



PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

Lab 9: Management and Reporting

Document Version: 2016-04-19

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	4
Pod Topology	5
Lab Settings	6
1 Configure the Initial Settings	7
2 Explore the Dashboard, ACC, App Scope, and Session Browser	10
3 Create a Custom Report.....	13

Introduction

Scenario

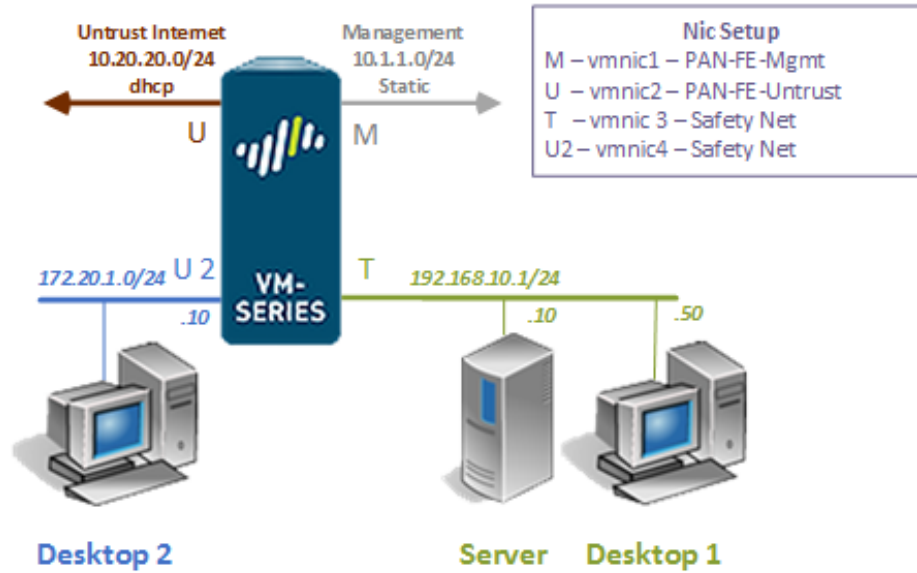
Your manager wants to see daily reports that detail the threats encountered by the firewall. Configure a custom report to show a threat summary for all traffic allowed in the past 24 hours. It should include the threat name, the application (including technology and sub-category for reference) and the number of times that threat was encountered. Export the file as a PDF.

Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Tour the Palo Alto Networks firewall dashboard
2. Tour the logs
3. Generate reports

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng\$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng\$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng\$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

1 Configure the Initial Settings

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **sysadmin** as the *username* and **Training\$** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.



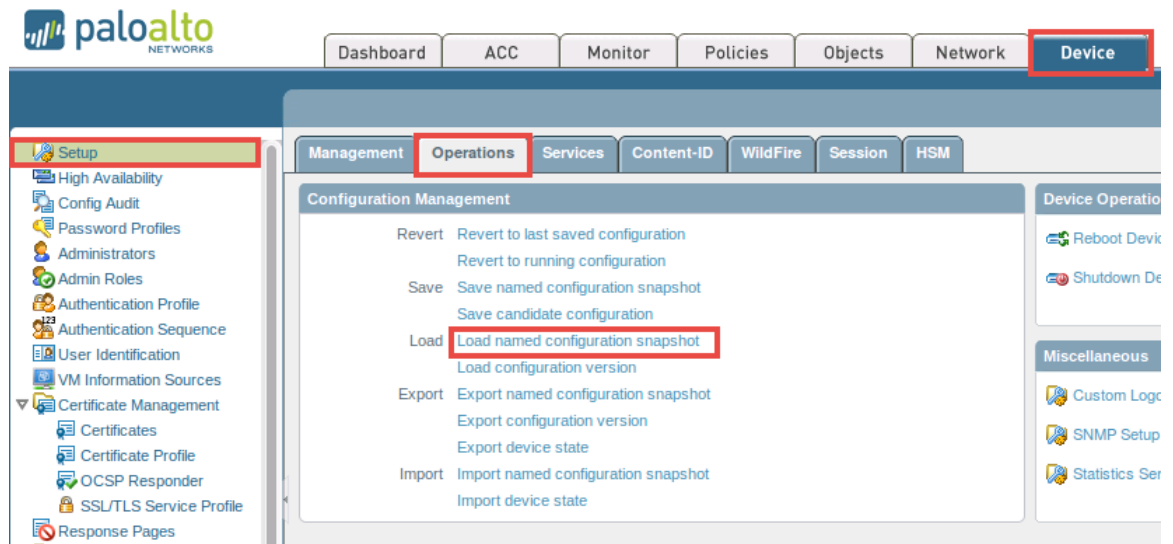
4. In the address field, type **https://192.168.10.1** and press **Enter**.

