Reporting

https://campus.barracuda.com/doc/84968187/

From the **Reports** page, select the device type for which you want to create reports.

Use the **Reports** pages to choose from more than 80 different reports that can help you keep track of data from the connected Barracuda Networks devices. You can either generate a report on-demand or configure the Barracuda Reporting Server to automatically generate reports. You can automatically generate reports on an hourly, daily, weekly, or monthly basis and email the reports to specific email addresses or send them to either an FTP or SMB server that you have configured on the Barracuda Reporting Server.

> If your Barracuda Reporting Server is sending reports via email through an email security product, such as Barracuda Email Security Gateway or Barracuda Essentials for Email Security, make sure to add the IP address of the Barracuda Reporting Server to the **IP and Port Exemptions** list on the **BLOCK/ACCEPT > IP Block/Exempt** page to prevent bad URLs from causing the emailed report to be blocked. If you are sending reports through another spam filtering device or service, make sure to allow the IP address of the Barracuda Reporting Server on that solution.

It is important to understand how time is calculated in reports. Refer to Browse Time Reporting for more information.

Specifying Filtering Options

> Reports and report options depend on the type of connected Barracuda Networks device. Refer to the online help for information on each report.

In the **Filtering Options** section, specify the following:

- **Time Frame** – Select a time frame from the list or select **Custom** and specify a particular **Start** date and time, along with a particular **End** date and time. Refer to Understanding Time Frames and Recurring Reports for important details.
- **Limit Report to** – *Web Security Gateway devices only.* Select one or more options from the list to limit output to an individual or group of users, groups, IP addresses, etc. Click the **Add** button to add another selection to your limit filtering.
  - **Authenticated Users** – Search for all authenticated users in the system.
  - **Unauthenticated Users** – Search for all users that are not authenticated in the system.

- **All Logged Users**– Search for all logged users in the system.
- **All Logged Groups** – Search for all logged groups in in the system.
- **Local User** – Type all or part of a user name, then click **Lookup** to search for that user. Use the wildcard character (*) when using only parts of the user name.
- **Local Group** – Select a group from the list, then click **Add**.
- **IP Address** – Enter one or more combinations of client IP Address and subnet mask that made requests to which you want to limit report results.
- **IP Group** – Select a group from the list, type all or part of a group name, then click Lookup to search for that group. Use the wildcard character (*) when using only parts of the group name. Then click **Add**.
- **NTLM User** – Select an NTLM directory, type all or part of a user name, then click Lookup to search for that user . Use the wildcard character (*) when using only parts of the user name. Then click **Add**.
- **NTLM Group** – Select an NTLM directory, type all or part of a group name, then click Lookup to search for that group. Use the wildcard character (*) when using only parts of the group name. Then click **Add**.
- **Google User** – Select a Google directory, type all or part of a user name, then click Lookup to search for that user . Use the wildcard character (*) when using only parts of the user name. Then click **Add**.
- **Google Group** – Select a Google directory, type all or part of a group name, then click Lookup to search for that group. Use the wildcard character (*) when using only parts of the group name. Then click **Add**.

- **Output Format** – Choose the output format and delivery options: HTML, PDF, Text, or CSV. Note:In CSV formatted reports, bandwidth data is expressed in raw bytes, not formatted with units (KB, MB, etc.). Choose CSV format if you want to generate your own graphs or formatted reports with other tools.
- **Report On** – From the list, select one or more connected Barracuda Networks devices for which you want reports.

Reports are aggregated by default. To isolate reports for a single connected device, select only that single device.

Specifying Advanced Options

Reports and report options depend on the type of connected Barracuda Networks device. Refer to the online help for information on each report.

