

Configuring Profiler Options (NSM Procedure)

You configure Profiler options to enable Profiler features, set network addresses and applications subject to profiling, and set alerts.

The following topics describe how to configure Profiler options:

- Specifying General Options on page 1
- Specifying Tracked Hosts on page 2
- Specifying Context Targets on page 4
- Specifying Alert Options on page 4

Specifying General Options

You configure Profiler general options to enable Profiler features.

To specify Profiler general options:

1. From Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **General** tab.
3. Configure Profiler general options using Table 1.
4. Click **Apply**.

Table 1: Profiler Settings: General Tab

Setting	Description
Enable Profiling	Enables the Profiler.
Enable Application Profiling	Application profiling enables the profiler to collect and track application data. This setting can be started when you disable it in the profiler setting.
Enable Application Volume Tracking	Enables the Profiler to perform application volume tracking.
Include Probe and Attempt	Enables the Profiler to collect and track specific probes and attempts.
Include Non-tracked IP Profiles	Enables the Profiler to collect and track data from external hosts.
db limit (in MB)	Sets the maximum Profiler database size. By default, the maximum database size is 3 GB.

Table 1: Profiler Settings: General Tab (continued)

Setting	Description
Enable OS fingerprinting	Enables the Profiler to perform OS fingerprinting. OS fingerprinting detects the operating system of an end-host by analyzing TCP handshake packets. The OS fingerprinting process depends on an established TCP connection (one that has a SYN and a SYN/ACK). The OS fingerprinting process is capable of detecting the operating systems listed in <code>/usr/idp/device/cfg/fingerprints.set</code> .
Refresh Interval(in secs)	Sets the time interval (in seconds) that the Profiler refreshes OS fingerprinting. By default, the Profiler refreshes OS fingerprinting data every 3600 seconds (60 minutes).



NOTE: If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select **Update Device**, select the **Restart IDP Profiler After Device Update** checkbox, and click **OK**.

Specifying Tracked Hosts

You configure Profiler tracked host and excluded host settings to determine the network segments where Profiler gathers data.

To configure the tracked host and exclude lists:

1. From Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **Tracked Hosts** tab.
3. Click the + icon and then select **Add Host > Add Network** or **Add Group**. A dialog box appears where you create your tracked hosts list.
4. Configure Profiler tracked host settings using Table 2.

Table 2: Profiler Tracked Hosts/Exclude List Dialog Boxes

Setting	Description
Add Host	Name—Enter the name of the host.
	Color—Select any color from the drop-down list.
	Comment—Enter any additional comments.
	IP/IP Address—Enter the IP address when you select IP.
	Domain/Domain name—Enter the domain name when you select domain name.
	Resolve—Resolve the domain name with the IP and vice versa.
Add Network	Name—Enter the name of the host.
	IP Address—Enter the IP address of the network.
	Use Wildcard Mask—Enable this feature if you want to use wildcard mask.
	Netmask—Enter the netmask for the IP.
	Color—Select any color from the drop-down list.
	Comment—Enter any additional comments.
Add Group	Name—Enter the name of the group.
	Color—Select any color from the drop-down list.
	Comment—Enter any additional comments.
	Member List—Add or remove the members from the non-members list.

5. Click the **Exclude List** tab.
6. Click the + icon and then select **Add Host > Add Network** or **Add Group**. A dialog box appears where you create your exclude list.

Table 2 describes these dialog box settings.

7. Configure profiler settings using Table 2.
8. Click **Apply**.



NOTE: If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select **Update Device**, select the **Restart IDP Profiler After Device Update** checkbox, and click **OK**.

Specifying Context Targets

You configure Profiler context settings to determine whether Profiler logs include not only host and application data but also data pulled from application contexts. For example, if you specify context targets for FTP usernames, the Profiler logs will include the username specified for the FTP connection in addition to the host name and service (FTP).

To specify Profiler context targets:

1. From Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **Contexts To Profile** tab.
3. Browse and select from the predefined list of contexts.
4. Click **Apply**.



NOTE: If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select **Update Device**, check **Restart IDP Profiler After Device Update**, and click **OK**.

Specifying Alert Options

You configure Profiler alert options to determine whether you receive alerts when Profiler detects new hosts, protocols, or ports in use.

If you are configuring the Profiler for the first time, do not enable the new host, protocol, or port alerts. As the Profiler runs, the device views all network components as new, which can generate unnecessary log records. After the Profiler has learned about your network and has established a baseline of network activity, you should reconfigure the device to record new hosts, protocols, or ports discovered on your internal network.

To specify Profiler alert options:

1. From Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **Alert** tab.
3. Configure alert settings using Table 3.
4. Click **Apply**.
5. Click **OK**.

Table 3: Profiler Alert Tab

Setting	Description
New Host Detected	Sends an alert when Profiler detects a new host.

Table 3: Profiler Alert Tab (continued)

Setting	Description
New Protocol Detected	Sends an alert when Profiler detects a new protocol. New Protocol detection alerts are used only for Layer3 protocols.
New Port Detected	Sends an alert when Profiler detects a new port.
Database Limit Exceeded	Sends an alert to indicate the maximum database size has been reached. After a device reaches this limit, it begins purging the database.



NOTE: If you change Profiler settings, you must push a configuration update to the device before the new settings take effect. From the Device Manager, right-click the device, select **Update Device**, select the **Restart IDP Profiler After Device Update** checkbox, and click **OK**.

-
- Related Topics**
- Configuring Profiler Database Preferences (NSM Procedure)
 - Querying the Profiler Database (NSM Procedure)
 - Purging the Profiler Database (NSM Procedure)
 - Viewing Profiler Logs (NSM Procedure)

