Barracuda Reporting Server - Overview

Required Product Version

Barracuda Reporting Server requires Barracuda Web Security Gateway version 11.0 or higher.

The Barracuda Reporting Server is a hardware appliance that rapidly generates reports while maintaining or improving accuracy of reporting data. It also provides an aggregate view of data for customers with multiple connected devices. The dashboard also provides a monitoring system for a quick overview of filtering statistics aggregated across all the connected devices. The current version supports Barracuda Web Security Gateways.

The Barracuda Reporting Server is purpose-built for reporting, so there is considerable improvement in performance and data accuracy compared with the built-in reporting found in other product lines. Connecting the Barracuda Reporting Server with the Barracuda Web Security Gateway can offload reporting and data processing intensive functions, resulting in better filtering performance of the connected Barracuda Web Security Gateways.

The Barracuda Reporting Server is currently in Early Availability release. For more information, contact your Barracuda representative.

Deployment

For maximum security:

- Place the Barracuda Reporting Server behind your corporate firewall.
- Create access restrictions for your management interface.
- Change the default admin password once you have completed setting up the Barracuda Reporting Server.

To deploy a Barracuda Reporting Server appliance, connect it to one or more devices. Currently, the Barracuda Reporting Server can connect to Barracuda Web Security Gateways. You can connect one, many, or a cluster of Barracuda Web Security Gateways to a single Barracuda Reporting Server. You can then use the Barracuda Reporting Server to report on one or more of the connected devices.

Verify the following for each Web Security Gateway attempting to connect to the Barracuda Reporting Server:

- Firmware version 11.0 or higher is installed
- Can ping the Barracuda Reporting Server
- Can be pinged by the Barracuda Reporting Server

In general, traffic does not flow through the Barracuda Reporting Server. However, the Barracuda Reporting Server can send report information t o an external server. The only appliance type that should be in line after a Barracuda Reporting Server is an FTP or SMP server that receives report information.

Getting Started

Recommended Installation Steps

If you already installed your Barracuda Reporting Server using the Barracuda Reporting Server Quick Start Guide, which is shipped with your device, continue with the next section: Creating reports.

- Step 1 - Install the Barracuda Reporting Server
- Step 2 - Configure the Barracuda Reporting Server
- Step 3 - Activate the Barracuda Reporting Server
- Step 4 - Connect Devices
- Step 5 - Migrate Reports from Connected Devices

Creating Reports

After you have installed the Barracuda Reporting Server and connected one or more devices to it, you are ready to start creating reports. See Reporting for details.

Backing Up

Soon after you have set up your Barracuda Reporting Server, perform a backup so you have it saved in an almost new state. See Working with Backups for details.

30-Day Evaluation Guide

This guide can help you to become familiar with the Barracuda Reporting Server features. See 30 Day Evaluation Guide - Barracuda Reporting Server for details.

Step 1 - Install the Barracuda Reporting Server

Before you begin the installation process, check that you have everything you need.

Checklist for unpacking

Before installing your Barracuda Reporting Server, make sure you have the following equipment:

- Barracuda Reporting Server
- AC power cord
- Ethernet cables
- Mounting rails and screws
- VGA monitor (recommended)
- USB keyboard (recommended)

Installation process

1. Position the Barracuda Reporting Server in a stable location, such as fastened to a standard 19-inch rack. Do not block the cooling vents located on the front and rear of the unit.
   If you have a desktop Barracuda Reporting Server, you do not need to install it in a rack. If desired, you can use the rack-mount kit (sold separately).
   Connect a CAT6 Ethernet cable from your network switch to the LAN port on the back of your Barracuda Reporting Server, as shown in the following figure.

   > Be sure that the Barracuda Reporting Server, and the Barracuda Web Security Gateways you want to connect to it, are accessible through their respective IP addresses and can ping one another. Otherwise, the IP address of the Barracuda Reporting Server must be external.

   The Barracuda Reporting Server supports 10GBASE-T on the model 600, giving you a maximum of 1x10 Gigabit Ethernet.

2. Connect the following hardware to your Barracuda Reporting Server:
   - Power cord
   - VGA monitor
   - USB keyboard
3. Press the Power button located on the front of the unit. The login prompt for the administrative console displays on the monitor, and the power light on the front of the Barracuda Reporting Server turns on.

After you connect the AC power cord, power on the Barracuda Reporting Server.