If you experience the “Unable to connect” message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

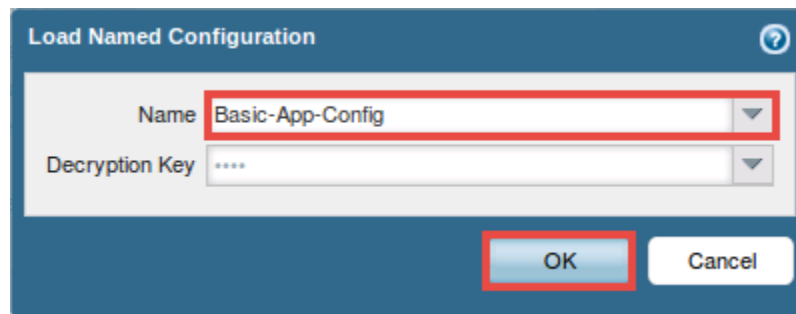
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



- Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



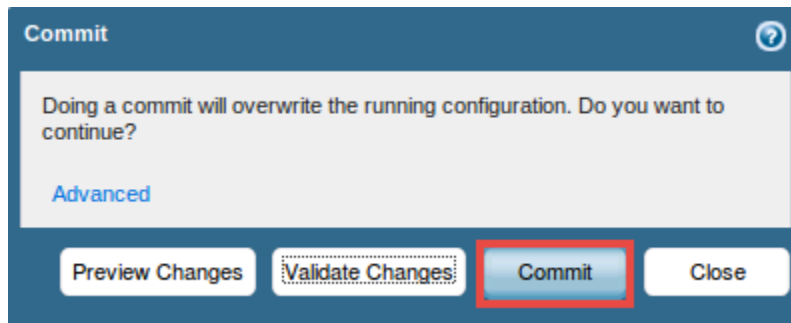
- In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.



