30 Day Evaluation Guide - Barracuda Reporting Server

https://campus.barracuda.com/doc/84968217/

Where to Start

Begin with the Barracuda Reporting Server Quick Start Guide. This guide is also included in printed form with your Barracuda Reporting Server. It will guide you in safe installation and initial configuration of your Barracuda Reporting Server.

For your model 600, you automatically have a Barracuda sales engineer assigned to help you make the most of your 30-day evaluation of the Barracuda Reporting Server. If you have not yet been contacted by a sales engineer, call your reseller or sales representative.

Deployment

Once you complete your deployment configuration, data begins forwarding to the Barracuda Reporting Server. Log into the web interface as the administrator, and go to the **BASIC > Dashboard** page. Processed data displays in the **REPORTS** tab.

Create and View Reports

Work with reports on the **REPORTS** tab.

For more information, refer to the article Reporting, or log into the Barracuda Reporting Server, go to the **REPORTS** tab, and click the Help ? icon.

Time-Based Retention Policies

Specify the log retention period for each connected device on the **BASIC > Administration** page, in the **Connected Device** section.

For more information, refer to the Administration article, or log into your Barracuda Reporting Server and go to the **BASIC > Administration** page, then click the Help ? icon.

Setting Up Email Notification

In the Email Notification section, specify how and where to deliver system alerts from the Barracuda Reporting Server.

- All of the fields in this section are required.
- Your email system must be able to handle large reports as attachments, on both the sending and receiving sides.

- **SMTP Host** – Name of your SMTP host to use for sending notifications, not localhost.
- **SMTP Port** – Network port for your SMTP host.
- **Connection Security** – Select the type of security for your email system, TLS or None.
- **Username** – Login username for your email system, if required by your SMTP host.
- **Password** – Password corresponding to the Username for your email system, if required by your SMTP host.
- **System Alerts Email Address** – Type one or more email addresses that receive automated alerts from the Barracuda Reporting Server, including system messages and notifications about available firmware updates. Separate multiple email addresses with a comma.
- **From Email** – Specify the address to use as the From address for system alert emails.
- **Test SMTP Configurations** – Type an email address to receive a test email. Click Send Test Email to ensure that the email system works.

View Performance Statistics

View performance statistics on the **BASIC > Dashboard** page, in the **Connected Devices** and **System Status** sections.

For more information, refer to the Dashboard article or log into the Barracuda Reporting Server, go to the **BASIC > Dashboard** page, and click the Help ? icon.

Common Use Cases

Use Case 1: Monitoring

The Barracuda Reporting Server dashboard enables you to monitor your connected devices in one location.

To use the Dashboard to monitor connected devices:

1. Set up your Barracuda Reporting Server and connect Barracuda Networks devices to it, following the instructions in Getting Started.
2. Within the Barracuda Reporting Server, navigate to the **BASIC > Dashboard** page.
   On the Dashboard, you can monitor:
   - **Device Statistics** for the connected devices you select
   - **Productivity** statistics for connected devices you select
   - **Connected Devices** status
   - **System Status** for this Barracuda Reporting Server device
   - **Storage** space for this Barracuda Reporting Server device
   - **Web Activity**, displaying the ratio of HTTP:HTTPS traffic

Notifications are available as a means of monitoring your environment. Refer to **Use Case 4: Alerting** below for more details.

By default, data on the Dashboard automatically refreshes every 30 minutes. You will not be automatically logged out of the dashboard.

Refer to Dashboard for details on using the Dashboard to monitor connected devices.

Use Case 2: Reporting

The Barracuda Reporting Server can create ad hoc reports (one-off reports created immediately) and scheduled reports. The first two steps of the process are the same.

1. Set up your Barracuda Reporting Server and connect Barracuda Networks devices to it, following the instructions in Getting Started.
2. Within the Barracuda Reporting Server, navigate to the **REPORTS** page.
3. In the **Filtering Options** section, select the **Time Frame**, **Output Format** (HTML, PDF, Text, or CSV), and which connected devices you want to include.
   If you do not make any selections in this section, the default settings will create a report for Today, in HTML, on all connected devices.