Note: The AC input voltage range is 100-240 volts at 50/60 Hz.

Continue with Step 2 - Configure the Barracuda Reporting Server.

Step 2 - Configure the Barracuda Reporting Server

Before configuring the Barracuda Reporting Server, complete Step 1 - Install the Barracuda Reporting Server.

Configure the IP address and network settings

1. Log onto the console of your Barracuda Reporting Server with the following default credentials:
   - **username**: admin
   - **password**: admin

   After you complete these steps, remember to change the password on the Barracuda Reporting Server **BASIC > Administration** page.
2. Enter the following information for TCP/IP configuration:
   - **System IP Address** – The address assigned to the Management port on the Barracuda Reporting Server.
   - **Subnet Mask** – The mask used to define this area of your network.
   - **Default Gateway** – The default router used for network traffic not destined for the local subnet.
   - **Primary DNS Server** – The IP address of the fastest DNS server accessible to the Barracuda Reporting Server. Typically, this will be one of the public DNS servers available from your ISP.
   - **Secondary DNS Server** – The IP address of the second-fastest DNS server accessible to the Barracuda Reporting Server. Typically, this will be the fastest DNS server on your internal network.
3. Exit the console.

Note: The system will reboot automatically. Allow the system to reboot completely before attempting to continue with the next section. This may take several minutes.

Configure the Barracuda Reporting Server

1. From a web browser, enter the IP address of the Barracuda Reporting Server followed by the port. The default port is 8000.
   For example: *http://192.168.200.200:8000*
2. To log into the web interface, use the following credentials:
   - **username**: admin
   - **password**: admin

   After you complete these steps, remember to change the password on the Barracuda Reporting Server **BASIC > Administration** page.
3. Navigate to the **BASIC > IP Configuration** page and perform the following steps. Click the Help button for additional online help.
   a. Confirm the **IP address** of the Barracuda Reporting Server that you chose in the steps above. Enter the **Netmask** that is used to define this area of your network, and the **Gateway**, which is the IP address of the next outbound hop from the Barracuda Reporting Server.
   b. Confirm the IP address of your primary and secondary DNS servers.
   c. If you have not already done so, enter the **Default Hostname** that will be displayed in alerts, notifications, and messages sent by the Barracuda Reporting Server.
   d. If you have not already done so, enter the **Default Domain** that will be displayed in alerts, notifications, and messages sent by the Barracuda Reporting Server.
   e. Click **Save**. The appliance automatically reboots.

Allow the system to completely reboot before attempting to log in.

If the IP address of your Barracuda Reporting Server on the **BASIC > IP Configuration** page is changed, you are disconnected from the web interface. If this occurs, log in again using the new IP address.

Specify the Time Zone and Email Information

Be sure to specify these settings so the reports run on the correct schedule and the proper people receive alerts.

1. In the Barracuda Reporting Server, navigate to the **BASIC > Administration** page.
2. In the **Time** section, specify the **Time Zone** in which to run the reports.
3. In the **Email Notification** section, enter the following fields. All are required.
   Note that 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.

4. Click **Save Changes**.

Specify the Shared Secret for Connections

Your Barracuda Reporting Server connects to other devices through the Shared Secret. Set the Shared Secret on the Barracuda Reporting Server, then use that Shared Secret on the devices you want to connect. The Barracuda Reporting Server is the authority for the Shared Secret.

1. In the Barracuda Reporting Server interface, navigate to the **BASIC > Administration** page.
2. Scroll down to the **Connected Devices** section and type a Shared Secret of your choice. There are no restrictions regarding length or character usage.
   You will enter this same Shared Secret in the devices for which you want to create reports. See Step 4 - Connect Devices.

Note: If you change the Shared Secret when there are connected devices, the Barracuda Reporting Server disconnects itself from the devices. You must reconnect each device using the new Shared Secret.

Continue with Step 3 - Activate the Barracuda Reporting Server.

Step 3 - Activate the Barracuda Reporting Server

Before you activate the Barracuda Reporting Server, complete Step 2 - Configure the Barracuda Reporting Server.

Product Activation

1. At the top of every page, you may see the following warning:
   Activation has not been completed. Please activate your Reporting Server to enable functionality. Click here to activate
2. Click on the link to open up the **Product Activation** page in a new browser window.
3. On the **Product Activation** page, fill in the required fields and click **Activate**. A confirmation page opens to display the terms of your subscription.
4. Return to the Barracuda Reporting Server web interface and navigate to the **BASIC > Dashboard** page. In the **Subscription Status** sec tion, verify that the word *Current* appears next to **Energize Updates**, **Instant Replacement Service** (if purchased) and **Premium Support** (if purchased).

