

Configuring Profiler Options (NSM Procedure)

Profiler option settings are valid for standalone IDP sensors only. For more information, see the *NSM online Help*.

To configure the Profiler on a given IDP sensor, open the Device window and select **Profiler Settings**.

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

Setting Up the Profiler

Using the Profiler involves the following steps:

- Collecting specific information about your internal network
- Starting the Profiler to enable your device to begin collecting data
- Customizing Profiler preferences

You configure your device to collect specific information and compile it into the Profiler database.

Configuring the Profiler

You can configure the Profiler using the Profiler settings available on the device settings in the Device Manager. Using the Device Manager, double-click to access a device managed in NSM, and click **Profiler Settings**.

The Profile Configuration dialog box appears with the General tab selected. Once you select the device for profiling, you can configure the options for the device to collect data from your internal network.

The following topics describe the steps to configure Profiler options:

- Specifying General Options on page 1
- Specifying Tracked Hosts on page 3
- Specifying Context Targets on page 5
- Specifying Alert Options on page 5

Specifying General Options

In this tab, indicate whether you want to enable Application Profiling and Probe and Attempt and whether Non-tracked IP Profiles will be included in the profiling. Also indicate the size of the Profiler database and whether to enable OS fingerprinting.

You configure Profiler general options to enable Profiler features.

OS fingerprinting passively detects the operating system of an end-host by analyzing TCP handshake packets. To ensure that this works, you need to verify that OS

fingerprinting is first enabled on the profiled device. After you have configured the Profiler with the tracked hosts and contexts, you must update the device.

OS fingerprinting works only for packets that contain a full-fledged TCP connection, that is the TCP connection should have a SYN, SYN/ACK, and a FIN connection. OS fingerprinting only works for operating systems that are supported on the device. A list of the supported operating systems is available on the device in a file called **fingerprints.set** at the following location:

```
/usr/idp/device/cfg/fingerprints.set
```

Configuring Network Objects

The first part of configuring the Profiler is to inform the device which network objects you want the device to profile. When you start the Profiler, the device begins collecting data from the selected hosts.

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	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)	Specifies maximum database size for the Profiler on each device. By default, the maximum database size is set to 3GB.

Table 1: Profiler Settings: General Tab (continued)

Setting	Description
Enable OS fingerprinting	<p>Enables the Profiler to perform passive OS fingerprinting to determine the operating system of an end host.</p> <p>OS fingerprinting detects the operating system of an end host by analyzing TCP handshake packets.</p> <p>The OS fingerprinting process depends on an established TCP connection (one that has a SYN and a SYN/ACK).</p> <p>The OS fingerprinting process is capable of detecting the operating systems listed in <code>/usr/idp/device/cfg/fingerprints.set</code>.</p>
Refresh Interval(in secs)	Specifies 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

Select the known hosts you want to track in the Tracked Hosts tab. Select **Object Manager > Address Objects** to add entries to the hosts list.

In the Tracked Hosts tab, select the Network Objects that represent your internal hosts. The device collects detailed information about traffic that passes between internal hosts, and then groups traffic that does not match an internal host in a special IP: 73.78.69.84. Communication between an internal host and an external host is recorded only once. For example, the device records internal host A communicating to www.yahoo.com and www.cnn.com as one entry in the Profiler database. You can select unlimited internal network objects. You can also use the Exclude List tab to select the Network Objects that represent internal hosts that you do not want to include in IDP profiling. You might want to exclude a host from the Profiler if you select a group of network objects in the Tracked Host tab. Also, you might want to exclude specific members of that group.

You configure Profiler tracked host and excluded host settings to determine the network segments where the 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** check box, and click **OK**.

Specifying Context Targets

Select the contexts you want to profile in the Context Targets tab. Next, determine which contexts you want the device to record. In the Contexts to Profile tab, the context list includes only the contexts that can clearly identify a host, a user, and/or an application. When you start the Profiler, the device begins collecting data on traffic that matches the selected contexts. For example, To track FTP logins, usernames, and commands, select the FTP contexts in the Contexts to Profile tab. After the Profiler is started, the device begins collecting information about FTP logins, usernames, and commands, enabling you to quickly identify the users using FTP on your network and the actions they perform over that protocol.

When you first configure the Profiler, select all contexts. This enables the device to collect data about every context on your network, giving you a complete view of your network traffic. Later, when you have analyzed your traffic, you can eliminate contexts that you know will not be used on your network.

Select **Profile Context** to include context information. If you clear **Profile Context**, IDP profile data only includes high-level traffic data such as source, destination, and service. If you want Profiler information to include context values and network probes (for example, port scans), also configure the Profiler to include probes and attempts.

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 hostname 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

Indicate which profiler events you want to generate alerts for in the Alert Options tab. Use this tab to configure the Profiler to indicate the appearance of a new host, protocol, or port on your internal network. When you select **New Host Detected**, **New Protocol Detected**, or **New Port Detected**, the device generates a specific log record, such as PROFILER_NEW_HOST, in the Profiler Logs section of the Log Viewer when the device discovers a new host, protocol, or port.

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. For details, see the *Network and Security Manager Administration Guide*.

Select the **Database Limit Exceeded** alert to indicate when you have reached the maximum limit of the database size. You can configure the maximum limit of the Profiler database using the dbLimit parameter in the General tab of the Profiler Configuration dialog box. The default is 500 MB; the minimum-maximum range is 0 to 500 MB. After a device reaches this limit, it begins purging the database. For example, a network host performs the normal connections required for Internet connectivity (SMTP, POP3, HTTP, and so on). If the host is infected by a worm, it begins making outbound connections on an arbitrary port. The device logs the unique event and generates PROFILER_NEW_PROTO and PROFILER_NEW_PORT log records. The system immediately e-mails these log records to the security administrator, who can investigate the worm and take action to contain it.

Repeat the configuration process for each device in your network. When you have configured all devices on your network, you are ready to start the Profiler.

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.
New Protocol Detected	Sends an alert when Profiler detects a new protocol. New Protocol detection alerts are used only for Layer 3 protocols.
New Port Detected	Sends an alert when Profiler detects a new port.

Table 3: Profiler Alert Tab (continued)

Setting	Description
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)

Published: 2009-08-20