- **To create an ad hoc report**
  1. Scroll down to the section with all of the report types. Click the name of the report you want to generate.
     The report opens in a new tab as soon as it is created.
- **To create a scheduled report**
  1. (Optional) Configure an external server where you can save report logs. Navigate to the **ADVANCED > External Servers** page and refer to Working with External Servers for details.

2. Return to the **REPORTS** page and scroll to the **Reports** section. Select one or more reports you want to create.
3. Scroll down to the Schedule Report section. Configure the details on how you want the report to be delivered and how often. Click Schedule Report.
   When the report is created it will be sent to you via email or to the external server you specified.

Refer to Reporting in Barracuda Campus and to the Barracuda Reporting Server online help for details on creating reports.

Use Case 3: Aggregating Data Across Multiple Connected Barracuda Devices

The Barracuda Reporting Server enables you to monitor and create reports for multiple connected devices, viewed either individually or as a group.

- Viewing data per category enables you to see where resources are being used in each category across all connected devices.
- Viewing data across all connected devices saves you from monitoring each device separately. For example, you can view Flagged Terms across all connected devices, rather than separately for each individual device.

Refer to Dashboard and Reporting for information on selecting multiple connected devices for aggregated data.

Use Case 4: Alerting

The Barracuda Reporting Server offers two types of alerting – automatic notifications and scheduled reports.

Automatic Notifications alert you to the following types of events:

- Disconnected devices/connection errors – A warning on the dashboard and an email notification alert you to problems with device connections.
- Storage space – A warning on the dashboard and an email notification alert you if you are reaching storage capacity on the Barracuda Reporting Server.
- Subscription status – A warning on the dashboard alerts you if your subscriptions are about to expire or have expired.
- Flagged terms – Create a report to run at regular intervals to receive notifications about flagged terms on connected devices.

Emails alert you when **Scheduled Reports** are generated and sent. Reports are sent either to email addresses or to an external server. All reports can be scheduled to run at any frequency in any of the formats: HTML, PDF, Text, and CSV.

Refer to Administration for details on setting up email notification.

Refer to Reporting for details on scheduling reports.

Use Case 5: Migrating Scheduled Reports from Connected Devices

> **Note**
>
> Only connected Barracuda Web Security Gateway devices have scheduled reports that can be migrated to Barracuda Reporting Server. This feature is not available in Barracuda CloudGen Firewalls.

When you connect one or more Barracuda Web Security Gateway devices to a Barracuda Reporting Server, the scheduled reports automatically migrate to the Barracuda Reporting Server so you can run and manage them there.

To migrate scheduled reports:

1. *On the Barracuda Web Security Gateway, n*avigate to **BASIC > Administration** page.
    1. For **Connect to Barracuda Reporting Server**, select **Yes**, then specify the Barracuda Reporting Server's Shared Secret and IP address.
    2. Save your changes.
2. *On the Barracuda Reporting Server*, navigate to the **BASIC > Administration** page and scroll down to the **Connected Devices** section. Locate the newly connected device(s) and click **View Migrated Reports**.
3. In the **Scheduled Reports Migrated** dialog, note whether the reports were migrated successfully. If there is an error on a report, click **View Detail** to see any issues with a report.
4. Navigate to the REPORTS page and scroll down to the Scheduled Reports section. Newly migrated reports will display as Disabled.
5. Click **Edit** for a migrated report. Verify that its information is correct, click **Enabled**, and then click **Save Changes**.

- Refer to Migrating Reports to the Barracuda Reporting Server for details on the migration process from the Barracuda Web Security Gateway side.
- Refer to Step 5 - Verify Scheduled Reports Migrated from Connected Devices for details on the migration.
- Refer to Reporting for details on scheduling reports.

Figures