There might be a slight delay of a few minutes for the display to reflect your updated subscription status. If the status is still showing as not activated, click **Refresh** in the **Subscription Status** section.

If your subscription status does not change to *Current* within an hour, *and you have ensured that all required network ports are open*, or if you have trouble filling out the **Product Activation** page, please call your Barracuda Networks sales representative.

Update the Barracuda Reporting Server Firmware

Prior to upgrading the firmware on your Barracuda Reporting Server, it is always recommended that you read the release notes.

To update the firmware on your Barracuda Reporting Server:

1. From the web interface, select **ADVANCED > Firmware Updates**.
2. Read the Release Notes to learn about the latest features and fixes provided in the new firmware version.
3. Click **Download Now** next to Latest General Release. **Download Now** is disabled if the Barracuda Reporting Server is already up-to-date with the latest firmware version.
   The Barracuda Reporting Server begins downloading the latest firmware version. You can view the download status by clicking **Refresh**. A message displays once the download is complete. **Do not power-cycle the unit during the download.**
   Updating the firmware may take several minutes. Do not turn off the unit during this process.
4. Click **Apply Now** when the download completes. The Barracuda Reporting Server will apply the firmware and automatically reboot. **Do not power-cycle the unit during this process.** A Status page displays the progress of the reboot. After the reboot is complete, the login page appears.

Update Definitions

To apply the newest definitions provided by Energize Updates:

1. Select **ADVANCED > Energize Updates**.
2. Select **On** for **Automatically Update**. The recommended setting is **On** for all available definitions.
3. Click **Update** to download and install the latest available definitions onto the Barracuda Reporting Server.

Continue with Step 4 - Connect Devices.

Step 4 - Connect Devices

Before you connect devices, complete Step 3 - Activate the Barracuda Reporting Server

To connect a Barracuda Web Security Gateway to the Barracuda Reporting Server:

1. *In the Web Security Gateway*, go to the **BASIC > Administration** page. For **Connect to Barracuda Reporting Server**, select **Yes**, then specify the Barracuda Reporting Server's Shared Secret and IP address. Click **Save**.

   The Barracuda Reporting Server is the Shared Secret authority. Specify the Shared Secret for the Barracuda Reporting Server, then use that Shared Secret in devices you want to connect.

   You must specify these settings in the Barracuda Reporting Server first. If they are not specified in the Barracuda Reporting Server, you will receive an error when you click **Connect**.

2. *In the Barracuda Reporting Server*, navigate to the **BASIC > Administration** page, then scroll down to the **Connected Devices** section to confirm that the connection was successful. The devices connect automatically.
3. Repeat these steps to install additional devices. Use the same Shared Secret for each connected device.
4. Ensure that all Barracuda Web Security Gateways attempting to connect to the Barracuda Reporting Server can be accessed through their respective IP addresses and can ping one another.

If you change the Shared Secret within the Barracuda Reporting Server, all currently connected devices are disconnected. You must reconnect each device using the new Shared Secret.

Continue with Step 5 - Migrate Reports from Connected Devices.

Step 5 - Migrate Reports from Connected Devices

When you connect one or more Barracuda Web Security Gateway devices to the Barracuda Reporting Server, your scheduled reports in the connected devices are automatically migrated to the Barracuda Reporting Server.

The migration process begins when you enter the Barracuda Reporting Server connection information within the Barracuda Web Security Gateway. Refer to Reporting with the Barracuda Reporting Server in the Barracuda Web Security Gateway documentation for details.

All Barracuda Web Security Gateway information remains on the device, even after it is connected to the Barracuda Reporting Server. Reports created with the Barracuda Reporting Server include data from the time the report is migrated to the Barracuda Reporting Server. Historical data, gathered by the device before its connection to the Barracuda Reporting Server, are not migrated to the Barracuda Reporting Server. If the device is disconnected from the Barracuda Reporting Server, either intentionally or unintentionally, then data will be missing from that period of time. If you intentionally disconnected the device, that data will not be sent to the Barracuda Reporting Server. If there was an unintentional connection error, Barracuda Web Security Gateway will store the data and continually attempt to resend it to the Barracuda Reporting Server.

