

Barracuda Report Creator

<https://campus.barracuda.com/doc/48203132/>

The Barracuda Report Creator creates customized reports using statistics and logs collected on NextGen Firewalls. Each report can be configured to use multiple appliances, custom or predefined report data templates, and a customizable layout and delivery method. Reports for managed firewalls are collected directly from the firewall and not the Control Center. Custom reports can include the following information:

- **User Activity Reports** - Includes information on traffic caused by individual users, IP addresses or networks, or Active Directory user groups.
- **Address Activity Reports** - Includes information for accessed URL categories per source IP address or network.
- **URL Category Reports** - Includes information on which URLs were accessed in this specific URL category per source IP address or network.
- **Application Category Reports** - Includes information on detected application categories.
- **Application Property Reports** - Includes information on top blocked or allowed application properties.
- **Applications Reports** - Includes information on detected applications in a specific application category per source IP address or network.
- **Security Reports** - Includes IPS, Virus Scanner, and ATP threat reports.
- **VPN Usage Reports** - Includes information on usage of TINA client-to-site and site-to-site tunnels.

Limitations

- Microsoft .NET Framework 4.0 Client Profile is not contained in the installation archive for the Report Creator.
- Application Control data displayed in the Report Creator might not include the entire data set for the specified time period because old data may be deleted on the F-Series if the disc space gets too low. Due to this limitation, the Report Creator is not suitable for comprehensive auditing purposes. In this case, use FW Audit instead. For more information, see [FW Audit](#).

Installation and requirements

| | |
|-------------------------------|---|
| Operating System | Microsoft Windows 7, or higher |
| Additional Requirement | Microsoft .NET Framework 4.0 Client Profile |

Download the Report Creator from the [Barracuda Download Portal](#), double-click to start the installation, then follow the on-screen instructions.

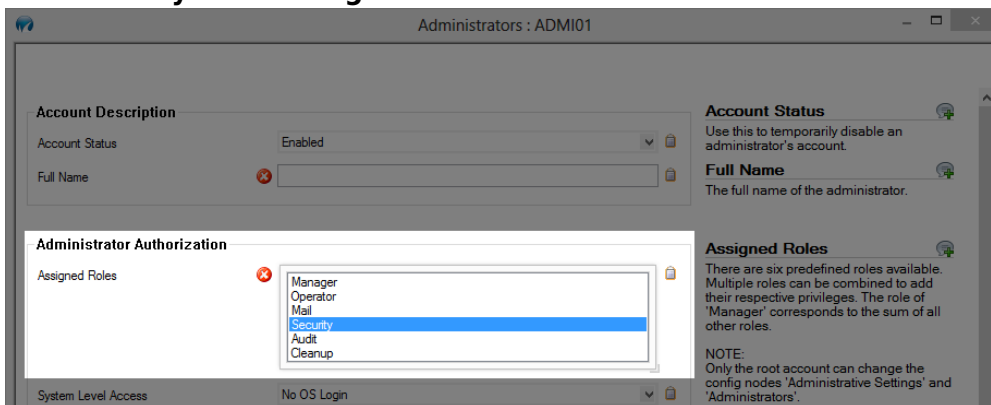
Step 1. Add dedicated Report Creator administrator

Add a dedicated administrator or a CC admin for Report Creator depending on if you are connecting to a standalone or managed firewall:

Stand-alone firewall

The administrator must be included in the **Security** role:

1. On the Firewall, go to **CONFIGURATION > Configuration Tree > Box > Administrators**.
2. Click **Lock**.
3. Create or edit the administrator account to be used by the Report Creator.
4. Add **Security** to the **Assigned Roles** for the administrator.

