



## CHAPTER 7

# McAfee IntruShield

---

To configure McAfee IntruShield (formerly known as IntruVert IntruShield) in MARS, you must perform the following tasks:

1. Generate CSV file that identifies each of the IntruShield sensor hosts by logging into the database to which IntruShield Manager writes and performing and saving a database query.
2. Configure the IntruShield Manager to send SNMP traps to the MARS Appliance
3. Define a host that represents the management console (McAfee IntruShield Security Manger) in MARS web interface.



---

**Note** Beginning in 6.x, MARS discovers the IntruShield sensors from the IntruShield Security Manager SNMP traps. Therefore, you are not required to define the network sensors manually or via a seedfile.

---

4. (Optional) From that host in the MARS web interface, import the IntruShield network sensor seed file to identify the IntruShield sensors running on other hosts.

This chapter contains the following topics:

- [Configure McAfee IntruShield 4.1 to Send SNMP Traps to MARS, page 7-1](#)
- [Add the IntruShield Manager Host to MARS, page 7-2](#)
- [Add IntruShield Sensors in MARS using Seed Files, page 7-4](#)

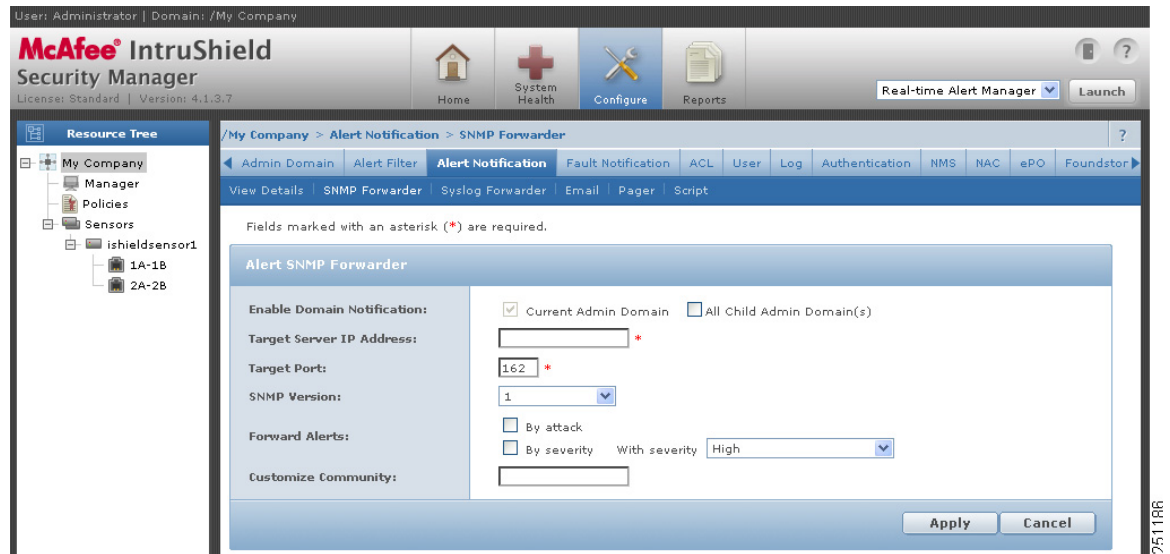
## Configure McAfee IntruShield 4.1 to Send SNMP Traps to MARS

Using the IntruShield Security Manager interface, you can identify the MARS appliance as a target for SNMP traps and specify what types of event data to forward to MARS.

To configure IntruShield to forward SNMP traps to MARS, follow these steps:

- 
- Step 1** Log in to the IntruShield Security Manager 4.1.
  - Step 2** Click **Configure**.
  - Step 3** In the Resource Tree, click **My Company**.
  - Step 4** Click the **Alert Notification** tab, and then click the **SNMP Forwarder** sub-tab..
  - Step 5** Verify the **Yes** option is selected for Enable SNMP Forwarder.
  - Step 6** To define an new SNMP target, click **Add**.

The Alert SNMP Forwarder page appears.



**Step 7** Specify values for the following fields:

- **Enable Domain Notification**—Verify that both the Current Admin Domain and All Child Admin Domain(s) check boxes are selected.
- **Target Server IP Address**—Specify the IP address of the target Local Controller as it appears to IntruShield.
- **Target Port**—Enter *162* to identify the SNMP port on which the Local Controller listens for SNMP messages.
- **SNMP Version**—Select *1*. This value identifies the version of SNMP running on the target Local Controller.
- **Forward Alerts**—Verify that both the By attack and By severity check boxes are selected. Continue defining the severity level as follows:
  - **With severity**—Select the **Informational and above** option.
- **Customize Community**—Specify the SNMP community string that allows MARS to access your protected IntruShield data.

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

## Add the IntruShield Manager Host to MARS

To define the host and represent the management console for IntruShield, follow these steps:

- Step 1** Click **Admin > System Setup > 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.