Migrating Scheduled Reports to the Barracuda Reporting Server

Step 1: Viewing Migrated Reports

To complete the migration process:

1. In the Barracuda Reporting Server, navigate to the **BASIC > Administration** page.
2. In the **Connected Devices** section, locate the newly connected device and click **View Migrated Reports**.
3. The **Migrated Scheduled Reports** dialog appears. It displays the **Report Name**, **Frequency**, and **Time Frame** to help you identify the reports. The **Migration Status** column shows whether the report was migrated successfully. Occasionally, errors occur during migration.
4. For reports showing an error, click **View Details** to see the issues with migrating that report.

No Migrated Reports

The are some cases in which the Migrated Scheduled Reports dialog might not display any reports. A message informs you why there are no reports to display.

For details, refer to Troubleshooting.

Step 2: Verifying and Enabling Migrated Reports

After migration is complete, you must enable the migrated reports. This is an opportunity to double-check the report information for errors before the reports are generated.

To enable migrated reports:

1. Navigate to the **REPORTS** page.
2. In the **Scheduled Reports** section at the bottom of the page, locate a newly migrated report. It will display as **Disabled**.
3. Click **Edit** for the migrated report. Scroll to the top of the page and verify that the information is correct for the migrated reports.
4. In the **Schedule Report** section, select **Enabled**, then click **Save Changes** in the top right corner.
   In the **Scheduled Reports** section, the report appears with the status of **Enabled**.

Disconnecting Devices and Associated Reports

If you choose to disconnect a Barracuda Web Security Gateway device from the Barracuda Reporting Server, the reports you originally created on the connected device are re-enabled with their original settings. You can again manage reports within the Barracuda Web Security Gateway. Any updates you might have made to those original reports, or any new reports you created in Barracuda Reporting Server, are not migrated back to the disconnected Web Security Gateway.

If you choose to disconnect a device, reports created or migrated to the Barracuda Reporting Server, and report modifications made within Barracuda Reporting Server, remain within the Barracuda Reporting Server and can continue to be managed there.

30 Day Evaluation Guide - Barracuda Reporting Server

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 Web Security Gateway 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 Web Security Gateway 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**

  a. 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**

  a. (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.

  b. Return to the **REPORTS** page and scroll to the **Reports** section. Select one or more reports you want to create.

  c. 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 Barracuda Web Security Gateway 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

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*, go to the **BASIC > Administration** page and enter the Barracuda Reporting Server's IP address and Shared Secret. For **Connect to Barracuda Reporting Server**, click **Yes**.
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 - Migrate Reports from Connected Devices for details on the migration.
- Refer to Reporting for details on scheduling reports.

Dashboard

The Barracuda Reporting Server includes an interactive Dashboard where you can get an overview of issues in one place.

To view the Dashboard, navigate to the **BASIC** > **Dashboard** page.

By default, the information on the Dashboard refreshes automatically every 30 minutes, so you can leave the page up and see recent status.

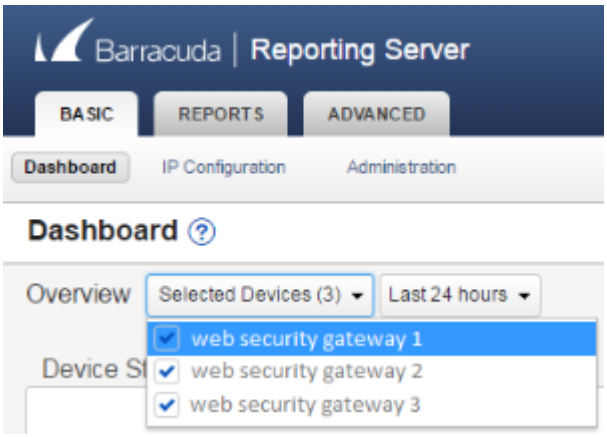
Overview – Device Selection

You can set the connected device for which you want the Dashboard to display reports.

At the top of the **BASIC > Dashboard** page, make selections in the **Report on** area.

