



CHAPTER 4

Cisco IPS 6.x and 7.x Devices and Virtual Sensors

This chapter describes how to prepare a Cisco IPS 6.x and 7.x devices and any configured virtual sensors to act as a reporting devices to Cisco Secure MARS.

This chapter contains the following topics:

- [Bootstrap the Cisco Sensor, page 4-1](#)
- [Add and Configure a Cisco IPS 6.x or 7.x Device in MARS, page 4-3](#)
- [Verify that MARS Pulls Events from a Cisco IPS Device, page 4-6](#)
- [IPS Signature Dynamic Update Settings, page 4-6](#)
- [Applying Custom Signature Updates, page 4-8](#)

Bootstrap the Cisco Sensor

Preparing a sensor to be monitored by MARS involves preparing the sensor so MARS can communicate with it and ensuring that the correct data is being generated.

This section contains the following topics:

- [Cisco IPS 5.x, 6.x, and 7.x Software, page 4-1](#)
- [View Detailed Event Data for Cisco IPS Devices, page 4-2](#)

Cisco IPS 5.x, 6.x, and 7.x Software

For Cisco IPS 5.x, 6.x, and 7.x devices, MARS pulls the logs using SDEE over SSL. Therefore, MARS must have HTTPS access to the sensor. To prepare the sensor, you must enable the HTTP server on the sensor, enable TLS to allow HTTPS access, and make sure that the IP address of MARS is defined as an allowed host, one that can access the sensor and pull events. If the sensors have been configured to allow access from limited hosts or subnets on the network, you can use the **access-listip_address/netmask** command to enable this access.

View Detailed Event Data for Cisco IPS Devices

In addition to the alert message, you can view the trigger packets and IP log data associated with incidents reported by Cisco IDS 4.x and Cisco IPS 5.x, 6.x, and 7.x devices, whether they are sensor appliances or modules. This information is useful when an in-depth understanding of the attack method is desired. MARS includes two event types that focus on these two data types:

- **Trigger packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. The trigger packet provides a single data packet—the data packet that caused the alarm to fire.
- **Packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. Although the amount of data contained in an IP log varies based on sensor configuration, by default an IP log contains 30 seconds of packet data. To view this data, you must enable the Pull IP Logs option on the Cisco IPS device under Admin > System Setup > Security and Monitor Devices.

For the correct signature settings required to generate this data, see [Enable the Correct Signatures and Actions, page 4-2](#).

If the IP log feature is enabled for the reporting Cisco IPS device, these event types are combined as part of the incident data. You can view this data by drilling down in an incident, expanding the desired event type (either Packet Data or Trigger Packet Data), selecting an event, and clicking on the RAW Events for this Session icon under the Reporting Device column of that event. The source, destination, and other data displayed for these events matches that of the original alert. In addition, this data appears hexadecimal and binary format.



Note

The trigger packet and IP log data is stored using a base64-encoded format in the MARS database. Therefore, keyword search does not work on it if you just provide the search string.

Enable the Correct Signatures and Actions

If the signature actions are correctly configured, MARS can display the trigger packet information for the first event that fires a signature on a Cisco IDS or IPS device. MARS is also able to pull the IP log data from Cisco IDS and IPS devices, however, this operation is system intensive. Therefore, you should select the set of signatures that generate IP log data carefully.

When configuring the active signatures on a Cisco IDS or IPS device, you must specify the alert action and the action that generates the desired data:

- To view trigger packets, you must enable the “produce-verbose-alert” action.
- To view IP logs, you must enable the alert or “produce-verbose-alert” action and the “log-pair-packets” action.



Caution

Configuring IP logging and verbose alerts on the sensor is system intensive and does affect the performance of your sensor. In addition, it affects the performance of your MARS Appliance. Because of these effects, you be cautious in configuring signatures to generate IP logs.

Add and Configure a Cisco IPS 6.x or 7.x Device in MARS

When you define a Cisco IPS 6.x or 7.x device in MARS, you can discover any virtual sensors configured on the device. Discovering these virtual sensors allows MARS to separate the reported events by virtual sensor. It also allows you to tune the list of monitored networks to each virtual sensor, improving the accuracy of the desired reporting.

To add and configure a Cisco IPS 6.x or 7.x device in MARS, follow these steps:

- Step 1** Click **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** Select **Cisco IPS 6.x** or **Cisco IPS 7.x** from the Device Type list.

