

Viewing Profiler Logs (NSM Procedure)

The Profiler Viewer contains multiple tabs with different views of Profiler data. The following topics describe these views:

- Application Profiler on page 1
- Protocol Profiler on page 2
- Network Profiler on page 4
- Violation Viewer on page 5

Application Profiler

The Application Profiler tab displays Application Volume Tracking (AVT) data. The Application Profiler tab is a table of information such as the NSM Log Viewer which enables you to view and analyze dynamic application (Layer-7) traffic within a specific context.

The Application Profiler view is divided into two sections:

- In the left pane, the Application Profiler tab displays a hierarchical tree of application categories. Applications are grouped by common functionality. For example, Peer-to-Peer applications include Chat and File Sharing applications. Under Chat, you can display Yahoo messenger, MSN, and AIM; under File Sharing, you can display Kazaa, Bittorrent, and Gnutella.

The left pane also displays aggregate statistics for volume (bytes) and packet count for the application category, application group, or application you select in the tree.

- In the right pane, the Application Profiler tab displays tables of session logs related to the application category or application you select in the left pane.

Table 1 describes Application Profiler session table.

Table 1: Application Profiler Session

Column	Description
Src IP	Source IP address of the traffic profiled.
Dst IP	Destination IP address of the traffic profiled.
User	The user associated with the traffic profiled.
Role	The role group to which the user that is associated with the traffic profiled belongs.
Context	All contexts of traffic that the devices selected in the Device table recorded.
Value	When you select a context, the values that your devices recorded for a selected context.
Src MAC	Source MAC addresses of traffic profiled.

Table 1: Application Profiler Session (continued)

Column	Description
Dst MAC	Destination MAC addresses of traffic profiled.
Src OUI	Source OUIs of traffic profiled. NOTE: The Organizationally Unique Identifier (OUI) value is a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs. You can obtain a list of OUIs at http://standards.ieee.org/regauth/oui/oui.txt .
Dst OUI	Destination OUIs of traffic profiled.
Src OS Name	Operating-system version running on the source IP of the traffic profiled.
Dst OS Name	Operating-system version running on the destination IP of the traffic profiled.
Hits	Number of occurrences that match the traffic profiled.
First Time	Timestamp for the first time the device logged the event (within the specified time interval).
Last Time	Timestamp for the last time the device logged the event (within the specified time interval).
Domain	Domain in which the device is managed in NSM.
Device	Device that profiled the data displayed.

By default, the Application Profiler view contains only the data collected during the configured time interval.

To display the Application Profiler view:

1. Navigate to **Investigate > Security Monitor > Profiler**.
2. Click the **Application Profiler** tab.



TIP: You can jump from the Application Profiler tab to the APE rulebase editor by right-clicking an application in the left pane and selecting a policy editor option. For information about using NSM features to sort, filter, and drill down on records, see the *NSM online help*.

Protocol Profiler

The Protocol Profiler tab displays information about applications that are running on your network.

Table 2 describes the protocol profiler data.

Table 2: Protocol Profiler Data

Column	Description
Src IP	Source IP address of the session. NOTE: Profiler tracks all traffic through the IDP appliance, including traffic for hosts not in your tracked hosts list. It records a value of 73.78.69.84 for the IP address for hosts not defined in the Tracked Hosts tab, such as external hosts you would not know and therefore could not configure.
Dst IP	Destination IP address. NOTE: Communication between an internal host and an external host is recorded only once. For example, the device records internal host A communicating to http://ca.yahoo.com and http://edition.cnn.com as one entry in the Profiler DB.
User	The user associated with the session.
Role	The role to which the user belongs.
Context	Matching contexts.
Value	Value retrieved from matching context.
Src MAC	Source MAC addresses.
Dst MAC	Destination MAC addresses.
Src OUI	Source OUI. NOTE: The Organizationally Unique Identifier (OUI) value is a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs. You can obtain a list of OUIs at http://standards.ieee.org/regauth/oui/oui.txt .
Dst OUI	Destination OUI.
Src OS Name	Operating-system version running on the source IP.
Dst OS Name	Operating-system version running on the destination IP.
Hits	Number of occurrences that match the session.
First Time	Timestamp for the first time the device logged the event (within the specified time interval).
Last Time	Timestamp for the last time the device logged the event (within the specified time interval).
Domain	NSM domain.
Device	Device through which the session was forwarded.