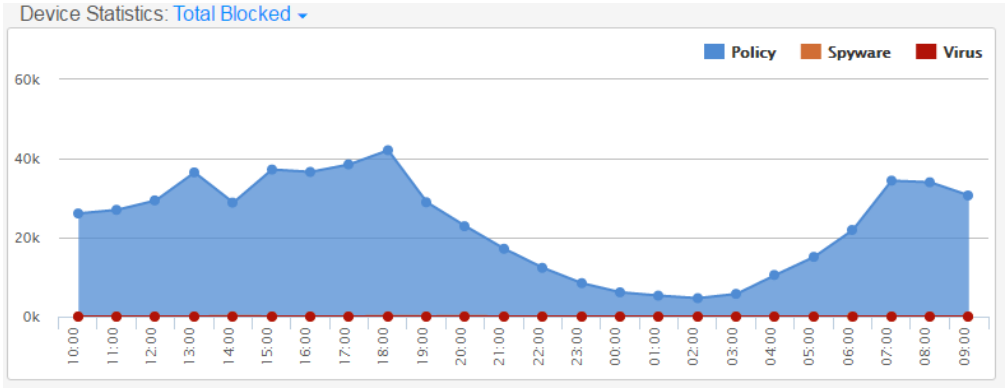
- In the first pull-down menu, select the connected device for which you want to see reports.
  Note that devices that are disconnected are still available here, since their data is still available.
- In the second pull-down menu, select the time frame for the reports: **Last 24 hours**, **Last 7 days**, **Last 30 days**

By default, **All Connected Devices** are displayed, showing data from the **Last 24 Hours**.



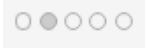
Note: Device selection and time frame are remembered each time you open the Dashboard.

Device Statistics



This graph can display a number of different statistics tied to the Barracuda Web Security Gateways that are connected to the Barracuda Reporti ng Server. Select the graph you want to view from the following options:

- **Total Blocked** – *(Default)* Displays the number of policy, spyware, and virus blocks for the specified time period.
- **Blocked Policy** – Displays the number of policy blocks for the specified time period.
- **Blocked Spyware** – Displays the number of spyware blocks for the specified time period.
- **Blocked Virus** – Displays the number of virus blocks for the specified time period.
- **Total Allowed** – Displays the number or requests allowed to pass through the Barracuda Web Security Gateway for the specified time period.

You can also cycle through the various graphs by clicking the circles below the graph  . Each circle represents a different graph subject.

Recently Flagged Terms

This section lists the most recent flagged terms being tracked by the Barracuda Web Security Gateway when both SSL Inspection and Web

Application Monitoring are enabled. If either one of these settings is not enabled, no data can be displayed in this section.

The following information is displayed in table form:

- **Device Name** – The name of the device you selected at the top of the page, in the **Report On** section.
- **User** – The name of the user making the requests.
- **IP Address** – The IP address of the user.
- **Source** – The domain in which the flagged terms were used.
- **Keywords** – The word or phrase that was flagged.
- **Time** – The time the flagged term was used, in local time, according to your configuration.

Note: If no flagged terms are available, ensure that the following two settings are enabled on your connected Barracuda Web Security Gateways.

- SSL Inspection
- Web Application Monitoring

If either one of these settings is not enabled, no data can be displayed in this section.

System Status

This section indicates the current operational status of the Barracuda Reporting Server.

For detailed information about the status of the Barracuda Reporting Server, click **Details**. The following information displays in a separate table. Note that there are multiple CPU and system fans.

- **Uptime** – How long the Barracuda Reporting Server has been up and running.
- **System Load** – A dynamic representation of the load on the Barracuda Reporting Server.
- **CPU Temperature** – The temperature of the CPU within the Barracuda Reporting Server appliance.
- **CPU Fan Speed** – The fan speed of the CPU within the Barracuda Reporting Server appliance, in revolutions per minute (RPMs).
- **System Temperature** – The temperature of the Barracuda Reporting Server appliance.
- **System Fan Speed** – The fan speed of the Barracuda Reporting Server appliance, in revolutions per minute (RPMs).

Subscription Status

Displays the current status of the **Energize Updates**, **Instant Replacement**, and **Premium Support** subscriptions for the Barracuda Reporting Server.

Connected Devices

Lists the current operational status of each of the Barracuda Web Security Gateways linked to the Barracuda Reporting Server, as well as the Barracuda Reporting Server operational status for the logs received and processed for each connected device.

