

How to Use Scheduled Reports

<https://campus.barracuda.com/doc/6553622/>

This documentation applies to the Barracuda Web Security Service sold **prior** to April 1, 2017. As of this date, the service is still maintained, while new customers can purchase the new Barracuda Web Security Service cloud based solution powered by Zscaler, the leading cloud web security solution for enterprises. Click [here](#) for documentation on the **new** Barracuda Web Security Service.

Manage reports for the Barracuda Web Security Service by accessing your Barracuda Cloud Control login.

You can schedule reports to run automatically at regular intervals you choose, such as at the conclusion of mandatory reporting periods. You can configure Barracuda Web Security Service Manager to email scheduled reports (in .pdf format) to groups or individuals.

Viewing and Editing Existing Reports

Select the **REPORTS** tab then select **Scheduled** to view a list of all currently scheduled reports. To edit an existing report, click the report's name.

Creating a Scheduled Report

1. In the Barracuda Web Security Service Manager, click the **REPORTS** tab, and then click **Scheduled**.
2. Click **Add New**. The **Scheduled Report Settings** page appears.
3. Enter a **Name** for the report.
4. Select the time **Period** you want to report on.
5. Select a **Delivery Schedule** to control how frequently the Barracuda Web Security Service Manager creates the report.
6. Select whether you want the report to cover all users or a group of users. If you choose **Group**, the Barracuda Web Security Service Manager displays a text box for you to define which groups you want to cover.

If you configured the Barracuda Web Security Service to integrate with your existing directory service, rather than defining local groups in the Barracuda Web Security Service Manager, you must add the group names on the **CONFIGURATION > Group Management** page to use them here for group-based reporting.

7. Enter the email addresses of report recipients in the **To Addresses** field.
8. Choose the reports you want to generate by clicking the caret(s) to expand the **Traffic Reports**

and **User Browsing** areas. You can select one or more **Traffic Report(s)** and/or **User Browsing** reports within the same schedule. See below for additional configuration instructions for each section.

9. When you are finished, click **Save**.

Group-based scheduled reports are available only for **User Browsing** reports.

Configuring Traffic Reports

- Both the **Show Chart** and **Show Table** checkboxes are selected by default. You can deselect one of them if you want the report to focus on the other.
- If you chose one of the **Top** instances reports, use the **Top** drop-down to choose the number of instances you want the report to include.

Configuring User Browsing Reports

- Choose between **Summary view**, which provides an overview of activity, and **Activity view**, which examines activity data in greater detail.

Deleting a Scheduled Report

1. In the Barracuda Web Security Service Manager, click the **REPORTS** tab, and then click **Scheduled**.
2. Select the **Delete** checkbox next to the report(s) you want to delete.
3. Click **Delete Selected**.

Editing a Scheduled Report

1. In the Barracuda Web Security Service Manager, click the **REPORTS** tab, and then click **Scheduled**.
2. Select the report you want to edit.
3. Make your changes, and then click **Save**.

Report Descriptions

The following table lists the reports shipped with Barracuda Web Security Service Manager and provides brief descriptions of their contents. Use the instructions in the preceding sections to

generate an Immediate report or schedule a report to run automatically.

Report	Description
Protocol - Bytes In	Incoming byte totals for a time period you specify, broken out by protocol. Example protocols are HTTP, HTTPS, and FTP.
Protocol - Bytes Out	Same as above, but bytes outgoing.
Protocol - Connections	Number of connections per time, broken out by protocol.
Top Applications Blocked	Most frequently blocked Applications and the number of times each has been blocked.
Top Blocked Categories	Most frequently blocked Categories and the number of times each has been blocked.
Top Blocked Viruses	Most frequently blocked virus programs and the number of times each has been blocked.
Top Categories - Bytes In	Top categories of incoming web traffic, measured in bytes.
Top Categories - Bytes Out	Top categories of outgoing web traffic, measured in bytes.
Top Categories - By Time	Top categories of web traffic, based on time spent surfing.
Top Categories - Connections	Top categories of web traffic, measured in number of connections.
Top Sites	Top requested websites. Shows number of requests per site. All pages within a site are included.
Top Sites - By Time	Top sites visited, based on time spent surfing.
Top Users - Application Blocks	Shows who is causing the most blocked Applications and the number of times each has been blocked.
Top Users - Bytes In	Top users, measured in bytes in and broken out by protocol. Example protocols are HTTP, HTTPS, and FTP.
Top Users - Bytes Out	Top users, measured in bytes out and broken out by protocol. Example protocols are HTTP, HTTPS, and FTP.
Top Users - By Time	Top users based on time spent surfing.
Top Users - Connections	Top users based on number of connections made out to the Internet.
Top users by Malware Blocked	Shows who is causing the most Malware to be blocked and the number of blocks.
Top users by Virus Blocked	Shows who is causing the most viruses to be blocked and the number of blocks.
Total traffic - Bytes In	Total amount of incoming traffic for all protocol types, measured in bytes.
Total traffic - Bytes Out	Total amount of outgoing traffic for all protocol types, measured in bytes.
Total traffic - Connections	Total amount of outgoing traffic for all protocol types, measured in connections.
User Browsing Activity Report	Detail data on browsing activity of a specific user.

User Browsing Summary	Data on browsing activity of a specific user, rolled up to summarize overall activity and trends.
-----------------------	---

© 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.