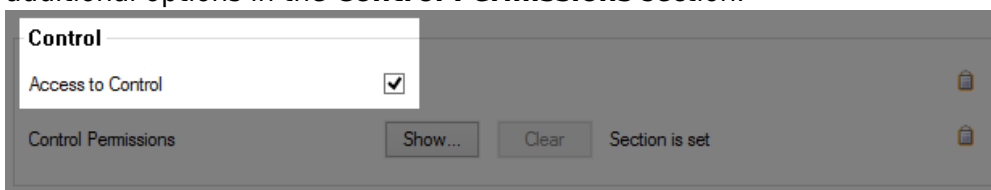


5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Control Center

The CC administrator must have access to the **Control** and **Firewall** modules.

1. On the Control Center, go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Administrative Roles**.
2. Click **Lock**.
3. In the **Administrative Role Configuration**, click **+** to add a new role.
4. In the **Control** section, select the **Access to Control** check box. You do not have to enable any additional options in the **Control Permissions** section.



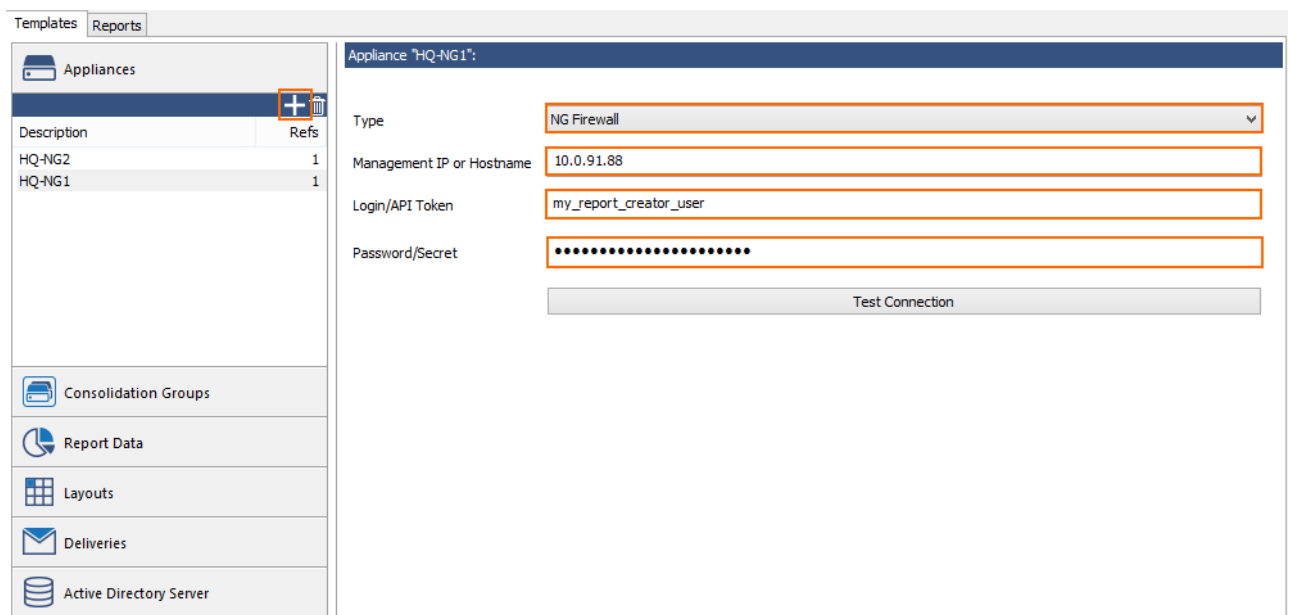
5. In the **Firewall service** section, select the **Access to Firewall** service check box. You do not have to enable any additional options in the **Firewall service** section.

6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 2. Add your firewall

Add the Firewalls to be queried when creating a report. Use the administrator user created in Step 1 to connect.