For information about the status of each device, click **Details**. The following information is displayed in a separate table:

- **Device Name** – Name of the Barracuda Web Security Gateway linked to the Barracuda Reporting Server.
- **Model** – Model number of the linked Barracuda Web Security Gateway.
- **Firmware** – Version of the firmware installed on the linked Barracuda Web Security Gateway.
- **Status** – Whether the Barracuda Web Security Gateway is connected to the Barracuda Reporting Server. Status values are:
  - **Connected** – The device is connected and functioning properly.
  - **Disconnected** – The device was intentionally disconnected and was disconnected successfully.
  - **Error** – There is an error with the device connection. The device is not communicating with the Barracuda Reporting Server. For troubleshooting information, refer to Troubleshooting.
- **Last Log Received** – Date and time stamp of the last time a log was passed from the Barracuda Web Security Gateway to the Barracuda Reporting Server.
- **Last Log Processed** – Date and time stamp of the last time a log from this device was processed by the Barracuda Reporting Server.
- **Storage Used** – How much of the available storage on the device has been used.
- **Log Retention** – Length of time event logs are maintained on the Barracuda Reporting Server. Change this setting on the Administration page.

Pending Log Status

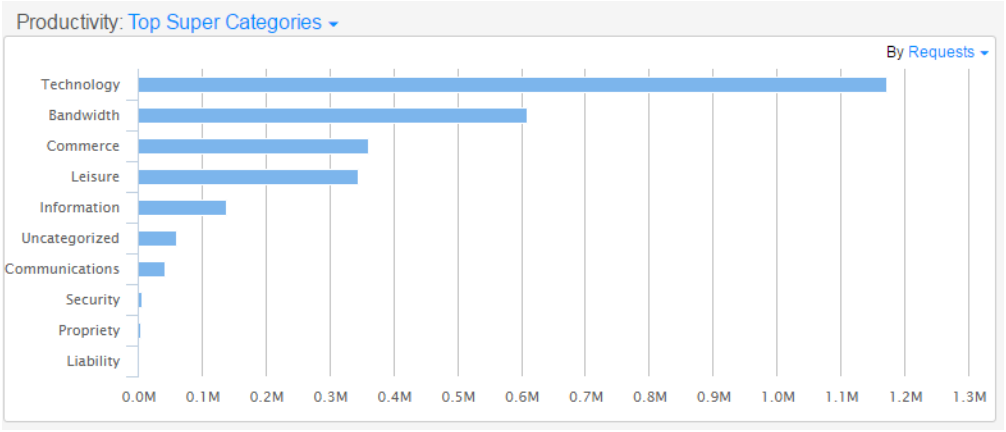
If the **Last Log Received** or **Last Log Processed** in the **Connected Devices Details** window shows as **Pending**, make sure that:

- In the same **Connected Devices Details** window, the **Status** is **Connected**, rather than **Disconnected** or **Error**.
- Your Web Security Gateway device has data going through it.
- The credentials of **Shared Secret** and **IP Address** are entered correctly, as described in Step 4 - Connect Devices.

The time frame for **Pending** status corresponds to how long the Web Security Gateway has been connected to the Barracuda Reporting Server:

- **For new connections**: about 10-15 minutes until the Web Security Gateway sends data to the Barracuda Reporting Server.
- **For established connections**: up to 30 minutes for the Barracuda Reporting Server to receive incoming logs.

Productivity



Select to display a graph of the **Top Super Categories** *(default),* **Top Categories**, **Top Users**, or **Top Domains** from the drop-down menu on the top left. Adjust the units to display by **Requests**, **Bandwidth**, or **Browsing Time** with the drop-down menu on the top right.

Web Activity

Select to display a graph of total web activity in **Bandwidth** (default) or **Requests** as measured by the Barracuda Web Security Gateway.

HTTP traffic is the difference between Total Traffic and HTTPS Traffic shown on the graph.

Reporting Server Storage

Displays a graph of the hard disk space currently being used to store reporting information. Hover over the gray section of the graph to see space that is still available.

Each connected device appears in a different color. Hover over each color for details on the corresponding connected device.

Reporting

Reports by Use Cases

Use the **Reports** page to choose from more than 80 different reports that can help you keep track of data from the connected Barracuda Web Security Gateway 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 Accurately Reporting User Browsing Times for more information.

