C H A P T E R 8

Configuring Host-Based IDS and IPS Devices

Revised: September 10, 2007

Host-based intrusion detection and prevention devices provide MARS with detailed information about attacks seen at the host level, rather than the network level. They also provide information about the host operating system and successful prevention of attacks, both of which provide more targeted data for false positive analysis.

This chapter explains how to bootstrap and add the following host-based IDS and IPS devices to MARS:

- Entercept Entercept 2.5 and 4.0, page 8-1
- Cisco Security Agent 4.x and 5.x Device, page 8-4

Entercept Entercept 2.5 and 4.0

To configure Entercept in MARS, you must perform the following tasks:

1. Generate CSV file that identifies each of the Entercept hosts by logging into the host running the Entercept console and copying the data out of the database table.

2. Configure the Entercept console to send SNMP traps to the MARS Appliance

3. Identify the events that should be generated as SNMP traps.

4. Define a host that represents the management console (Entercept console) in MARS web interface.

5. From that host in the MARS web interface, import the CSV seed file to identify the Entercept agents running on other hosts.

The following sections provide details on performing each of these tasks:

- Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5), page 8-2
- Define the MARS Appliance as an SNMP Trap Target, page 8-2
- Specific the Events to Generate SNMP Traps for MARS, page 8-3

Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5)

> **Note** Entercept agent information is saved in a database file on the Entercept console.

When you configure the MARS box to add Entercept agents, you can extract them from the database file on the Entercept console, instead of typing the mapping for each agent.

Create a CSV file for Entercept Agents in Version 2.5

Step 1 Go to the directory `Program Files\Cisco IDS\Console\Database` and copy the file `CoreShield.mdb` to another directory, e.g.: `C:\temp`.

Step 2 Open the copied `CoreShield.mdb` with Microsoft Access, and go to the "Agents" table.

Step 3 Export the table to a file named: `Agents.txt` and choose the exported file format to be CSV.

Step 4 Copy `Agents.txt` to a specific directory that is ready for the MARS box to load.

  A sample `agents.txt` file could be:
```
1,3,"entercept1",6,1,1,1,438,1,"127.0.0.1",0,,1051055867,2086

where the fields are: AgentID, AgentTypeID, ComputerName, ComputerType,
NewFlag, StatusID, OperatingModeID, VersionID, VersionModeID, IP,
License, Note, NoConnection, and UpTime.
```

Define the MARS Appliance as an SNMP Trap Target

Step 1 Log in to the Entercept Console.

Step 2 Click **Configuration**.

Step 3 Click the **Address Book** tab.

Step 4 In the All Contacts tree, click **SNMP Trap**.

Step 5 Click the Plus (+) button.

Step 6 In the New SNMP Trap page:

  a. Enter an **Alias** for the MARS Appliance.

  b. Set **Privilege** Level to Global.

  c. Set **Status** to Enabled.

  d. Enter the MARS Appliance's name if the DNS server can resolve the name. Otherwise, use its IP address.

  e. Enter a community string name in the **Community** field.

  f. Enter a **Port** number.

  g. Select a **Protocol**.

Specific the Events to Generate SNMP Traps for MARS

Step 1   Click the **Notifications** tab.

Step 2   Click the Plus (+) button.

Step 3   On the General tab, in the name field, enter a name for the notification.

Step 4   Click the **Agent Groups** tab and select the **All Agents** radio button.

Step 5   Click the **Security Events** tab and select the **Events by Severity Levels** radio button. Select the events that you want (**High**, **Medium**, **Low**, and **Information**).

Step 6   Click the **System Events** tab and select the **Events by Severity Levels** radio button. Select the events that you want (**Error**, **Warning**, and **Information**).

Step 7   Click the **Address Book** tab and click a destination in the Available Destinations field. Click the **Down** arrow to move it into the Selected Destinations field.

Step 8   Click **OK** and exit the program.

Add and Configure an Entercept Console and its Agents in MARS

Adding an Entercept device has two distinct steps. First, you add configuration information for the for the Entercept Console host. Second, you add the agents managed by that console.

Add the Entercept Console Host to MARS

Step 1   Click **Admin > Security and Monitor Devices > Add**.

Step 2   From the **Device Type** list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.

Step 3   Enter the **Device Name** and **IP addresses** if adding a new host.

Step 4   Click **Apply**.

Step 5   Click on **Reporting Applications** tab.

Step 6   From the **Select Application** list, select **Entercept 2.5 or 4.0**

Step 7   Click **Add**.

Step 8   Enter the **Console Name**.

Step 9   Check the "**Is Sensor**" check box—which is asking if it is a sensor or not.

Step 10   Enter the sensor's **Agent Name**, which is the agent name for the console if it is an agent.

Step 11   Click **Submit**.

You could now add the agents.

Add Entercept Agents Manually

Step 1   Click **Add Agent**.

Step 2   Select the device that already has agent running or **Add New**.

Step 3   Enter the **Device Name**, **Agent Name**, and its **Reporting IP** address if

Adding new device

- For the first interface, enter an IP address and mask.

- For multiple interfaces, click **Add Interface**, and add the new interfaces' IP address and mask.