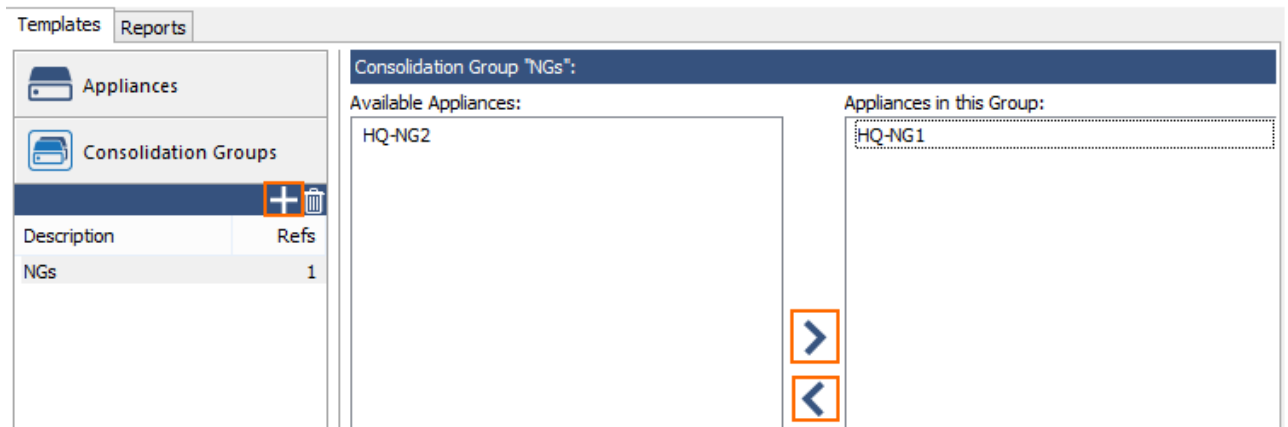
1. Click the **Templates** tab.
2. In the **Appliances** section in the left pane, click the plus sign.
3. Select **NextGen Firewall F-Series** from the **Type** list.
4. Enter the **Management IP** or **Hostname** of the Firewall.
5. Enter the **Login** and **Password**.
6. Click **Test Connection** to verify that the Report Creator can connect to the appliance.
7. Click **Save**.



The screenshot shows the 'Appliances' configuration page in the Barracuda Report Creator. The left sidebar has a plus sign icon next to the 'Appliances' section. The main area shows the configuration for 'Appliance *HQ-NG1*'. The configuration fields are: Type (NG Firewall), Management IP or Hostname (10.0.91.88), Login/API Token (my_report_creator_user), and Password/Secret (masked with dots). A 'Test Connection' button is visible at the bottom.

If you are creating reports for a large number of firewalls, sort them into **Consolidation Groups**:

1. Click the **Templates** tab.
2. In the left menu, click **Consolidation Groups**.
3. Click the plus sign.
4. Right-click the group name, select **rename**, and enter a name.
5. In the **Consolidation Group "Group name"** section, select the firewalls you want to add and click the right arrow icon to add them to the **Appliances in this Group** list.