Reports can be anchored on user activity, content, or bandwidth usage and are grouped as follows:

For Human Resources, Teachers, and Managers

These reports are user-friendly, easy-to-read, and provide the following critical information:

- **Productivity** reports reflecting user activity with social networking and other applications; for example:
  - Top Users by Browse Time on Gaming Sites
  - Top Social Networking Domains by Requests – may determine which domains you want to block, warn, or monitor
  - Top YouTube Users by Bandwidth
  - Top Facebook Users by Browse Time
  - Top Users by Browse Time on Social Networking Sites
- **Safety and Liability** reports; for example:
  - Top Users by Requests to Intolerance and Hate Sites
  - Top Users by Requests to Anonymizer Sites. An anonymizer is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet, hiding the client computer's identity (IP address).
  - Suspicious Keywords by Users – for detection of possible cyberbullying, or mention of weapons or terrorism.

For IT and System Administrators

These report types show infection activity, blocked virus downloads, bandwidth usage by time frame, and many other system performance-related reports**,** such as:

- **Infection Activity**
  - Malware Blocks – IP addresses from which requests were made to known spyware sites.
  - Virus Blocks – A list of blocked virus downloads during the specified time frame.
- **Web Activity**
  - Session time or browse time, by hour, or by time of day.
  - Popular IP addresses to which requests were made.
  - Categories (e.g., adult, gaming, leisure) by bandwidth, number of requests, browse time, and more.
  - Users by session time, browse time, bandwidth, and more.
- **Administrative**
  - Audit Reports for Web Security Gateway track logins and logouts to the web interface, as well as changes to the configuration by role.
  - Temporary Access Request Log – Log of activity by teachers who have been given credentials to request temporary access for their students to domains that are typically regulated by system administrators. See Temporary Access for Education.
  - Temporary Access Requests by Domains, Users, or Categories.
- **Network Activity**
  - TCP Connection Usage
  - Daily Bandwidth
  - Web Requests Log
- **Summary**
  - Internet, Network, and User activity summaries
  - Total Usage

For a complete list and detailed descriptions of the system reports, see the online help for the **Reports** page.

Specifying Filtering Options

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** – 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.
  - **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.
  - **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**.
  - **LDAP User** – Select an LDAP directory, then type all or part of a user's name, then click **Lookup** to search for that user. Use the wildcard character (*) when using only parts of the user name.
  - **LDAP Group** – Select an LDAP directory, then 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.
  - **LDAP Organizational Unit** – Select an LDAP directory, then type all or part of a organizational unit name, then click **Lookup** to search for that organizational unit. Use the wildcard character (*) when using only parts of the organizational unit name.
- **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 Web Security Gateways 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

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** – 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** – 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** 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** to update the report.

Accurately Reporting User Browsing Times

Embedded web content is intelligently detected by the Barracuda Web Security Gateway to maximize reporting accuracy. For example, a site such as **cnn.com** embeds requests to Facebook, Twitter, and other social networks. While a user visiting the news site might not explicitly click on any of the embedded links, the embedded content still makes periodic web requests. On a report, this could appear as if the user visited CNN, Facebook, and Twitter and spent 15 minutes on each site.

While this is technically accurate, it can misrepresent the user's actions on reports that are reviewed by the Human Resources department, for example. The Barracuda Web Security Gateway can make the distinction between such embedded requests – also known as "referred requests" – and actual user visits in most cases, but there are some limitations, due to the behavior of some client applications. Consequently, reports reflect estimates of actual user browse and session times.

If you have used the reporting feature of Barracuda Web Security Gateway, you will likely notice that the times in the Barracuda Reporting Server reports differ from those in the Barracuda Web Security Gateway reports. This is due to improved reporting accuracy on the Barracuda Reporting Server.

Important
The Barracuda Web Security Gateway uses an HTTP referer (sic) to make the distinction between embedded requests and user visits. The Barracuda Reporting Server uses this information, and other logs that are collected from the Barracuda Web Security Gateway, to make an improved calculation of browsing and session times. However, it is important to note that there are various client applications that limit the accuracy of calculating browse times. Here are some examples:

- JavaScript that downloads assets from another site and may not set referers;
- iOS apps that request web assets and may not set referers;
- Android apps that request web assets may place the app package name in referers.

Session Time Versus Browse Time

Session time is the time calculated for each browsing session generated, with an idle timeout value of about three minutes. So if, for example, a user visits **campus.barracuda.com**, but does not click anything else for more than three minutes, that counts as one session of three minutes for that user on **campus.barracuda.com**. If the user does click around **campus.barracuda.com** within the three minute time frame, the session continues to increase in length until there is a three minute idle time. If a user hits a blocked page, the session time will be zero minutes.