Step 4   Click **Submit**.

Add Entercept Agents Using a Seed File

Step 1   Click **Load From CSV**.

Step 2   Enter the FTP server information and location of the CSV (comma separated values) file.

- If you need to generate the Entercept Agent CSV file, see Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5), page 8-2.

Step 3   Click **Submit**.

Cisco Security Agent 4.x and 5.x Device

To enable Cisco Security Agent (CSA) as a reporting device in MARS, you must identify the CSA Management Console (CSA MC) as the reporting device. The CSA MC receives alerts from the CSA agents that it monitors, and it forwards those alerts to MARS as SNMP notifications.

When MARS receives the SNMP notification, the source IP address in the notification is that of the CSA agent that originally triggered the event, rather than the CSA MC that forwarded it. Therefore, MARS requires host definitions for each of the CSA agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the CSA MC.

As of MARS, release 4.1.1, the MARS Appliance discovers CSA agents as they generate alerts, eliminating the need to manually define them. MARS parses the alert to identify the CSA agent hostname and to discover the host operating system (OS). MARS uses this information to add any undefined agents as children of the CSA MC as a host with either the Generic Windows (all Windows) or Generic (Unix or Linux) operating system value. You are still required to define the CSA MC; however, you are not required to define each agent. The default topology presentation for discovered CSA agents is within a cloud.

Note   The first SNMP notification from an unknown CSA agent appears to originate from the CSA MC. MARS parses this notification and defines a child agent of the CSA MC using the discovered settings. Once the agent is defined, all subsequent messages appear to originate from the CSA agent.

Prior to 4.1.1., you were required to manually add each agent or by using an exported hosts file, as defined in Export CSA Agent Information to File, page 8-6.

Note   Prior to the 4.1.1 release, CSA was identified by the device type name *Cisco CSA 4.0*. As part of an upgrade, any Cisco CSA 4.0 devices were renamed as *Cisco CSA 4.x*. This new name includes support for Cisco CSA 4.0 and 4.5.

This section contains the following topics:

Configure CSA Management Center to Generate Required Data

To bootstrap CSA, you must configure the CSA MC to forward SNMP notifications to the MARS Appliance. In addition, you can export the list of CSA agents in a format that MARS can import. However, this export operation is not necessary, as MARS discovers the agents as they generate notifications.

This section contains the following topics:

Configure CSA MC to Forward SNMP Notifications to MARS

The only required configuration is to ensure that CSA MC forwards the SNMP notifications that it receives from agents to MARS. From these notifications, MARS is able to discover the agent and its relevant settings. It is also from these events that MARS learns about the host-level activities transpiring on your network.

To forward all notifications to the MARS Appliance, follow these steps:

Step 1 Log in to the CiscoWorks Server desktop.

Step 2 From the navigation tree, select **VPN/Security Management Solution >Management Center > Security Agents**.

Step 3 In the Management Center screen, click the **Alerts** link.

Step 4 Click **New**.

Step 5 In the Name and Description fields, enter a name and description for the SNMP notification.

Step 6 Scroll down and select the **SNMP** check box.

Step 7 In the Community name field, enter the SNMP notification's community name.

Step 8 In the Manager IP address field, enter the MARS's IP address.

Step 9 Click **Save** and exit the program.

Export CSA Agent Information to File

With the release of MARS 4.1.1, you are no longer required to define each Cisco CSA agent, as they are discovered as a device sends an SNMP notification to the CSA Management Console (CSA MC).

Note The following instructions apply to Cisco CSA 4.x when Microsoft Internet Explorer is used to access the CSA MC web interface.

To export the all hosts report as a tab-delimited file, follow these steps:

Step 1 Log in to the CSA MC by accessing the console using the fully qualified domain name in the URL.

When accessing the CSA MC, you must use a fully qualified domain name in the URL. If you use the CiscoWorks Desktop to launch CSA MC, the ActiveX reports do not display.

Step 2 Click **Reports > Host Details**.

Step 3 Click **New**.

Step 4 In **Groups**, choose **<All Hosts>**, in **Viewer Type**, choose **ActiveX (IE only)**.

Step 5 Click **View report**.

A window appears that contains the host details.

Step 6 Click **Export**, and select export to an **Excel 5.0 Document** type.

Step 7 In the **Name** box, identifies the name for the file that you are exporting, for example, csahosts.xls.

Step 8 Open the exported file in Excel, and click **File > Save As...**

Step 9 In the Save as type box, click **Text (Tab delimited) (*.txt)**.

Step 10 In the File name box, enter the name for this file, for example, csahosts.txt, and click **Save**.

Step 11 Upload the generated file to an FTP server where the MARS Appliance can access it.

You will return to this file when adding the CSA device n the MARS web interface, as defined in Add and Configure a CSA MC Device in MARS, page 8-7.

Add and Configure a CSA MC Device in MARS

Before you can identify the agents, you must add the CSA MC to MARS. All CSA agents forward notifications to the CSA MC, and the CSA MC forwards SNMP notifications to MARS. Once you define the CSA MC and activate the device. MARS can discover the agents that are managed by that CSA MC. However, you can also chose to manually add the agents.

