



CHAPTER 28

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.



Caution

Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

This chapter contains the following topics:

- [Extracting Entercept Agent Information into a CSV file \(for Entercept Version 2.5\), page 28-1](#)
- [Define the MARS Appliance as an SNMP Trap Target, page 28-2](#)
- [Specify the Events to Generate SNMP Traps for MARS, page 28-2](#)
- [Add and Configure an Entercept Console and its Agents in MARS, page 28-3](#)

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 Intercept 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 Intercept 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, specify the following values:
- **Alias**—Enter an name for the MARS Appliance.
 - **Privilege Level**—Set to Global.
 - **Status**—Set to Enabled.
 - **Name**—Enter the MARS Appliance’s name if the DNS server can resolve the name. Otherwise, use its IP address.
 - **Community**—Enter a community string name,
 - **Port**—Enter the SNMP port number used by the MARS Appliance.
 - **Protocol**—Select SNMP.
-

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 Intercept Console and its Agents in MARS

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

This section contains the following topics:

- [Add the Intercept Console Host to MARS, page 28-3](#)
- [Add Intercept Agents Manually, page 28-4](#)
- [Add Intercept Agents Using a Seed File, page 28-4](#)

Add the Intercept 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 Intercept 2.5 or 4.0
- Step 7** Click **Add**.
- Step 8** Enter the Console Name.
- Step 9** Check the **Is Sensor** check box, which identifies the device as a sensor.
- Step 10** Enter the sensor's **Agent Name**, which is the agent name for the console if it is an agent.

Management Console

→ *Console Name:

→ Is Sensor

*Agent Name:

143220

Step 11 Click **Submit**.

You can now add the agents.

Add Entercept Agents Manually



Caution

Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

Step 1 Click **Add Agent**.

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

Step 3 If you selected Add New, then specify the following values:

- **Device Name**
- **Agent Name**
- **Reporting IP**
 - 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



Caution

Monitoring devices that support dynamic discovery of agents do not discover the agent on the monitoring device server, if applicable. This agent is intentionally not discovered, as it causes issues in event processing from that device. In addition, you must not manually define the agent that runs on the monitoring device server.

-
- 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 28-1.
- Step 3** Click **Submit**.
-