In the **Advanced Options** section, you can optionally specify the following:

- **Traffic Type** – Specify whether to generate data for **All** traffic, for **Web Security Agent** only, or for **Remote Devices**.
- **Destination**– Select one of the following on which to filter:
  - **Domain** – If selected, you can list specific domains to include in the report or check the **Exclude Specified Domains** checkbox to exclude a domain from the report.
  - **Category** – If selected, you can select several categories from the drop-down list, which you can either include in the report or exclude by clicking the **Exclude Selected Categories** checkbox.
- **Exclude Timeframe** – To exclude certain times of day from report data (e.g., lunch hour or weekend days), enter the **From** and **To** times in HH:MM format and select the one or more days of the week to exclude.
- **Action** – Check the box for one or more request types that you want to include in the report results. Request types include: **Allow**, **Block**, **Warn**, and **Monitor.**
- **Chart Type** – For most reports, you can choose to include a graphical representation of the primary data. Select **Vertical Bars**, **Horizontal Bars**, or **Pie Chart,** as applicable to the report. You can only view charts when the **Output Format**, specified above, is either **HTML** or **PDF**.
- **Drill-Down Limit Level** – There are five possible values you can enter to limit the drill-down depth of the reports. To see all records, leave the fields blank.
  For example, if you select **Action** = **Blocked** above, and enter **10** in the first **Drill-Down Limit Level** box and run the **Top Users by Browse Time on Social Networking Sites** report, the generated report will be a **Top 10 Blocked Users by Browse Time on Social Networking Sites**. You can further limit the report by using the next **Drill-Down Limit Level** box, setting it to **3**, limiting drill-down results by Domains to a maximum of three domains.

Scheduling a Report

In the **Schedule Report** section, specify the following:

- **Report Name** – Type a unique, meaningful name for this report.
- **Delivery Option** – Specify how you want to receive the results of this report, **Email** or **External Server**.
  - **Recipients** – If you specified **Email** as the Delivery Option, specify one or more email addresses here, separated by commas.
  - **External Server** – If you specified **External Server** as the Delivery Option, select an External Server from the list.
    Specify External Servers on the **ADVANCED > External Servers** page.
- **Frequency** – Specify how often you want this report to run:
  Refer to Understanding Time Frames and Recurring Reports for important details.
  - **Once** – The report runs immediately.
  - **Hourly** – The report will run immediately, then every hour thereafter.

    - **Daily** – Specify the hour, in 24-hour time, when you want the report to run each day.
    - **Weekly** – Specify the day of the week and the hour, in 24-hour time, when you want to report to run each week.
    - **Monthly** – Specify the day of the month and the hour, in 24-hour time, when you want the report to run each month.
- **Split Report** – *Web Security Gateway devices only.* Specify if you want to split a report into sub-reports using **User/Group** or **Type**. This is helpful for delivering multiple reports to various recipients.
- **Disable** – Specify whether the report is enabled or disabled. You might choose to temporarily disable a report

Click **Schedule Report** to create the report and add it to the **Scheduled Reports** section below. Click **Save Changes** in the top right corner of the page if you are editing the report.

Scheduled Reports

This section lists all of the scheduled reports you have created.

Information in the Scheduled Reports table includes:

- **Name** – The name of the report, specified in the **Schedule Report** section.
- **Report Type** – The report type, specified by selecting check boxes in the **Reports** sections.
- **Frequency** – How often the report will run, specified in the **Schedule Report** section.
- **Time Frame** – The time frame from which the report will use data, specified in the **Filtering Options** section.
- **Delivery Option** – Whether the report will be sent via email or to an External Server, specified in the **Schedule Report** section.
- **Status** – Whether the report is **Enabled** or **Disabled**, specified in the **Schedule Report** section, described above.

Reports created to run only once are not listed in this table. If you create or edit a scheduled report to run only once, it will be listed here very briefly before it is run.

Taking Action with Reports

- **Remove** – Deletes the report from the Barracuda Reporting Server. If you think you might use this report in the future, consider marking the report as **Disabled** in the section above.
- **Run Now** – Starts the report immediately. Does not change the reports status for future reports.
- **Edit** – Opens the report for editing in the sections above. Be sure to click **Save Changes** in the top right corner of the page to update the report.