



Think fast.™

Integration Notes

Integrating with Netcool/OMNIbus

The Cascade Profiler integrates with Netcool/OMNIbus through the use of SNMP traps. It has been tested with Netcool/OMNIbus Versions 3.6 and 7.x.

When the two systems are integrated, Profiler notifies Netcool of any events that trigger Profiler alerts. These are listed in the Netcool/OMNIbus Event List. The Netcool operator can right-click an entry in the event list and choose Cascade Profiler from the Tools submenu to display the Profiler Event Detail Report on the Netcool GUI.

The general procedure for integrating Profiler with Netcool/OMNIbus is as follows. (The Profiler tasks are described in more detail in the sections that follow. Refer to the Netcool/OMNIbus documentation for detailed descriptions of the Netcool/OMNIbus tasks.)

1. On Profiler, create an Event Viewer account for Netcool/OMNIbus. Alternatively, specify a RADIUS source for Profiler to use to authenticate Netcool/OMNIbus access to Profiler.
2. On Profiler, add the Event Viewer account for Netcool/OMNIbus to the Profiler access control list.
3. On Profiler, specify the Netcool/OMNIbus destination to which Profiler is to send SNMP traps and which types of traps to send.
4. Ensure that you have Netcool/OMNIbus Version 3.6 or 7.x, including the SNMP Probe and Netcool Knowledge Library or Netcool Knowledge Library Lite.
5. Obtain the Netcool/OMNIbus Integration Module for the Cascade Networks Profiler.
6. Install and configure this module as described in *Netcool/OMNIbus Integration Module for the Cascade Networks Profiler* or other documentation. This includes installing the Probe Rules files, installing the Netcool EventList Tool, and adding Profiler to the Tools menu.
7. When the two systems are integrated and operating, verify that:
 - Events reported by Profiler can be displayed in the Netcool/OMNIbus event list.
 - Right-clicking a Profiler event in the event list and choosing Cascade Profiler from the Tools submenu causes Netcool/OMNIbus to contact the Profiler. When you log in to the Event Viewer account on Profiler, Netcool/OMNIbus displays the Profiler Event Detail Report for the event.

Giving Netcool/OMNIBus Event Viewer access to Profiler

When Profiler receives a request for information, it authenticates the requesting user before sending the information. There are three methods by which Profiler can authenticate the request from the Netcool/OMNIBus user:

- When prompted, the Netcool/OMNIBus user enters the user name and password of a Profiler Event Viewer account.
- When prompted, the Netcool/OMNIBus user enters a user name and password known to a RADIUS server that Profiler checks.
- The Netcool/OMNIBus IP address and Event Viewer user account name are in the Profiler access control list.

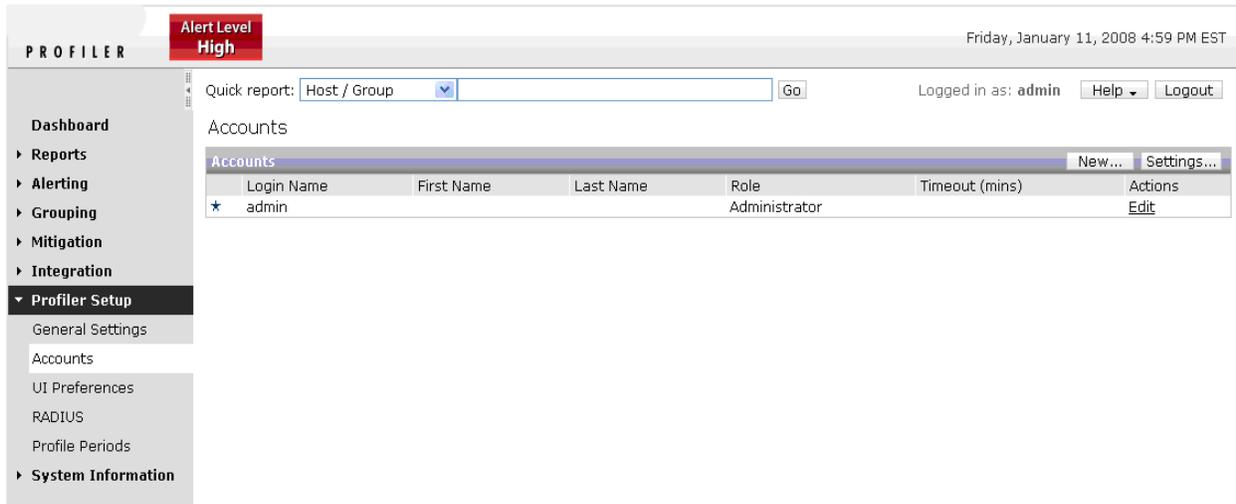
Note that users who are authenticated by RADIUS are given the privileges of a Monitor account, which exceed those of an Event Viewer account. An Event Viewer account can view a specific Event Detail Report, but cannot navigate away from that page.