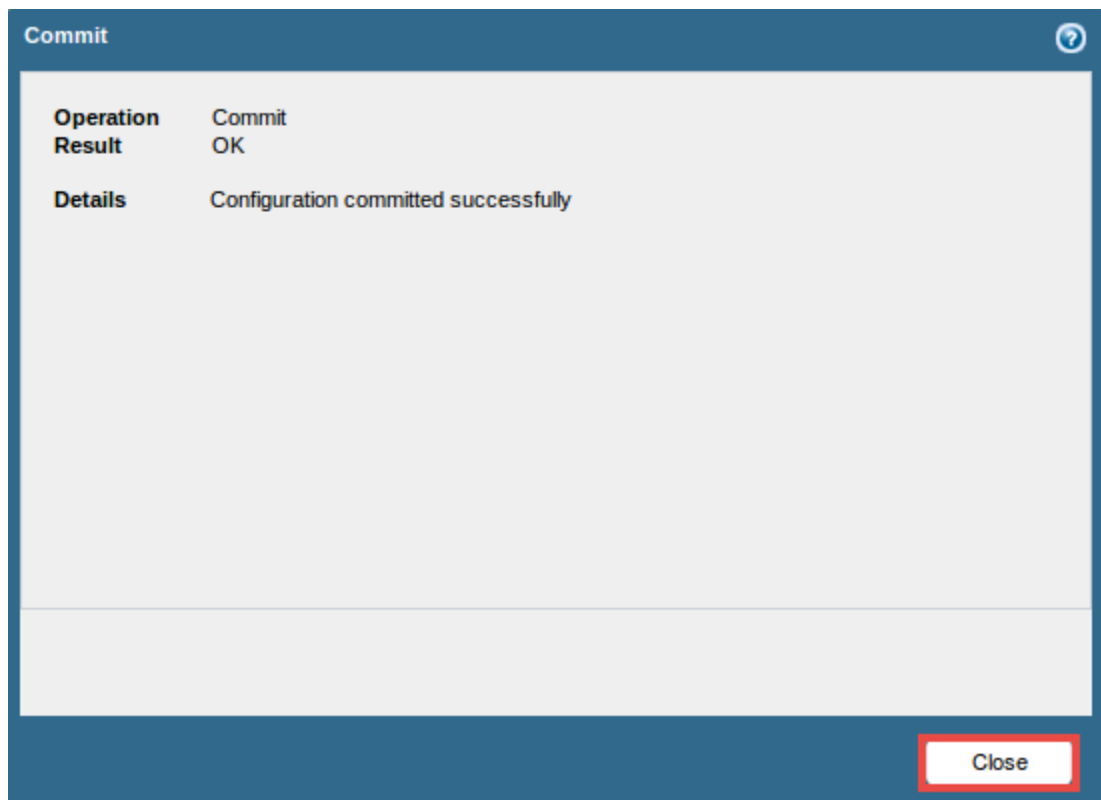
- When prompted with the config loaded message, click on the **Close** button to continue.
- Click on the **Commit** link located at the top-right of the *WebUI*.



10. In the *Commit* window, click **Commit** to proceed with committing the changes.



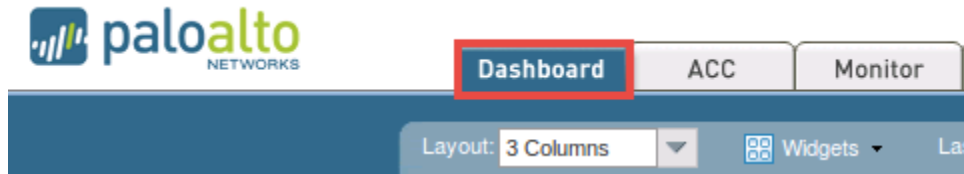
11. Once the operation successfully completes, click **Close** to continue.



12. Leave the *WebUI* opened to continue with the next task.

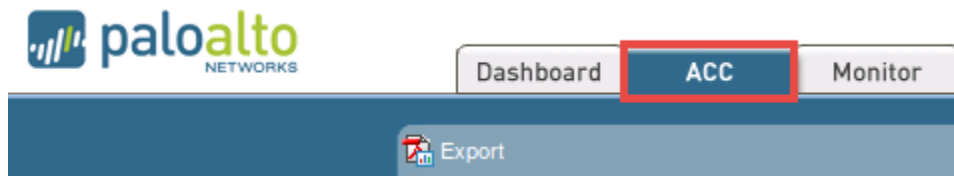
2 Explore the Dashboard, ACC, App Scope, and Session Browser