Figure 4-1 Configure Cisco IPS 6.x

Device Type: Cisco IPS 6.x

→ *Device Name:

→ Reporting IP:

→ *Access Type: SSL

 Login:

 Password:

 Port:

→ Monitor Resource Usage: NO

 Pull IP Logs: NO

- Step 3** Enter the hostname of the sensor in the Device Name field.
The Device Name value must be identical to the configured sensor name.
- Step 4** Enter the administrative IP address in the Reporting IP field.
The Reporting IP address is the same address as the administrative IP address.
- Step 5** In the Login field, enter the username associated with the administrative account that will be used to access the reporting device.
- Step 6** In the Password field, enter the password associated with the username specified in the Login field.
- Step 7** In the Port field, enter the TCP port on which the webserver running on the sensor listens. The default HTTPS port is 443.



Note While it is possible to configure HTTP only, MARS requires HTTPS.

- Step 8** Verify that **NO** is selected in the Monitor Resource Usage list.
While the Monitor Resource Usage option appears on this page, it does not function for Cisco IPS.
- Step 9** (Optional) To pull the IP logs from the sensor, select **Yes** from the Pull IP Logs list.

This setting applies to the entire sensor, including those logs generated for virtual sensors alerts. For details on this setting, see [View Detailed Event Data for Cisco IPS Devices, page 4-2](#).

Step 10 To verify the configuration and enable the discovery of virtual sensors, click **Test Connectivity**.

Step 11 To discover any defined virtual sensors, click **Discover**.



Tip MARS is unaware of changes made to the sensor. Anytime you make changes to the virtual sensor settings, you must click **Discover** on that sensor configuration page to refresh the virtual sensor details in MARS.

Any virtual sensors are discovered.

Device Type: Cisco IPS 6.x

→ *Device Name:	<input type="text" value="test4260"/>
→ Reporting IP:	<input type="text" value="10"/> <input type="text" value="89"/> <input type="text" value="178"/> <input type="text" value="218"/>
→ *Access Type:	SSL
Login:	<input type="text" value="cisco"/>
Password:	<input type="password" value="*****"/>
Port:	<input type="text" value="443"/>
→ Monitor Resource Usage:	<input type="button" value="NO"/> ▼
Pull IP Logs:	<input type="button" value="NO"/> ▼

<input type="button" value="Discover"/>	<input type="button" value="Edit"/>
<input type="checkbox"/>	<input type="checkbox"/>
Virtual Sensor Name	Monitoring Networks
<input checked="" type="checkbox"/> test4260/vs0	

251172

Step 12 To define the monitored networks for each virtual sensor, select the checkbox next to the Virtual Sensor Name and click **Edit**.

The IPS Module page appears.

Device Type: Cisco IPS 6.x

→ *Device Name:

[Optional: for attack path calculation and mitigation enter monitoring networks information]

→ Monitored Networks:

Select a Network:

Define a Network:

Network IP:

Mask:

251173

- Step 13** (Optional) For attack path calculation and mitigation, specify the networks being monitored by the sensor. To manually define the networks, select the **Define a Network** radio button.
- Enter the network address in the Network IP field.
 - Enter the corresponding network mask value in the Mask field.
 - Click **Add** to move the specified network into the Monitored Networks field.
 - Repeat as needed.
- Step 14** (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.
- Select a network from in the Select a Network list.
 - Click **Add** to move the specified network into the Monitored Networks field.
 - Repeat as needed.
- Step 15** (Optional) Repeat [Step 12](#) through [Step 14](#) for each virtual sensor.
- Step 16** To save your changes, click **Submit**.

The device name appears under the Security and Monitoring Information list. The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

- Step 17** To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to sessionize events generated by this module and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).

Verify that MARS Pulls Events from a Cisco IPS Device

**Note**

If the Test Connectivity operation does not fail when configuring a Cisco IPS device in the MARS web interface, then communications are enabled. This task allows you to further verify the alerts are generated and pulled correctly.

It is common to create benign events on the network to verify the data flow. To verify the data flow between a Cisco IPS device and MARS, perform the following tasks:

1. On the Cisco IPS device, enable and alert on the signatures 2000 and 2004. The signatures monitor ICMP messages (pings).
2. Ping a device on the subnet on which the Cisco IPS device is listening. The events are generated and pulled by MARS.
3. Verify that the events appear in the MARS web interface. You can perform a query using the Cisco IPS device.
4. Once the dataflow is verified, you can disable the 2000 and 2004 signatures on the Cisco IPS device.

IPS Signature Dynamic Update Settings

In releases 6.0 and later, Cisco IPS supports dynamic signature updates. MARS can discover the new signatures and correctly process and categorize received events that match those signatures. If this feature is not configured, the events appears as unknown event type in queries and reports, and MARS does not include these events in inspection rules. These updates provides event normalization and event group mapping, and they enable your MARS Appliance to parse Day Zero signatures from the IPS devices.