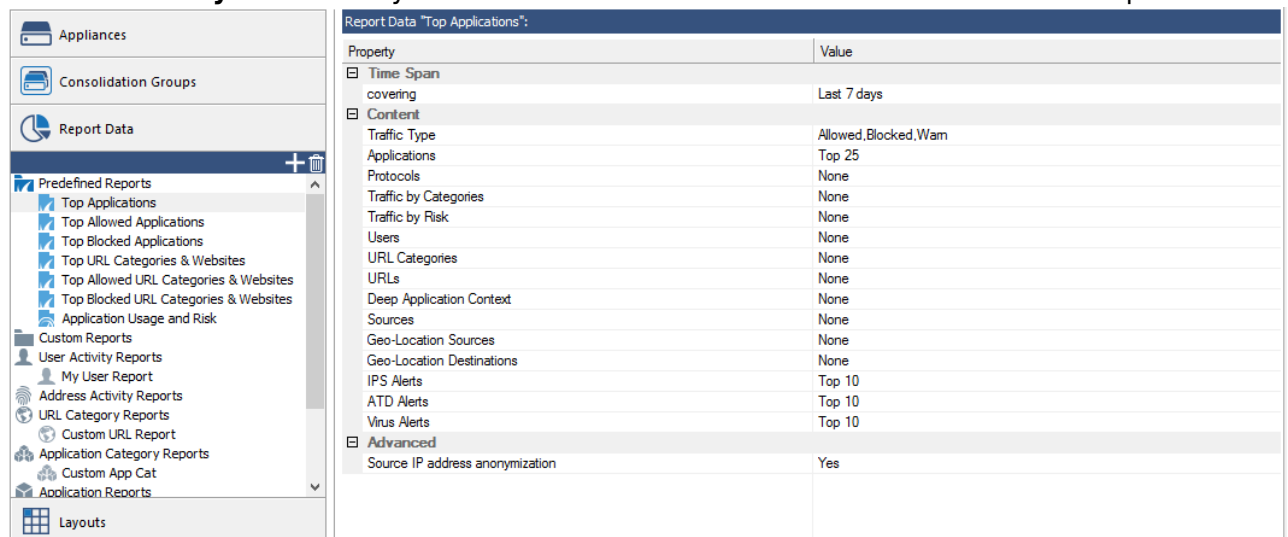
6. Click **Save**.

The Report Creator is now configured to create reports containing selected data from your Firewalls.

Step 2. Configure report data

The **Report Data** templates specify the type of information included in the report.

1. Click the **Templates** tab.
2. In the left menu, click **Report Data**.
3. To modify the settings, select the predefined report in the **Report Data** section.
4. Change the settings as necessary. For example, change the time span, or enable **Source IP Address Anonymization** if you do not want to include the source address in the report.



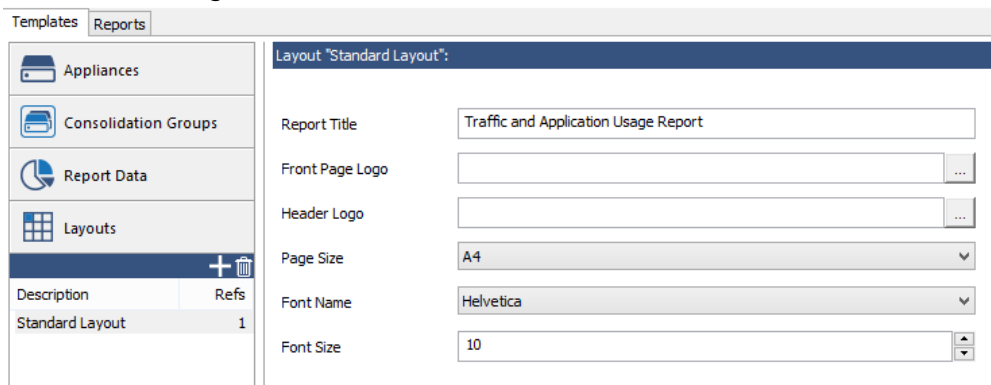
5. Click **Save**.

You can use custom or predefined reports. For more information, see [How to Create Custom Reports](#).

Step 3. Configure the report layout

Create a **Report Layouts** template to configure how the report is displayed.

1. Click the **Templates** tab.
2. In the left menu, click **Layouts**.
Either select the **Standard Layout** default template or create a new template by clicking the plus sign.
3. Right-click the template name, select **rename**, and enter a name.
4. Configure the following settings for the layout:
 - **Report Title** - The heading text that is displayed on the first page of the report.
 - **Front Page Logo** - The larger image that is displayed on the first page of the report. This image must be in PNG format. Your custom logo image is not automatically resized. Use images with a maximum width of 500 pixels.
 - **Header Logo** - The small logo that is displayed in the headline. This image must be in PNG format and have a maximum height of 44 pixels. The custom header image is automatically resized to 155 X 44 pixels. Upload it in multiples of these values to get the best results.
 - **Page Size** - The print page size.
 - **Font Name** - The font used in the report.
 - **Font Size** - The size of the font for the continuous text. Headlines have a fixed size that cannot be changed.