1. Using the *WebUI*, navigate to the **Dashboard**.

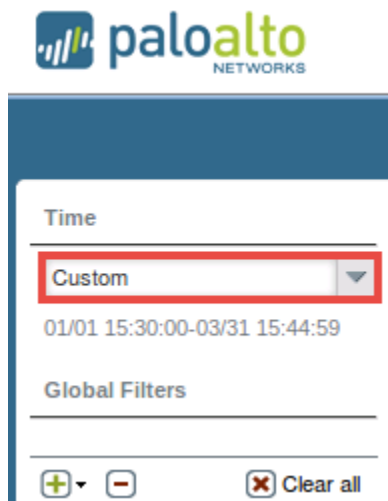


2. Review the contents of the available widgets. What information is available?

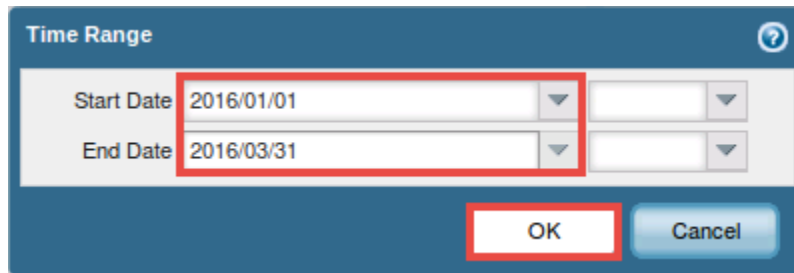
3. Navigate to the **ACC** tab.



4. Change the *Time* period to the **Custom**.



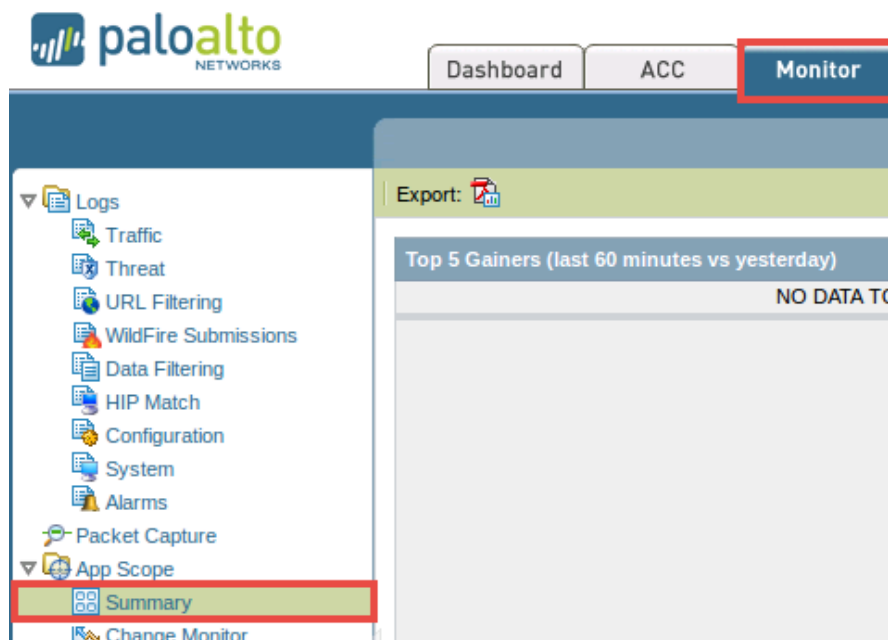
5. In the *Time Range* window, enter 2016/01/01 as the *Start Date* and select **Current Date** as the *End Date*. Click **OK**.



The image shows a 'Time Range' dialog box with a blue header and a white body. It contains two date pickers: 'Start Date' and 'End Date'. The 'Start Date' is set to '2016/01/01' and the 'End Date' is set to '2016/03/31'. Both date pickers are highlighted with a red rectangle. Below the date pickers are two buttons: 'OK' and 'Cancel'. The 'OK' button is also highlighted with a red rectangle.

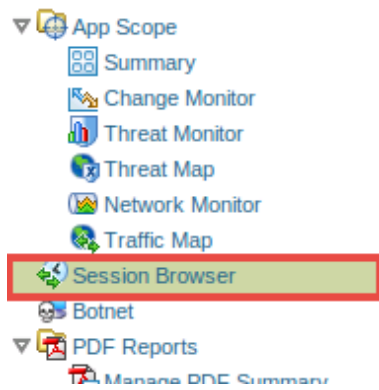
6. Explore the information on the **Network Activity** tab.
7. Explore the information available on the **Threat Activity** tab.
8. Explore the information available on the **Blocked Activity** tab.
9. Using the *WebUI*, navigate to **Monitor > App Scope > Summary**.

The summary will likely display a “NO DATA...” statement when going through the lab. This is due to the VM100 being reverted to a snapshot prior to bootup.