To add a CSA MC to MARS, follow these steps:

Step 1   Click **Admin > Security and Monitor Devices > Add**.

Step 2   From the **Device Type** list, select **Add SW security apps on a new host** or **Add SW security apps on existing host**.

Step 3   Enter the **Device Name** and **IP addresses** if adding a new host.

Step 4   Click **Apply**.

Step 5   Click **Reporting Applications** tab.

Step 6   From the **Select Application** list, select one of the following values:

- Cisco CSA 4.x.

- Cisco CSA 5.x

> ✎
> **Note**   As of the 4.3.1 and 5.3.1 releases of MARS, CSA 5.x is supported.just as 4.x is supported (including agent discovery.

Step 7   Click **Add**.

Step 8   The Management Console page appears.

Management Console

Add or edit agents for this csa management console.

| Add Agent | Edit Agent | Delete Agent | Load From File |

Cancel   Submit

143194

Step 9   Do one of the following:

- To save your changes and allow the CSA agents to be discovered automatically, click **Submit**, and then click **Done.**

- To add agents using an exported hosts report, continue with Add CSA Agents From File, page 8-9.

- To add a single agent manually, continue with Add a CSA Agent Manually, page 8-8.

Add a CSA Agent Manually

You can manually add a CSA Agent as a child of the CSA MC. This feature allows you to represent all of your agents, even if they have not generated any notifications.

To add CSA agents manually, follow these steps:

Step 1   Click **Admin > Security and Monitoring Devices**.

Step 2   From the list of devices, select the host running Cisco CSA Management Center, and click **Edit**.

Step 3   Click the **Reporting Applications** tab, select **Cisco CSA Management Center** in the Device Type list, and click **Edit**.

Step 4   Click the **Add Agent**.

Step 5   Do one of the following:

- Select the existing device, click **Edit Existing**, and continue with Step 8.

    A page displays with the values pre-populated for hostname, reporting IP address, and at least one interface.

- Click **Add New**, and continue with Step 6.

Step 6   In the Device Name field, enter the hostname on which this CSA agent resides.

This value should reflect the DNS entry for this device.

Step 7   In the Reporting IP field, enter the IP address that the agent uses to send logs to the CSA MC.

Step 8   Define each interface that is configured for this host by specifying the interface name, IP address, and network mask. To add a new interface, click **Add Interface**.

The interface settings are used for attack path calculation. It is very important that you identify any dual-homed hosts by defining each interface.

Step 9   Click **Submit**, and then click **Done**.

Step 10   To activate this device, click **Activate**.

Add CSA Agents From File

You can add the complete list of hosts on which CSA Agents are installed by exporting the all hosts report from CSA MC and importing that file into MARS. The only advantage to adding agents using an export file is that the first notification received that originates from the agent is not attributed to the CSA MC.

To add CSA agents from a file, follow these steps:

Step 1 Click **Admin > Security and Monitoring Devices**.

Step 2 From the list of devices, select the host running Cisco CSA Management Center, and click **Edit**.

Step 3 Click the **Reporting Applications** tab, select **Cisco CSA Management Center** in the Device Type list, and click **Edit**.

Step 4 Click **Load From File**.

a

Remote File Location:

→ *IP Address:

→ *User Name:

→ *Password:

→ *Path:

→ *File Name:

143193

⚠

Caution The file should be formatted as a tab delimited file. You cannot use a CSV file. To generate a tab delimited file of the CSA agents managed by the CSA MC, see Export CSA Agent Information to File, page 8-6.

Step 5 In the IP Address field, enter the address of the FTP server where you stored the exported hosts file, as described in Export CSA Agent Information to File, page 8-6.

Step 6 In the User Name field, enter the name of the account used to authenticate to the FTP server.

Step 7 In the Password field, enter the password that corresponds to the account specified in Step 6.

Step 8 In the Path field, enter the path to the folder where the file is stored. If this file is stored in the root folder, you must specify a backslash (\) in this field. The format of this value is `\<path_here>\`.

Step 9 In the File Name field, enter the name of the tab delimited file.

Step 10 Click **Submit**.

The following message displays and the hosts are added as agents of the CSA MC:

```
Success:
Status: OK
```

Step 11 Click **Done**.

Troubleshooting CSA Agent Installs

When importing CSA agents from a file, the following messages can occur.

Table 8-1   Error and Status Messages when Importing CSA Agents from File

Message	Description/Issue
Status: NumberFormatException occurred parsing the file at line *X*	Occurs when you have a CSV file rather than a tab delimited file. The line number varies.
Error Occurred: Status: DbDevice occurred parsing the file at line -1	Occurs when duplicate files are imported, even if you have deleted all of the agents and the CSA MC.
Success: Status: OK	Indicates a successful import of CSA agents using the tab-delimited file.
Error Occurred: Status: FileNotFoundException	Indicates that the file does not exist at the specified path. If the path is at the root of your FTP server, verify that you have included \ as the path value.
Error Occurred: Status: NoRouteToHostException	Indicates that the identified FTP server is not reachable from the MARS Appliance. You may need to define additional routes or enable traffic flows to ensure the connection is allowed.