5. Click **Save**.

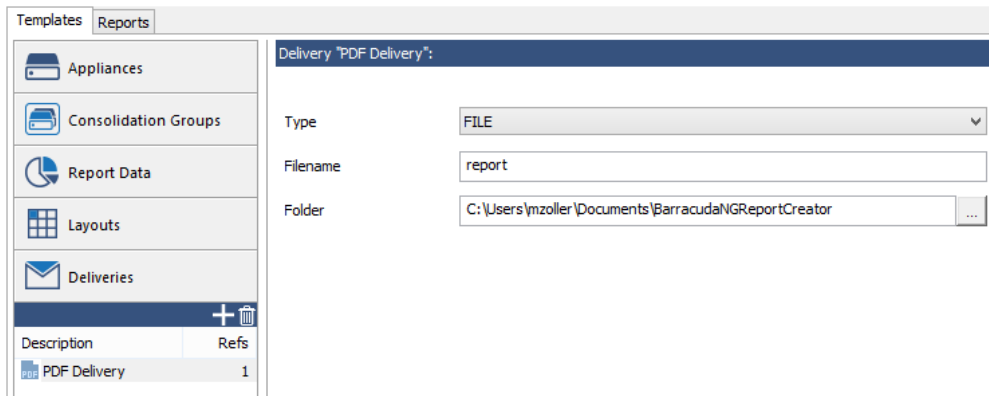
Step 4. Configure report delivery

Create a **Deliveries** template to specify how the reports are delivered. You can either store reports in a local directory or email the reports.

1. Click the **Templates** tab.
2. In the left menu, click **Delivery**.

3. Click the plus sign.
4. Right-click the template name, select **rename**, and enter a description.
5. To store the reports in a local directory, select **FILE** from the **Type** list and then configure the following settings:

- **Filename** - The report's file name. When the report is generated, a time stamp is appended to the report name. For example, report_2013_08_06_09_53_50.pdf.
- **Folder** - The folder where the reports are saved.



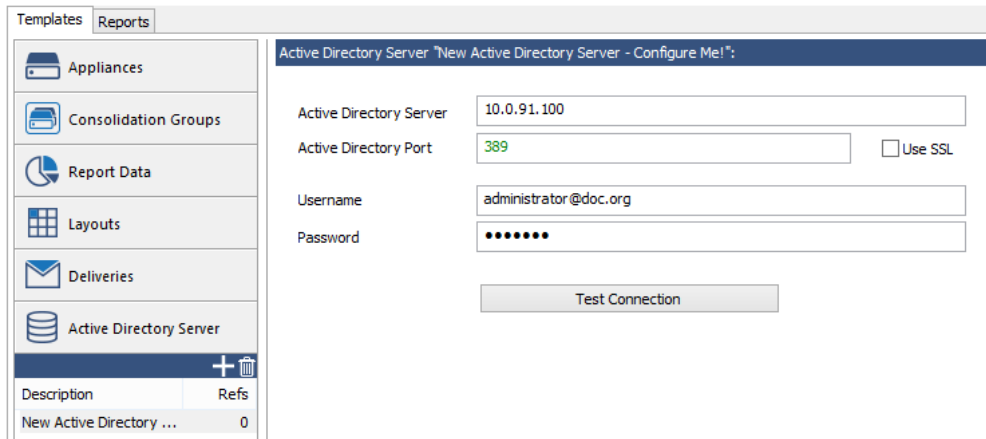
6. To email reports, select **EMAIL** from the **Type** list and then configure the following settings:
 - **Sender** - The sender email address.
 - **Recipient(s)** - The email addresses that should receive the report. Separate multiple addresses with a semicolon (;).
 - **Mail Text** - (Optional) Text for the email body.
 - **Server Address** - The IP address of the email server.
 - **Port** - The SMTP port on the email server to connect to. Common default values are:
 - **25** - Anonymous sending.
 - **587** - TLS authenticated sending.
 - **Force TLS encryption** - Enables authenticating at the email server, with the username and password configured below. This option requires a valid **Sender Address**.
 - **Use anonymous authentication** - Allows use of the email server without a username and password. This option does not require a valid **Sender Address**.
 - **User Name** and **Password** - If required, the credentials to authenticate on the email server.
7. Click **Save**.