10. What information is available? Explore other branches underneath the *App Scope* tree in the left pane.

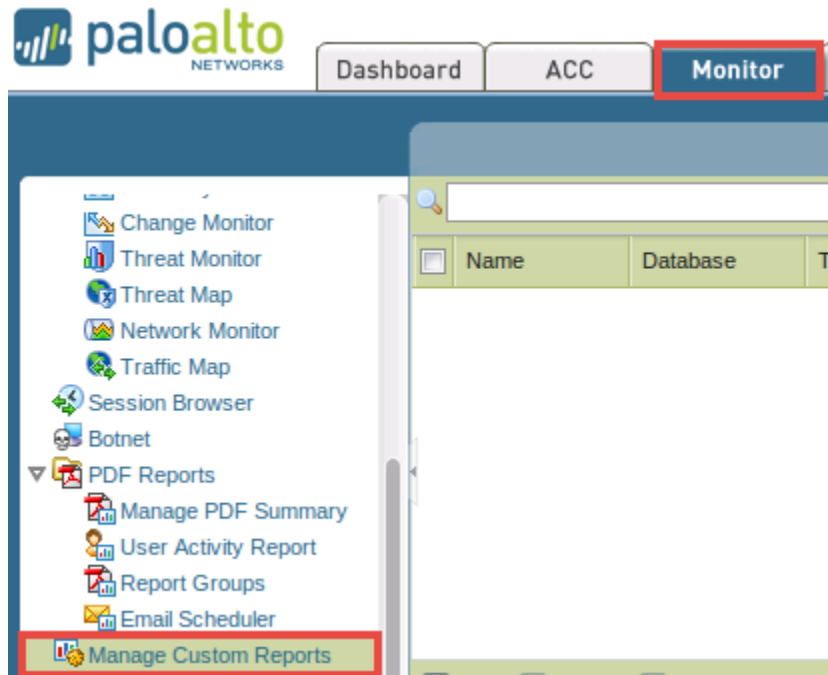
11. Click on **Session Browser** to view any current sessions.



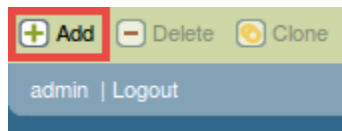
12. Leave the *WebUI* opened to continue with the next task.