By default, the Protocol Profiler tab contains only the data collected during the configured time interval.

To display the Protocol Profiler tab:

1. In the NSM navigation tree, select **Investigate > Security Monitor > Profiler**.
2. Click the **Protocol Profiler** tab.



TIP: For information about using NSM features to sort, filter, and drill down in records, see the *NSM online Help*.

Network Profiler

The Network Profiler view is a table of information such as the NSM Log Viewer which enables you to view and analyze data related to static traffic (Layer-3, Layer-4, and RPC protocols, ports, and program numbers) within the context of data corresponding to peer, host, and operating system.

Table 3 describes Network Profiler data.

Table 3: Network Profiler Data

Column	Description
Src IP	Source IP address of the traffic profiled.
Dst IP	Destination IP address of the traffic profiled.
User	The user associated with the traffic profiled.
Role	The role group to which the user that is associated with the traffic profiled belongs.
Service	All services of traffic profiled.
Access Type	Type of the traffic profiled: <ul style="list-style-type: none">■ Access indicates a successful connection, during which the device recorded valid requests and responses from the server to a client.■ Attempt indicates a request that did not receive a reply. The device recorded a packet from a client to a server, but never saw a reply.■ Probe indicates a request that does not expect a reply. For non-TCP sessions, the device recorded an ICMP error; for TCP sessions, the device recorded a SYN packet from the client followed by a RST from the server.
Src MAC	Source MAC addresses of traffic profiled.
Dst MAC	Destination MAC addresses of traffic profiled.
Src OUI	Source OUIs of traffic profiled. NOTE: OUI stands for Organizationally Unique Identifier. This value is a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs. You can obtain a list of OUIs at http://standards.ieee.org/regauth/oui/oui.txt .
Dst OUI	Destination OUIs of traffic profiled.

Table 3: Network Profiler Data (continued)

Column	Description
Src OS Name	Operating-system version running on the source IP of the traffic profiled.
Dst OS Name	Operating-system version running on the destination IP of the traffic profiled.
Hits	Number of occurrences that match the traffic profiled.
First Time	Timestamp for the first time the device logged the event (within the specified time interval).
Last Time	Timestamp for the last time the device logged the event (within the specified time interval).
Domain	Domain in which the device is managed in NSM.
Device	Device that profiled the data displayed.

To display the Network Profiler view:

1. Navigate to **Investigate > Security Monitor > Profiler**.
2. Click the **Network Profiler** tab.



TIP: For information about using NSM features to sort, filter, and drill down on records, see the *NSM online Help*.

Violation Viewer

The Violation Viewer is a filtered view of the Network Profiler view. In the Violation Viewer, you configure permitted objects. Permitted objects are filtered from the display, allowing you to focus on unpermitted traffic.

To configure permitted objects:

1. Navigate to **Investigate > Security Monitor > Profiler**.
2. Click the **Violation Viewer** tab.
3. Click on the + icon that appears on the top of the right-hand window to display the New Permitted Object dialog box.
4. Type a name for the permitted object.
5. Within the New Permitted Object dialog box, click the + icon to add a rule to match source, destination, and services values for the permitted object.
6. To change the source, destination, or service value from **Any**, right-click the value and select **Add Source**, **Add Destination**, or **Add Service**.
7. Use the selection controls to select the desired address objects or service objects and click **OK**.
8. Click **OK** to save the permitted object.

The object appears in the filters windows within the Violation Viewer tab.

9. Select the object and click **Apply** to hide all matching objects from the Violation Viewer.



TIP: For information about using additional NSM features to sort, filter, and drill down on records, see the *NSM online Help*.

- Related Topics**
- Configuring Profiler Options (NSM Procedure)
 - Displaying Profiler Database Information (NSM Procedure)
 - Querying the Profiler Database (NSM Procedure)