Users authenticated through a RADIUS server can view Profiler displays related to traffic volumes and connections, in addition to specific Event Detail Reports. However, they cannot view user identity information or change the Profiler configuration, user settings, or their passwords.

Event Viewer account

To specify an Event Viewer user account:

1. Log in to a Profiler account that has Administrator permission.
2. Go to the **Profiler Setup** → **Accounts** page.



The screenshot shows the Profiler web interface. At the top, there is a navigation bar with 'PROFILER' on the left, an 'Alert Level High' indicator in a red box, and the date 'Friday, January 11, 2008 4:59 PM EST' on the right. Below the navigation bar is a search area with a 'Quick report:' dropdown menu set to 'Host / Group', a 'Go' button, and a 'Logged in as: admin' status with 'Help' and 'Logout' buttons. The main content area is titled 'Accounts' and contains a table with the following columns: 'Login Name', 'First Name', 'Last Name', 'Role', 'Timeout (mins)', and 'Actions'. There is one row in the table with the following data: 'admin' (Login Name), an empty cell (First Name), an empty cell (Last Name), 'Administrator' (Role), an empty cell (Timeout), and 'Edit' (Actions). A 'New...' button is visible above the table. On the left side of the interface, there is a sidebar menu with the following items: 'Dashboard', 'Reports', 'Alerting', 'Grouping', 'Mitigation', 'Integration', 'Profiler Setup' (which is expanded to show 'General Settings', 'Accounts', 'UI Preferences', 'RADIUS', and 'Profile Periods'), and 'System Information'.

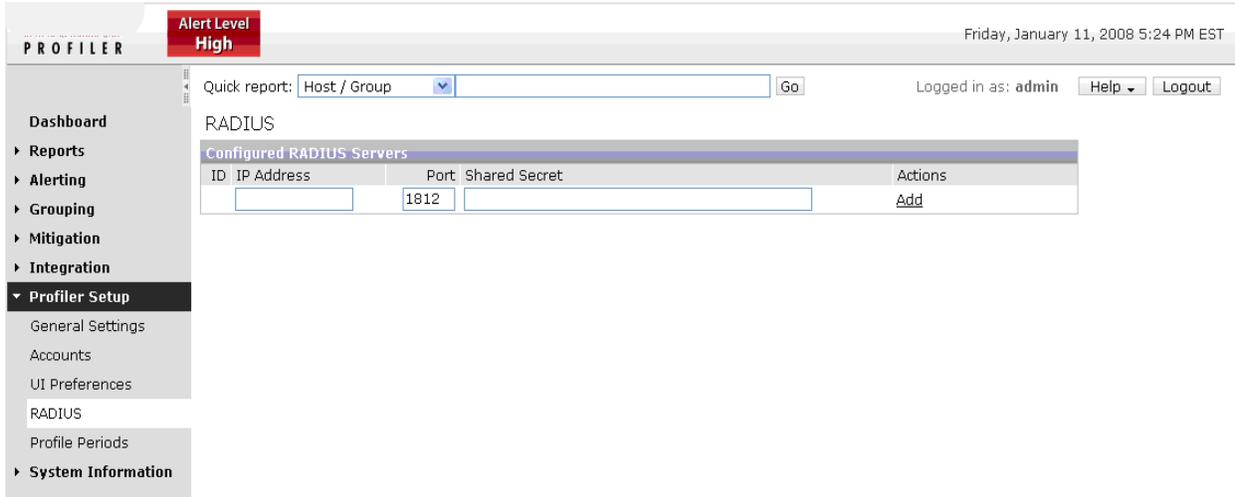
3. On the Accounts page, click **New...**. This displays the New User Profile page.