3 Create a Custom Report

1. Using the *WebUI*, navigate to **Monitor > Manage Custom Reports**.

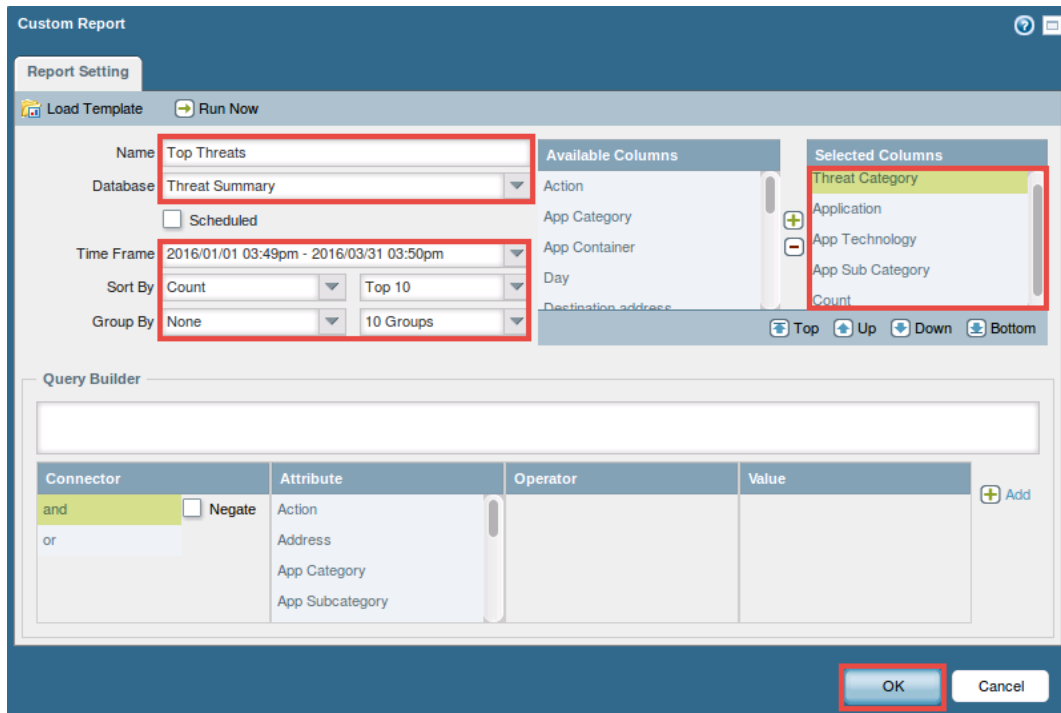


2. Click on **Add**, located near the bottom of the window, to define a new custom threat report.



3. In the *Custom Report* window, use the information from the table below to make appropriate configurations.

Field	Data/Selection
<i>Name</i>	Enter Top Threats
<i>Database</i>	Select Threat from <i>Summary Databases</i> in the <i>Databases</i> drop-down
<i>Time Frame</i>	Select Custom <i>Start Date: 2016/01/01</i> <i>End Date: 2016/03/31</i>
<i>Sort by</i>	Select Count and Top 10
<i>Group by</i>	Select None and 10 Groups
<i>Selected Columns</i>	Populate the Selected Columns field with these values, in this order (remove any values not listed): <ul style="list-style-type: none"> • Threat Category • Application • App Technology • App Sub Category • Count



The screenshot shows the 'Custom Report' window with the 'Report Setting' tab selected. The configuration is as follows:

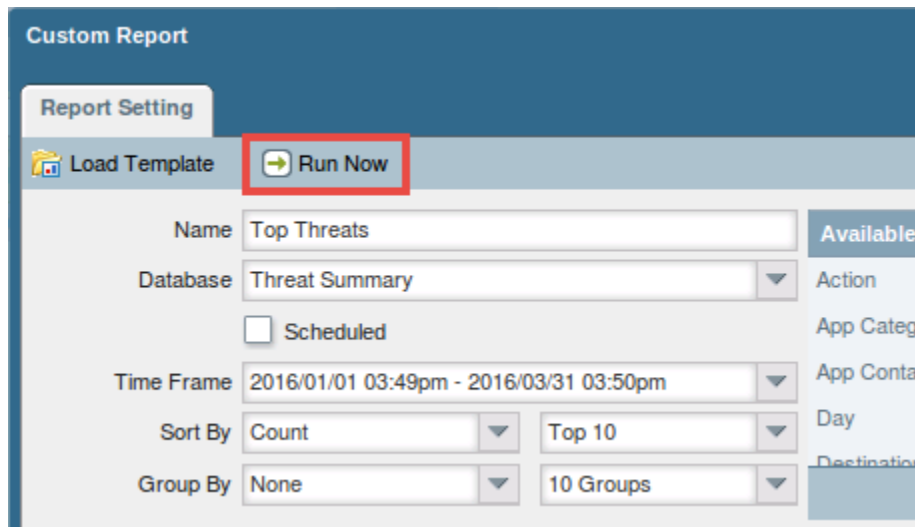
- Name:** Top Threats
- Database:** Threat Summary
- Scheduled:** ☐
- Time Frame:** 2016/01/01 03:49pm - 2016/03/31 03:50pm
- Sort By:** Count, Top 10
- Group By:** None, 10 Groups
- Available Columns:** Action, App Category, App Container, Day, Destination address
- Selected Columns:** Threat Category, Application, App Technology, App Sub Category, Count
- Query Builder:**
 - Connector: and (selected), Negate: ☐
 - Attribute: Action, Address, App Category, App Subcategory
 - Operator: (empty)
 - Value: (empty)
 - + Add button
- Buttons:** OK, Cancel

4. Click **OK** to save the custom report definition.
5. Verify that the *Top Threats* custom report appears in the list.