The downloaded update information is an XML file that contains the IPS signatures. However, this file does not contain detailed information, such as vulnerability information. Detailed signature information is provided in later MARS signature upgrade packages just as with 3rd-party signatures.

**Note**

The dynamic IPS signature updates is an aspect of the version of software running on a MARS Appliance. Therefore, in addition to running the same MARS software versions on the Global Controller and Local Controller, the IPS signature version must match or the communications fail. To check the version, click **Help > About**.

Before You Begin

- Dynamic IPS signature updates are disabled by default.
- Custom IPS signatures are not supported. You must manually import these signatures using the process defined in [Applying Custom Signature Updates, page 4-8](#).
- You can retrieve updates from CCO or from a local web server. After downloading and installing an update, the MARS Appliance performs an auto-activate to load the new signature information.
- If configured to retrieve the signatures from CCO, MARS downloads the most recent package as determined by a combination of package name and the MD5 sum.
- MARS checks for updates at the specified interval, hourly (1, 2, 3, 6, or 12) or daily (1 through 14).

- In a Global Controller-Local Controller deployment, configure the dynamic signature URL and all relevant settings on the Global Controller. Do not attempt to configure these features on the Local Controllers even though the web interface allows you to do so.
- When the Global Controller pulls the new signatures from CCO, all managed Local Controllers download the new signatures from the Global Controller.

To specify the dynamic update settings, follow these steps:

Step 1 Click **ADMIN > System Setup > IPS Signature Dynamic Update Settings**.

IPS Signature Dynamic Update Settings

URL:	<input type="text" value="https://www.cisco.com/cgi-bin/Software/IDS/locator/locator.pl"/> <small>(Example CCO URL: https://www.cisco.com/cgi-bin/Software/IDS/locator/locator.pl Example Local Server URL: https://myserver.com/cs-mars-ips.zip)</small>
Username:	<input type="text"/>
Password:	<input type="password"/>
Signature Pulling Interval:	<input type="text" value="Every day"/>
Last Updated Time and Version:	Jun 21, 2007 3:01:53 AM PDT - 259
Status:	Download Failed: CS-MARS could not download IPS Signature file at Sep 04, 2007 03:04:56 AM PDT

250319

Step 2 Enter the following values:

- **URL**—Verify that the path to the software locator is defined. The default value is <https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl> (<https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl>), which is located on the Cisco Software Download site. You can specify a local server using the following example <https://myserver.com/cs-mars-ips.zip> (the zip files can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/mars-ips-sigup>).
- **Username**—Specify the username of the account that accesses the secure server. If you are using the default URL value, this is a CCO username.
- **Password**—Specify the password associated with the username value provided.
- **Signature Pulling Interval**—Specify the interval at which the signature updates should be pulled from the server identified in the URL field. Valid options include: Never (default), Every 1, 2, 3, 6, or 12 hours, or Every 1 to 14 days.

Step 3 To verify the settings are correct, click **Test Connectivity**.

Step 4 Once the settings are verified, click **Submit**.

Step 5 Click **Activate**.



Tip Once this feature is enabled, you can determine the current signature version pulled down by MARS by selecting **Help > About** and reviewing the IPS Signature Version value.

Troubleshooting IPS Signature Dynamic Updates

Two types of failures can occur, and they are identified in the Status field of the IPS Signature Dynamic Update Settings page:

- **Failure to download the package.** Verify that the MARS Appliance has connectivity to the specified destination and that it is using the correct username and password.
- **Failure to install.** Indicates a problem with the package itself, possibly corrupted during the download.

Applying Custom Signature Updates

Cisco IPS 6.0 enables you to define custom signatures for Cisco IPS devices. Before you can define an inspection rule in MARS that fires when that signature is detected, you must map that signature to a MARS event type.

To enable this mapping within MARS, you must perform the following tasks:

1. Define a custom signature map file (an XML file) that maps between the custom IPS signature and a MARS event type.
2. Import that custom map file into the Local Controller that monitors the Cisco IPS device on which that custom signature is running.



Note

Cisco recommends that any Global Controller/Local Controller relationships be established prior to applying any custom signature updates.

This section contains the following topics:

- [File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File, page 4-8](#)
- [Example Custom Signature Map Files, page 4-9](#)
- [Import Custom Signature Maps into MARS, page 4-11](#)

File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File

Adhere to the following naming conventions for any XML file that maps a custom Cisco IPS signature to a MARS event type:

- **<number>.custom.inc.xml**—Where <number> is an integer . Start with 1 and increment for each additional signature (for example, 1.custom.inc.xml) This number indicates the version number of the custom signature package. Subsequent updates must increment this version number.