4. For the **Account role** field, select **Event Viewer** from the drop-down list.
5. Enter the user name and password for the Netcool/OMNIBus system. For information about the other options, refer to the Profiler help system.
6. Click **OK** to create the new account.
7. On the **Profiler Setup → Accounts** page, confirm that the account has been created correctly.
8. Ensure that the Netcool/OMNIBus users receive the login name and password for this account.

RADIUS

To allow Profiler to authenticate a Netcool/OMNIBus user via RADIUS:

1. Identify a RADIUS server that is accessible to Profiler.
2. Arrange for the RADIUS administrator to register the Netcool/OMNIBus user's user name and password.
3. On the Profiler, click **Profiler Setup → RADIUS** to open the RADIUS page.



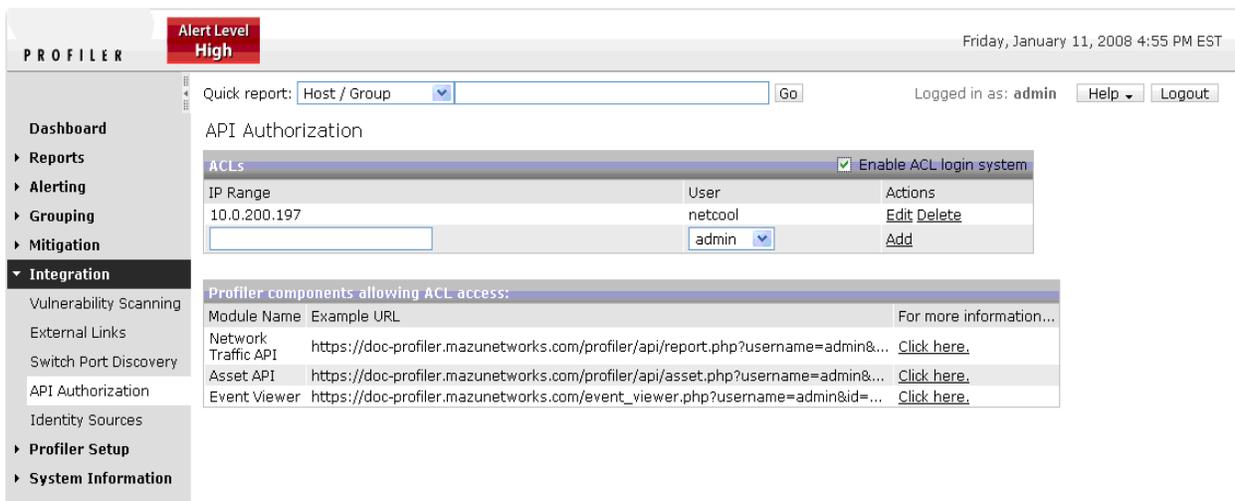
4. Enter the server information. (The shared secret is provided by the RADIUS server administrator.)
5. Click **Add**. This adds the server to the list of configured RADIUS servers on the RADIUS page.
6. Check the **Profiler Setup** → **RADIUS** page to confirm the server is listed.

When a Netcool/OMNIBus user enters a username and password that is not found in Profiler's database of user accounts, Profiler goes to the RADIUS server to authenticate the user.