Step 5. (optional) Add Active Directory server

To be able to generate reports based on Active Directory user groups, you must configure the IP address and login credentials for the Active Directory server.

1. Click on the **Templates** tab.
2. In the left menu, click **Active Directory Server**.
3. Click the plus sign.
4. Right-click the template name, select **rename**, and enter a description.

5. Enter the IP address or hostname of the **Active Directory Server**.
6. Enter the **Active Directory Port**. Default: 389
7. (optional) If required, select **Use SSL**.
8. Enter the **Username** of the active directory user.
9. Enter the **Password** of the active directory user.
10. Click **Test Connection** to verify that the Barracuda Report Creator can connect to the appliance.



The screenshot shows the 'Active Directory Server' configuration page in the Barracuda Report Creator. The page is titled 'Active Directory Server "New Active Directory Server - Configure Me!:"'. On the left, there is a navigation menu with options: Appliances, Consolidation Groups, Report Data, Layouts, Deliveries, and Active Directory Server. The 'Active Directory Server' section is currently selected. The main configuration area contains the following fields:

- Active Directory Server: 10.0.91.100
- Active Directory Port: 389 (with a checkbox for 'Use SSL' that is unchecked)
- Username: administrator@doc.org
- Password: (masked with dots)

At the bottom of the configuration area, there is a 'Test Connection' button. Below the configuration area, there is a table with columns 'Description' and 'Refs'. The table contains one entry: 'New Active Directory ...' with a value of '0' in the 'Refs' column.