MARS uses this number to ensure that the Local Controllers are synchronized with the Global Controller. The Help About page of each MARS appliance displays the customer signature version, such as Custom version: 1.

The following elements or attributes are required for the custom signature XML mapping file:

- **encoding**—The header of the XML file varies based on the version of software running on the MARS appliance. If the software version is 4.3.1, then the header should be `<?xml version="1.0" encoding="ISO-8859-1"?>`. Otherwise, if it is running 5.3.1, the header must be `<?xml version="1.0" encoding="UTF-8"?>`.
- **<EventType />**—This element specifies the custom signature ID for this event. The `EVENT_TYPE` attribute value identifies either an existing MARS event type or a new MARS event type. If it is a new MARS event type, it should be in the range of 90000000-90490000. For example: ET-9000000. The prefix “ET-xxxxxxx” is required for all values in this attribute. This value range is reserved for custom signature IDs.



Note If the ID maps to a previously used custom ID, information for that custom event is updated with the data in this XML file. If ID maps to a system event type, the information is not updated.

- **<EVENT_PRIORITY />**—This element organizes the priority of this custom signature. The expected value is one of the following: HIGH, MEDIUM, or LOW. The event priority value should match the severity of the firing signature as configured on the Cisco IPS device.
- **<EVENT_TYPE_NAME />**—This element names the custom signature event. The expected value is a string of up to 300 characters. Valid character sets are WE8ISO8859P1 for 4.3.1 and AL32UTF8 for 5.3.1. Cisco recommends that this event type name match that of the signature name as configured on the Cisco IPS device.
- **<LONG_DESCRIPTION />**—This element describes the custom signature event. Acceptable value is a “unlimited” string of characters. Valid character sets are WE8ISO8859P1 for 4.3.1 and AL32UTF8 for 5.3.1.
- **<Device Event Type DEVICE_ET="signatureId/subId"/>**—The `DEVICE_ET` attribute of this element identifies the IPS custom signatureId/subId. For example, if the IPS signature has sigID=60001 and subID=0 then `DEVICE_ET=NR-60001/0`. The prefix “NR-” is required for all values in this attribute.
- **<DeviceType DEVICE_TYPE="Cisco IPS"/>**—The `DEVICE_TYPE` attribute value indicates that all signatures originate from a Cisco IPS device. You must specify this value as Cisco IPS in the mapping file.
- **<EventTypeGroup>**—The value of this required element must be an existing MARS event type group. You can map MARS event types to more than one event type group.

Example Custom Signature Map Files

This example, 1.custom.inc.xml, maps the custom signature NR-60000/0 to the new MARS normalized event type ET-9000001. It is written for a MARS appliance running 5.3.1:

```
<?xml version="1.0" encoding="UTF-8"?>
<CS_MARS_EVENT_DATA_UPDATE xsi:schemaLocation="EventDataUpdate.xsd"
xmlns="http://www.cisco.com/2007/CS-MARS/EVENT-DATA-UPDATE"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <EventTypeList>
    <EventTypeListElement>
      <EventType EVENT_TYPE="ET-9000001">
        <EVENT_PRIORITY>LOW</EVENT_PRIORITY>
        <EVENT_TYPE_NAME>Custom Event 9000001</EVENT_TYPE_NAME>
        <LONG_DESCRIPTION>This is custom event</LONG_DESCRIPTION>
        <CVE_NAME>String</CVE_NAME>
        <AffectedPlatforms>
```

```

<OSInfo>
  <Vendor>String</Vendor>
  <Model>String</Model>
  <Version>String</Version>
  <Patch>String</Patch>
</OSInfo>
<ApplicationInfo>
  <Program>String</Program>
  <ProgramVersion>String</ProgramVersion>
  <Application>
    <Vendor>String</Vendor>
    <Model>String</Model>
    <Version>String</Version>
    <Patch>String</Patch>
  </Application>
</ApplicationInfo>
</AffectedPlatforms>
<VULNTY_FLAG>0</VULNTY_FLAG>
<DENY_FLAG>0</DENY_FLAG>
<INFO_LINKS>http://cve.mitre.org</INFO_LINKS>
<FP_CONDITION>None</FP_CONDITION>
<RECOM_ACTION>None</RECOM_ACTION>
</EventType>
<EventTypeGroup ET_GROUP_NAME="Penetrate/BufferOverflow/Web" />
<DeviceEventType DEVICE_ET="NR-60001/0">
  <DeviceType DEVICE_TYPE="Cisco IPS" />
  <LINKS>http://www.mycompany.com</LINKS>
</DeviceEventType>
</EventTypeListElement>
</EventTypeList>
<Version>001</Version>
</CS_MARS_EVENT_DATA_UPDATE>

```

To remap this signature, NR-60000/0, to a different MARS event type, create a new xml file named 2.custom.inx.xml and change the <EventType> attribute to a different MARS event type, such as ET-3002071 (a system MARS normalized event type).