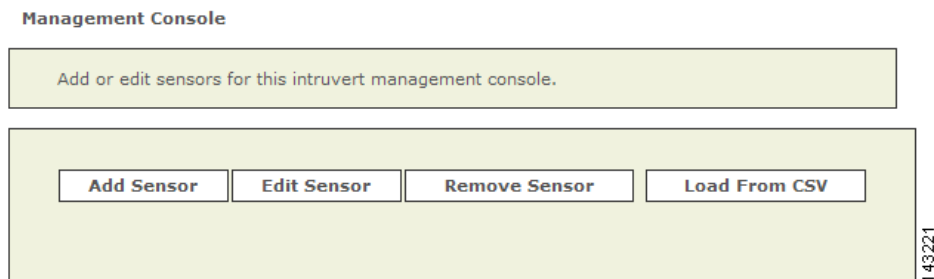
- Step 4** Click **Apply**.
- Step 5** Click **Reporting Applications** tab.
- Step 6** Select **McAfee IntruShield 4.1** from the Select Application list.
- Step 7** To complete the definition of this console, click **Add**.



**Note** MARS discovers IntruShield sensors as they report data through the IntruShield Manager SNMP traps.

- Step 8** (Optional) To manually define sensors that the console manages, you can use one of two methods:
- [Add IntruShield Sensors Manually, page 7-3](#)
  - [Add IntruShield Sensors in MARS using Seed Files, page 7-4](#)

**Figure 7-1** Add IntruShield Sensors



- Step 9** To save your changes, click **Submit**.
- Step 10** To enable MARS to start sessionizing events from this application, click **Activate**.

## Add IntruShield Sensors Manually

While MARS discovers IntruShield sensors over time, you may want to know if an undiscovered device is not reporting via the standard device not reporting messages that MARS issues. To ensure that this functionality is operational, you may choose to add a sensor manually.



**Note** MARS discovers IntruShield sensors as they report data through the IntruShield Manager SNMP traps; therefore, this procedure is not required.

To add sensors manually, follow these steps:

- Step 1** Click **Add Sensor**.
- Step 2** Specify the following values:
- **Device Name**—The DNS entry for this device.
  - **Sensor Name**—The name as it appears in the console.
  - **Reporting IP**—The IP address that the agent uses to send logs to the console.

- Step 3** Add the interface information.
- Step 4** For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:
- To manually define the networks, select the **Define a Network** radio button.
    - a. Enter the network address in the Network IP field.
    - b. Enter the corresponding network mask value in the Mask field.
    - c. Click **Add** to move the specified network into the Monitored Networks field.
    - d. Repeat as needed.
  - To select the networks that are attached to the device, click the **Select a Network** radio button.
    - a. Select a network from in the Select a Network list
    - b. Click **Add** to move the specified network into the Monitored Networks field.
    - c. Repeat as needed.
- Step 5** To save your changes, click **Submit**.
- Step 6** To enable MARS to start sessionizing events from this module, click **Activate**.
- 

## Add IntruShield Sensors in MARS using Seed Files

Adding an IntruShield sensors manually using a seed file has two distinct steps. First, extract sensor information from the IntruShield Security Manager host. Second, import that seedfile into the MARS web interface.

This section contains the following topics:

- [Extracting IntruShield Network Sensor Information from the IntruShield Security Manager, page 7-4](#)
- [Add IntruShield Sensors Using a Seed File, page 7-5](#)

## Extracting IntruShield Network Sensor Information from the IntruShield Security Manager

IntruShield sensor information is saved in a database on the IntruShield Security Manager host. When you configure the MARS to add IntruShield sensors, you can manually add the mapping of each IntruShield sensor name or you can extract them as a seed file from the database on the IntruShield Manager.



### Note

MARS discovers IntruShield sensors as they report data through the IntruShield Manager SNMP traps; therefore, this procedure is not required.



### Note

The instructions apply for McAfee IntruShield version 1.5. IntruShield supports both MySQL and Oracle.

To create a CSV file for McAfee IntruShield, follow these steps:

- 
- Step 1** Log in to the database.
- Step 2** Perform the query:
- ```
use lf; select name, ip_address from iv_sensor where ip_address is not NULL;
```
- Step 3** Store the query result into a file, remove the header, trailer, and separator lines, and edit the result to a CSV format.

For example, the query result could be:

```
+-----+-----+
| name      | ip_address |
+-----+-----+
| intruvert | 0A010134  |
| intruvert1| 0A010135  |
+-----+-----+
2 row in set (0.00 sec)
```

You would then edit the above file to appear as:

```
intruvert,0A010134
intruvert1,0A010135
```

- Step 4** Save the edited CSV file, move the file to an FTP server from which you can load the seed file using the MARS web interface.
- 

## Add IntruShield Sensors Using a Seed File

To add sensors using a seed file, follow these steps:

- 
- 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 IntruShield sensors CSV file, [Extracting IntruShield Network Sensor Information from the IntruShield Security Manager, page 7-4](#).
- Step 3** Click **Submit**.
- The list of sensors appears on the management console page.
- Step 4** For each sensor that appears in the management console page, select the check box next to the sensor and click Edit Sensor.
- Step 5** For attack path calculation and mitigation, specify the networks being monitored by the sensor. Do one of the following:
- To manually define the networks, select the **Define a Network** radio button.
    - a. Enter the network address in the Network IP field.
    - b. Enter the corresponding network mask value in the Mask field.
    - c. Click **Add** to move the specified network into the Monitored Networks field.
    - d. Repeat as needed.

- To select the networks that are attached to the device, click the **Select a Network** radio button.
  - a. Select a network from in the Select a Network list
  - b. Click **Add** to move the specified network into the Monitored Networks field.
  - c. Repeat as needed.

**Step 6** To save your changes, click **Submit**.

**Step 7** To save the changes made to this management console and the sensors it manages, click **Submit**.

**Step 8** To enable MARS to start sessionizing events from this module, click **Activate**.

---