



# CHAPTER 5

## Enterasys Dragon 6.x

---

To configure the Enterasys Dragon devices, you must:

- Configure the Dragon Policy Manager (DPM) or Event Flow Processor (EFP).
- Configure the syslog daemon running on the same system as the DPM or EFP.
- Configure the MARS.

This chapter contains the following topics:

- [DPM/EFP Configuration, page 5-1](#)
- [Host-side Configuration, page 5-2](#)
- [MARS-side Configuration, page 5-2](#)

## DPM/EFP Configuration

Before you configure the DPM or EFP, you must install and enable the Alarmtool.

This section contains the following topics:

- [Configure the DPM or EFP, page 5-1](#)

## Configure the DPM or EFP

---

- Step 1** Log into the DPM or EFP.
- Step 2** Click **Alarmtool**.
- Step 3** In the left menu, click **Notification Rules**.
- Step 4** In the right window, select syslog if it exists. If not, you need to create it:
  - a.** Click **New Notification Rules** and select **syslog**.
  - b. Facility** - Make sure the localn you select is not in use by the syslog daemon
  - c. Level** - Select Debug
  - d. Message** - Make sure its in such format:

```
%TIME% %DATE% SigName=%NAME% from Sensor=%SENSOR%  
SrcIP=%SIP% DstIP=%DIP% SrcPort=%SPORT% DstPort=%DPORT%  
Protocol=%PROTO%
```
- Step 5** Click **Save**.

- Step 6** In the left menu, click **Alarm**.
  - Step 7** Set the **Type to Real-time** and the **Notification Rule to syslog**.
  - Step 8** Click **Save**.
  - Step 9** In the left menu, click **Deployment**.
  - Step 10** In the main screen, click **View Configuration**. Make sure the **localn** set in both notify syslog and alarm syslog match.
  - Step 11** In the main screen, click **Deploy and Reset** to confirm the configuration change.
- 

## Host-side Configuration

This section contains the following topics:

- [Configure the syslog on the UNIX host, page 5-2](#)

### Configure the syslog on the UNIX host

- Step 1** Log into the host as the root user.
- Step 2** On the same system running the DPM or EFP, edit the file `/etc/syslog.conf`.
- Step 3** Make sure `n` in `localn` matches the syslog entry you used on the DPM or EFP.
- Step 4** Add the line:

```
localn.*                @<mars ip address>
```

Replacing `n` with the value used in [Step 3](#) and replacing `<mars ip address>` with the IP address of the MARS Appliance.

- Step 5** Restart the syslog daemon by entering:

```
/etc/rc.d/rc.syslog restart
```

---

## MARS-side Configuration

This section contains the following topics:

- [Add Configuration Information for the Enterasys Dragon, page 5-2](#)
- [Add a Dragon NIDS Device, page 5-3](#)

### Add Configuration Information for the Enterasys Dragon

- 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** From the Select Application list, select **Enterasys Dragon 6.x**.
- Step 7** Click **Add**.
- 

## Add a Dragon NIDS Device

---

- Step 1** Click **Add Sensor**.
- Step 2** Select existing device or **Add New Device**.
- Step 3** Enter values for the following fields:
- **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 4** Add the interfaces, which important information for attack path calculation.
- For multiple interfaces, click **Add Interface**, and add the new interfaces's name, IP address and mask.
- 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** Click **Done** when you are done adding the sensor.
- Step 8** To enable MARS to start sessionizing events from this module, click **Activate**.
-

