, you must configure at least one DNS server and it must be reachable for 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 global correlation 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 global 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 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 10 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 11 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 12 To enable daylight saving time, check the **Enable Summertime** check box, and then click **Configure Summertime**.

Step 13 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 14 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.

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

Step 15 In the Start Time field, enter the time to apply summertime settings.

Step 16 In the End Time field, enter the time to remove summertime settings.

Step 17 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 18 Click **OK**.

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

Step 19 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 AIM IPS, AIP SSM, or NME IPS.

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

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 “Unassigned” and the Details column reads “Promiscuous.” 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 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—Name of the interface. The values are FastEthernet or GigabitEthernet for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
- Details—Tells you whether the interface is promiscuous or inline and whether there are VLAN pairs.
- Assigned Virtual Sensor—Whether the interface or interface pair has been assigned to a virtual sensor.
- Enabled—Whether this interface is enabled or disabled.
- Description—Your description of the interface.

Restore Defaults to an Interface Dialog Box

The Restore Default Interface dialog box displays all 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, such as the AIM IPS, 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:

- Promiscuous Mode

  The sensor is not in the data path of the inspected packets. The sensor cannot modify or drop packets.

- Inline Interface Pair Mode

  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 Mode

  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. 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

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 AIM IPS, and NME IPS do not support inline VLAN pairs.

Note You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

Field Definitions

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

- Subinterface—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—Name of the inline VLAN pair.
- Virtual Sensor—Name of the virtual sensor for this inline VLAN pair.
- Description—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 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, and 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

Note The AIM IPS, AIP SSM, and NME IPS do not have configurable interfaces; therefore you must use the default virtual sensor.

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 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.

Field Definitions

The following fields are found in the Virtual Sensors window:

- Interface(s)—Lists the interface(s) that you want to assign to a virtual sensor.
- 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.
- IPS Policy Summary Information—Displays the assigned interfaces with assigned policies.
- Default Block Policy—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 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 signature policy, event action rules policy, and anomaly detection policy, but you cannot configure them. You create the policy by cloning the default policy.

To configure the new policy:

- For new signature policies, choose **Configuration > *sensor_name* > Policies > Signature Definitions > *NewSigPolicy* > All 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***.

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
  - Assign an Existing Signature Policy—Lets you assign a signature policy that has already been created.
  - Create a New Signature Policy—Lets you create a signature policy;
- Assign and Event Action Rules Policy
  - Assign an Existing Event Action Rules Policy—Lets you assign an event action rules policy that has already been created.

  - Create a New Event Action Rules Policy—Lets you create a event action rules policy.
- Assign an Anomaly Detection Policy
  - Assign an Existing Anomaly Detection Policy—Lets you assign an anomaly detection policy that has already been created.
  - Create a New Anomaly Detection Policy—Lets you create an anomaly detection policy.

Adding a Virtual Sensor

To add a virtual sensor using the Startup Wizard, 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 > 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 choose 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* > All 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 choose 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 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 **OK** to save your changes.