API Authorization

To avoid Netcool/OMNIBus users needing to log into Profiler in order to view Event Detail Reports, you can grant Netcool/OMNIBus automatic access the Event Detail Reports. To do this:

1. On the Profiler, click **Integration** → **API Authorization** to open the API Authorization page.



2. Enter the IP address of the Netcool/OMNIbus system.
3. In the **User** list, select the name of the Event Viewer account that you set up for Netcool/OMNIbus users.
4. Click **Add**.
5. Select the **Enable ACL login system** checkbox.

Sending Profiler traps to Netcool/OMNIbus

Profiler can be configured to send traps for events of different types and severities to different or multiple recipients. It can also direct notifications on the basis of who is responsible for the groups of hosts in which an event is occurring. Refer to *Notifications* in the setup section of the Profiler help system or user's manual for descriptions of complex configurations. The procedure below assumes a simple configuration.

1. Go to the **Alerting** → **Notifications** page **Recipients** tab and click **New**.

The screenshot shows the Profiler web interface. At the top, there is a navigation bar with 'PROFILER' on the left, 'Alert Level High' in a red box in the center, and the date 'Friday, January 11, 2008 5:42 PM EST' on the right. Below the navigation bar is a search area with a 'Quick report:' dropdown set to 'Host / Group' and a 'Go' button. On the right of this area, it says 'Logged in as: admin' with 'Help' and 'Logout' buttons. A left-hand sidebar contains a menu with items: Dashboard, Reports, Alerting (expanded), Event Detection, Rule-based Events, Notifications, Grouping, Mitigation, Integration, Profiler Setup, and System Information. The main content area is titled 'Notification delivery settings' and has three tabs: 'Basic', 'Advanced', and 'Recipients' (which is selected). In the 'Recipients' tab, there is a 'New...' button and a table with the following structure:

Label	Email	SNMP	Actions
Default			Edit

2. On the New Recipient page, enter a label to identify the Netcool/OMNIbus recipient configuration.
3. Enter the IP address and port number of the Netcool/OMNIbus system.
4. Select the trap type, enter the required information for the trap receiver, and click **OK**.
5. Click **Test Now**, if desired, to send test notifications to the Netcool/OMNIbus system.

New Recipient

Recipient Label: [Assign Group Ownership...](#)

Email Test Now

Address:

Format: HTML PDF

SNMP Test Now

IP address: Port:

IP address: Port:

Type: V1 V3 Trap V3 Inform

Community:

Privacy: No privacy Use privacy

Username:

Authentication passphrase:

Authentication protocol:

Privacy passphrase:

Privacy protocol:

Security Engine ID:

6. Select the **Advanced** tab.

PROFILER Alert Level High Friday, January 11, 2008 5:52 PM EST

Quick report: Logged in as: admin

Notification delivery settings

Basic **Advanced** **Recipients**

To select a cell in the table, click it.
To select an entire row or column, click the label for that row or column.

	Low	Medium	High
DoS/Bandwidth Surge	Default	Default	Default
Host Scan	Default	Default	Default
New Host	Default	Default	Default
New Server Port	Default	Default	Default
Port Scan	Default	Default	Default
System Health	Default	Default	Default
Suspicious Connection	Default	Default	Default
Worm	Default	Default	Default
Firewall Tunneling Activity	Default	Default	Default
P2P Application Activity	Default	Default	Default
P2P Port Activity	Default	Default	Default
SpamBot Activity	Default	Default	Default
Tunneled Application Activity	Default	Default	Default

7. Select the cells or column cells in the table that correspond to the event types and alert levels that you want reported to the Netcool/OMNIBus system. (Click in the empty area of the first table cell to select all trap types.)

8. With the desired trap types selected, click the **Set Recipients** drop-down list and choose the recipient name that you just defined for the Netcool/OMNIbus system.
9. Click **Apply** and observe that all selected cells display the Netcool/OMNIbus recipient name.

For Additional Information

If you have questions or need additional information, please contact Riverbed Technical Support at <https://support.riverbed.com> or call 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States.