If the MARS normalized event type is the new user-created normalized event type, you can modify the information of the event type. This example, 3.custom.inc.xml, sets the priority to HIGH and it is written for a MARS appliance running 4.3.1:

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<CS_MARS_EVENT_DATA_UPDATE xsi:schemaLocation="EventDataUpdate.xsd"
xmlns="http://www.cisco.com/2007/CS-MARS/EVENT-DATA-UPDATE"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <EventTypeList>
    <EventTypeListElement>
      <EventType EVENT_TYPE="ET-9000001">
        <EVENT_PRIORITY>HIGH</EVENT_PRIORITY>
        <EVENT_TYPE_NAME>Custom Event 9000001</EVENT_TYPE_NAME>
        <LONG_DESCRIPTION>This is custom event</LONG_DESCRIPTION>
        <CVE_NAME>String</CVE_NAME>
        <AffectedPlatforms>
          <OSInfo>
            <Vendor>String</Vendor>
            <Model>String</Model>
            <Version>String</Version>
            <Patch>String</Patch>
          </OSInfo>
          <ApplicationInfo>
            <Program>String</Program>
            <ProgramVersion>String</ProgramVersion>
          </ApplicationInfo>
        </AffectedPlatforms>
      </EventType>
    </EventTypeListElement>
  </EventTypeList>
</CS_MARS_EVENT_DATA_UPDATE>

```

```

        <Application>
          <Vendor>String</Vendor>
          <Model>String</Model>
          <Version>String</Version>
          <Patch>String</Patch>
        </Application>
      </ApplicationInfo>
    </AffectedPlatforms>
    <VULNTY_FLAG>0</VULNTY_FLAG>
    <DENY_FLAG>0</DENY_FLAG>
    <INFO_LINKS>http://cve.mitre.org</INFO_LINKS>
    <FP_CONDITION>None</FP_CONDITION>
    <RECOM_ACTION>None</RECOM_ACTION>
  </EventType>
  <EventTypeGroup ET_GROUP_NAME="Penetrate/BufferOverflow/Web" />
  <DeviceEventType DEVICE_ET="NR-60001/0">
    <DeviceType DEVICE_TYPE="Cisco IPS" />
    <LINKS>http://www.mycompany.com</LINKS>
  </DeviceEventType>
</EventTypeListElement>
</EventTypeList>
<Version>001</Version>
</CS_MARS_EVENT_DATA_UPDATE>

```

Import Custom Signature Maps into MARS

Once you've defined a custom signature map, you can import that map into the Local Controller. This operation allows MARS to begin processing events about your custom signature and allow you to include such events in event type groups and inspection rules.

Before You Begin

The following requirements must be satisfied before attempting this procedure:

- An xml file that defines the custom signature mappings and that adheres to the guidelines specified in [File Naming, Encoding, and Structure Guidelines for the Custom Signature Map File](#), page 4-8.
- A http server that hosts the xml file to be uploaded into the Local Controller.

To import a custom signature map file into MARS, follow these steps:

- Step 1** To import a customer signature map file, click **Admin > System Setup > IPS Custom Signature Update** in the web interface of the Local Controller.

IPS Custom Signature Update Settings

URL:	<input type="text" value="https://www.myserver.com/1.custom.inc.xml"/> (Example Local Server URL: https://myserver.com/1.custom.inc.xml)
Username:	<input type="text"/>
Password:	<input type="password"/>
Last Updated Time and Version: Jan 10, 2008 6:10:46 PM PST - Custom Signature package version: 0	
Status:	
<input type="button" value="Back"/> <input type="button" value="Test Connectivity"/> <input type="button" value="Update Now"/>	

25/1184

Step 2 Enter the local server and the xml filename in the URL field.

This server identifies the HTTP server from which MARS can download the custom XML file. For example, `https://www.myserver.com/1.custom.inc.xml`.

Step 3 If required by the local server, enter the Username/password required for the Local Controller to authenticate to that server.

Step 4 Click **Update Now** to start the on demand custom signature import.

Step 5 Click **Activate** to enable the custom signatures on the Local Controller.