11. Click **Save**.

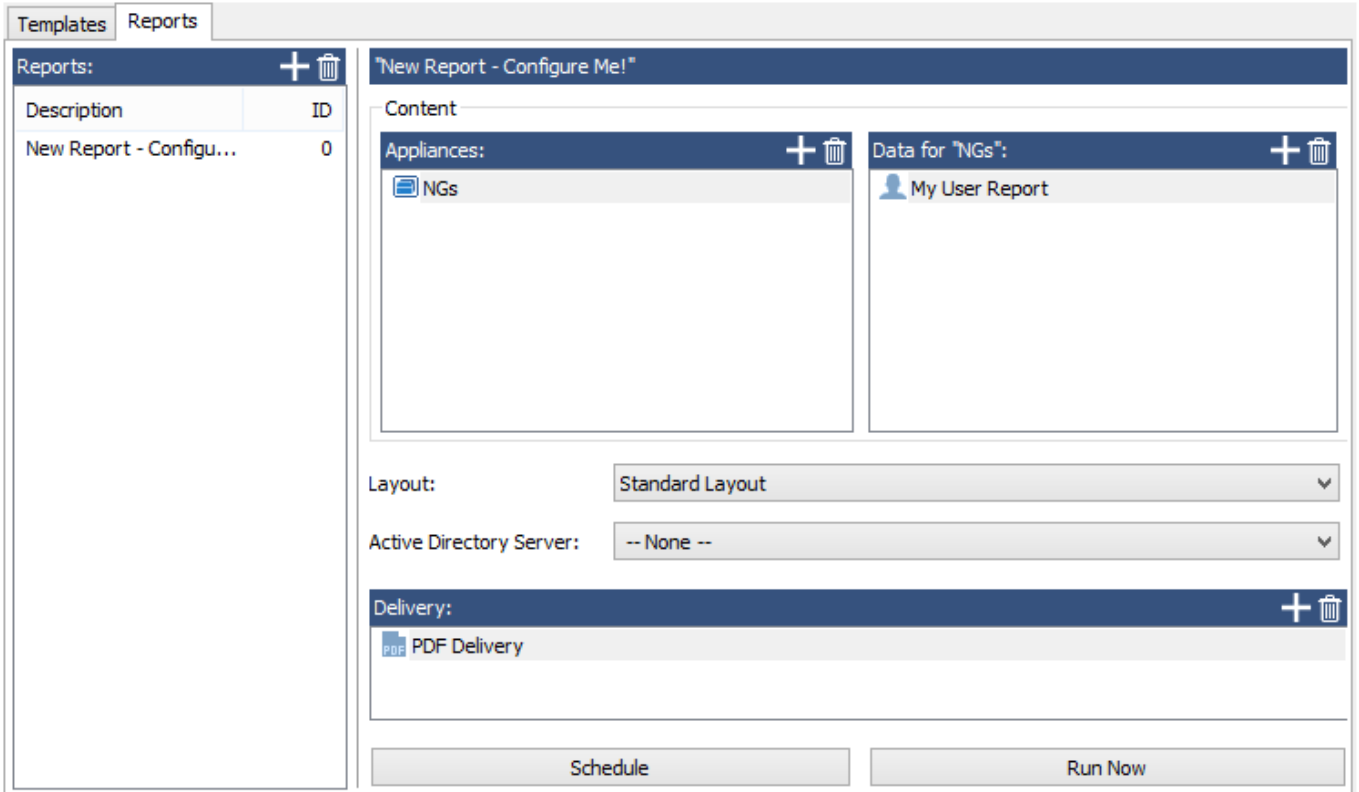
Step 6. Generate a report

After setting up the Report Creator, you can generate a report.

1. Click the **Reports** tab on the upper left of the window.
2. In the **Reports** section in the left menu, click the plus sign.
3. Left-click the template name, select **rename**, and enter a name for the report.
4. In the **Content** section of the main pane, repeat the following steps for each appliance or consolidation group you want to add to the report:
 1. In the **Appliances** section, click the plus sign and then select the consolidation group or appliance.
 2. In the **Data for "your appliance name"** section, click the plus sign and then select the types of reports that you want to generate.
5. Select the **Layout** from the list.
6. In the **Delivery** section, click the plus sign and then select the delivery method you previously configured:
 - **EMAIL** - Sends the report to the email address specified in the **Deliveries** template.
 - **FILE** - Saves the report in the location path specified in the **Deliveries** template
7. Click **Save**.

Step 7. Run the report

Click **Run Now** to generate the report. The report is sent to your desktop or delivered via email, depending on the configuration of the selected **Deliveries** template.



| Description | ID |
|-------------------------|----|
| New Report - Configu... | 0 |

Content

Appliances:

- NGs

Data for "NGs":

- My User Report

Layout: Standard Layout

Active Directory Server: -- None --

Delivery:

