



CHAPTER 11

ISS RealSecure 6.5 and 7.0

To configure ISS RealSecure, you must perform the following four tasks:

1. Prepare each ISS sensor as follows:
 - Edit the *common.policy* files to point to the MARS Appliance as an SNMP target.
 - Modify the *current.policy* files to configure each signature so that the SNMP notification is a default response when triggered.
 - Edit the *response.policy* files to specify the IP of the SNMP manager (MARS Appliance) and the community string.
 - Restart the ISS daemon for the changes to take effect.

For more information, see [Configure ISS RealSecure to Send SNMP Traps to MARS, page 11-1](#).

2. Add the ISS sensor to MARS as a network-based IDS device. For more information, see [Add an ISS RealSecure Device as a NIDS, page 11-3](#).
3. Click **Activate** to enable proper processing of received events.

This chapter contains the following topics:

- [Configure ISS RealSecure to Send SNMP Traps to MARS, page 11-1](#)
- [Add an ISS RealSecure Device as a NIDS, page 11-3](#)
- [Add an ISS RealSecure Device as a HIDS, page 11-4](#)

Configure ISS RealSecure to Send SNMP Traps to MARS

To configure an ISS RealSecure sensor, follow these steps:

-
- Step 1** Log into the sensor.
 - Step 2** Locate the common.policy files in these directories:
 - Microsoft Windows

```
Program Files\ISS\issSensors\server_sensor_1
Program Files\ISS\issSensors\network_sensor_1
```
 - Linux

```
/opt/ISS/issSensors/server_sensor_1
/opt/ISS/issSensors/network_sensor_1
```
 - Step 3** Open the *common.policy* files in a text editor.

Step 4 Change the line that reads:

```
Manager =S
```

to:

```
Manager =S <MARS's IP address>
```

If MARS Appliance's IP address is NATed, you may need to use the NATed address. If you use the MARS Appliance's IP address as the destination IP address, make sure the SNMP trap can reach MARS Appliance.

Step 5 Save these edited files and exit the editor.**Step 6** Locate the *current.policy* files in these directories:

- Microsoft Windows

```
Program Files\ISS\issSensors\server_sensor_1
Program Files\ISS\issSensors\network_sensor_1
```

- Linux

```
/opt/ISS/issSensors/server_sensor_1
/opt/ISS/issSensors/network_sensor_1
```

Step 7 Open the *current.policy* files in a text editor.

Edit each signature to have SNMP as one of its responses, and set the choice for SNMP trap as default. For example, in this original signature:

```
[\template\features\AOLIM_File_Xfer\Response\];
[\template\features\AOLIM_File_Xfer\Response\DISPLAY\];
Choice =S Default;
[\template\features\AOLIM_File_Xfer\Response\LOGDB\];
Choice =S LogWithoutRaw;
```

Insert the following bolded lines to make it look similar to the following:

```
[\template\features\AOLIM_File_Xfer\Response\];
[\template\features\AOLIM_File_Xfer\Response\DISPLAY\];
Choice =S Default;
[\template\features\AOLIM_File_Xfer\Response\SNMP\];
Choice =S Default;
[\template\features\AOLIM_File_Xfer\Response\LOGDB\];
Choice =S LogWithoutRaw;
```

Step 8 Save these edited files and exit the editor.**Step 9** Locate the *response.policy* files in these directories:

- Microsoft Windows

```
Program Files\ISS\RealSecure SiteProtector\Console
```

- Linux

```
/opt/ISS/RealSecure SiteProtector/Console
```

Step 10 Edit the response.policy files to specify the IP of the SNMP manager (MARS Appliance) and the community string:

```
SMTP_HOST=S;
addr_1=S;
[\Response\SNMP\];
[\Response\SNMP\Default\];
Manager=S;
Community=Spbublic;
```

to:

```
Manager =S <MARS's IP address> ;  
Community = S <string> public;
```

If MARS Appliance's IP address is NATed, you may need to use the NATed address. If you use the MARS Appliance's IP address as the destination IP address, make sure the SNMP trap can reach MARS Appliance.

Step 11 Save these edited files and exit the editor.

Step 12 Restart the ISS daemon.

- For sensors installed on Microsoft Windows, restart it in the Services menu.
- For sensors installed on Linux, run:

```
/etc/init.d/RealSecure stop  
/etc/init.d/RealSecure start
```

Add an ISS RealSecure Device as a NIDS

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.

Step 4 Click **Apply**.

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

Step 6 From the Select Application list, select **ISS RealSecure 6.5** or **ISS RealSecure 7.0**.

Step 7 Click **Add**.

Step 8 Click the **NIDS** radio button, if it is not already selected.

Figure 11-1 Configure ISS Real Secure NIDS

Step 9 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 10 To save your changes, click **Submit**.

Step 11 To enable MARS to start sessionizing events from this module, click **Activate**.

Add an ISS RealSecure Device as a HIDS

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.

Step 4 Click **Apply**.

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

Step 6 From the Select Application list, select **ISS RealSecure 6.5** or **ISS RealSecure 7.0**.

- Step 7** Click **Add**.
- Step 8** Click the **HIDS** radio button.

Figure 11-2 *Configure ISS Real Secure HIDS*

→ NIDS HIDS

To add HIDS RealSecure, select the radio button and submit, then add interfaces in the General Tab.

Cancel Submit

143218

- Step 9** Click **Submit**.
- Step 10** For multiple interfaces, click the **General** tab, and add the new interfaces' name, IP address, and network mask.

Figure 11-3 *Adding Multiple Interfaces*

Device Type: Edit host with security applications

↓

General	Reporting Applications	Vulnerability Assessment Info												
<p>→ *Device Name: <input type="text" value="H-10.1.1.103"/></p> <p>→ Access IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/></p> <p>→ Reporting IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/></p> <p>→ Operating System: <input type="text" value="Generic"/> <input type="button" value="Logging Info"/></p> <p>Enter interface information:</p> <table border="1"> <thead> <tr> <th colspan="2">Add Interface</th> <th colspan="2">Remove Interface/IP</th> </tr> <tr> <th>Name:</th> <th>IP Address:</th> <th colspan="2">Network Mask:</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> <input type="text" value="eth0"/></td> <td><input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="103"/></td> <td><input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/> <input type="text" value="0"/></td> <td><input type="button" value="Add IP/Network Mask"/></td> </tr> </tbody> </table>			Add Interface		Remove Interface/IP		Name:	IP Address:	Network Mask:		<input type="checkbox"/> <input type="text" value="eth0"/>	<input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="103"/>	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/> <input type="text" value="0"/>	<input type="button" value="Add IP/Network Mask"/>
Add Interface		Remove Interface/IP												
Name:	IP Address:	Network Mask:												
<input type="checkbox"/> <input type="text" value="eth0"/>	<input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="103"/>	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/> <input type="text" value="0"/>	<input type="button" value="Add IP/Network Mask"/>											

143219

- Step 11** Click **Apply**.