- Click on the **Top Threats** link in the *Name* column to reopen the *Custom Report* window.

<input type="checkbox"/>	Name	Database	Time Frame
<input checked="" type="checkbox"/>	Top Threats	Threat Summary	Last 7 Days

- In the *Custom Report* window, click on **Run Now** to generate the report.

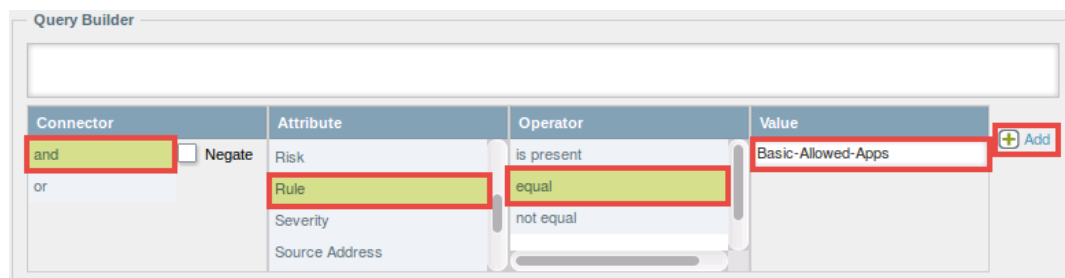


The screenshot shows the 'Custom Report' window with the 'Report Setting' tab selected. The 'Run Now' button is highlighted with a red box. Below the button, there are several input fields: 'Name' (Top Threats), 'Database' (Threat Summary), 'Scheduled' (unchecked), 'Time Frame' (2016/01/01 03:49pm - 2016/03/31 03:50pm), 'Sort By' (Count), 'Top 10', 'Group By' (None), and '10 Groups'.

The report will appear in a new tab in the same window.

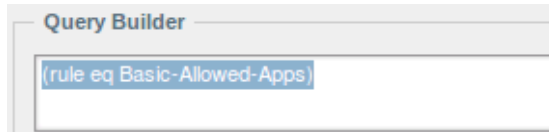
- Close the **Top Threats** tab and navigate back to the **Report Setting** tab.
- In the *Custom Report* window, create a query using the *Query Builder* located on the bottom pane. Use the information from the table below to configure the query parameters.

Field	Data/Selection
Query Builder	<p>Build a query using these parameters:</p> <ul style="list-style-type: none"> Connector: Select and Attribute: Select Rule Operator: Select equal Value: Enter Basic-Allowed-Apps Click Add

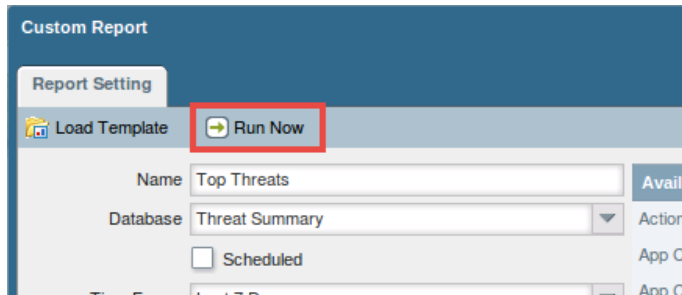


The screenshot shows the 'Query Builder' window. It has a table with four columns: 'Connector', 'Attribute', 'Operator', and 'Value'. The 'Connector' column has 'and' selected. The 'Attribute' column has 'Rule' selected. The 'Operator' column has 'equal' selected. The 'Value' column has 'Basic-Allowed-Apps' entered. An 'Add' button is visible on the right side of the table.

10. Verify that the *(rule eq Basic-Allowed-Apps)* query appears in the *Query Builder*.



11. Click on **Run Now** to run the report again, this time with the query.



12. On the new *Top Threats* tab, click **Export to PDF** to save the report as a PDF.

13. In the *Save To* window, choose the **Downloads** directory and click **Save**.

14. Click **OK** to close the Custom Report window.

15. Close the **Desktop 1** PC viewer.