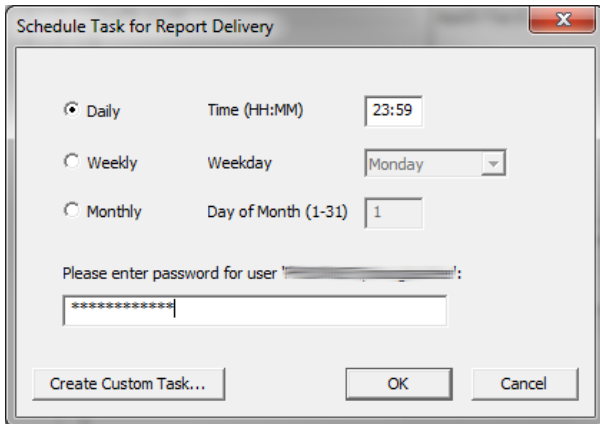
- PDF Delivery

Schedule Run Now

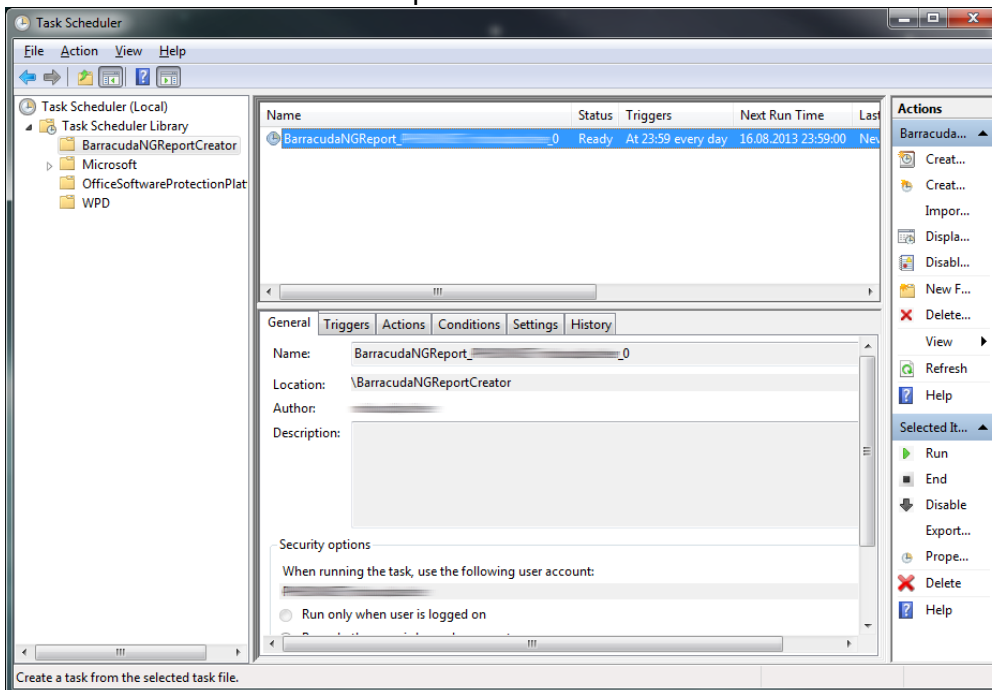
Step 8. Automate report creation

To automate the reporting, schedule a task and specify how often the report is generated.

1. Click the **Reports** tab.
2. In the left pane, select a report.
3. Click **Schedule**.
4. In the **Schedule Task for Report Delivery** window, specify the delivery times for the report and enter the password for your Windows user.



5. To open the Windows Task Scheduler, click **Create Custom Task**. Report Creator tasks are stored in the BarracudaNGReportCreator subfolder.



- 6. Click **OK**. Your scheduling task is created in the Windows Task Scheduler.
- 7. Save your configurations.

Using keyboard shortcuts

You can use various keyboard shortcuts within the Report Creator:

| Keyboard Shortcut | Action |
|-----------------------|--|
| Tab, Shift+Tab | Move forward or backward through the currently visible controls. |
| Ctrl+Tab | Move between the Templates and Reports pages. |
| F2 | Rename the selected item. |

| | |
|--------------|---|
| Del | Delete the selected item. |
| Alt+S | Save the current configuration. |
| Alt+E | Exit the configuration UI without saving your changes. |
| Alt+D | Schedule a task for the currently selected report. You can use this shortcut only in the Report tab. |
| Alt+R | Create a report. You can use this shortcut only in the Report tab. |

Figures

1. securityrole.png
2. controlmodule.png
3. report_creator_01.png
4. report_creator_02.png
5. report_creator_03.png
6. report_creator_04.png
7. report_creator_05.png
8. report_creator_06.png
9. report_creator_07.png
10. ReportCreatorSchedules.png
11. ReportCreatorScheduleTask.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.