Browse time as shown in reports is the sum of all estimated session times in a particular grouping (e.g., domain, category, user).

Sample Reporting Cases

This page includes examples of how you can effectively use reports.

Notes:

- It is important to select a **Time Frame** for all reports. The default value of **Today** might not yield results, so you will likely need to specify a longer period of time, such as **Last 30 days**.
- Drill-downs are available for HTML and PDF report formats.

Find a specific gaming user's activity by hour using drill-downs

1. On the **Reports** page, in the **Filtering Options** section, set the desired **Time Frame**.
2. Click **Top Users by Browse Time on Gaming Sites** to create an ad-hoc report.
3. For a specific user, drill down by hour to see that specific user's activity per hour.

Find user activity based on Recently Flagged Terms in the Dashboard

1. In the **Dashboard**, observe the **Recently Flagged Terms** section and click **View report**.
   In the report, note the user of interest.
2. Navigate to the **Reports** page. In the **Filtering Options** section,
   - **Time Frame** – Set the desired time frame.
   - **Limit Report to** – Locate the user in the system by searching. Click **Add** to add the user to the report limitation.
3. Scroll to the **Summary Reports** section and click **Internet Activity Summary** to create an ad-hoc report.
   In this report, you can see information for this user, including domains visited and browse time. At the bottom of the report, you can drill down by **Category**, **Hour**, or **Domain** for additional details.

Find users spending the most time on inappropriate categories of websites

1. In the **Dashboard**, observe the **Productivity category**, either the **Top Categories** or **Top Super Categories** selections. Make note of one or more categories you want to investigate.
2. Navigate to the **Reports** page. In the **Filtering Options** section, set the desired **Time Frame**.
3. In the **Advanced Options** section:
   - **Destination** – Select **Category**.
   - **Categories** – Select one or more **Categories** that you want to include in the report, such as Adult Content, Intolerance & Hate, and Spam.
4. Scroll to the **Summary Reports** section and click **Internet Activity Summary** to create an ad-hoc report.
   In this report, you can see information including the top users by requests and browse time. You can drill down within the categories of User, Category, and Domain to find more information.

Find malicious files on a user's computer

1. Navigate to the **Reports** page. In the **Filtering Options** section, set the desired **Time Frame**.
2. Scroll down to the **Infection Activity** section. Click **Malware Blocks** to create an ad-hoc report.
   In this report, you can see malware infections by user. Make note of the user with the infection. Find the user to find the computer that needs to be disinfected.
   a. Return to the **Reports** page. In the **Filtering Options** section
      - **Time Frame** – Set the desired time frame.
      - **Limit Report to** – Locate the user in the system by searching. Click **Add** to add the user to the report limitation.
   b. In the **Reports** section, go to the second **Web Activity** section. Click any of the "**Users by ...**" reports. There, you will see the IP address for the user. This is the computer you need to clean.

Understanding Time Frames and Recurring Reports

Time Frames

The following Time Frames have specific definitions within Barracuda Reporting Server:

- **Last 7 days**: Begins at 12:00 am seven days before the current day and lasts up to the current time.
- **Last Week**: Begins at 12:00 am the previous Monday and lasts up to this Monday at 12:00 am.
- **This Week**: Begins at 12:00 am the Monday of the current week and lasts up to the current time.
- **This and Last Week**: Begins at 12:00 am the previous Monday and lasts up to the current time.

Note that the **Time Frames** involving weeks function slightly differently in Barracuda Web Security Gateway. There, the time begins at 12:00 am the previous *Sunday*.

Recurring Reports

For example, on Wednesday, January 6 at 07:30 (7:30 am), you create a Weekly report for This Month. You choose to receive the Weekly reports on Fridays at 18:00 (6:00 pm). The following reports are generated:

- **First report** – Includes data from January 1 through Friday, January 8 at 18:00.
- **Second report** – Includes data from January 1 through Friday, January 15 at 18:00.
- **Third report** – Includes data from January 1 through Friday, January 22 at 18:00.
- **Fourth report** – Includes data from January 1 through Friday, January 29 at 18:00.

This behavior is similar for the following Time Frames. Other pre-defined Time Frames do not follow this behavior.

- This Week
- This and Last Week
- This Month
- This and Last Month

The following table explains how reports are generated with the possible combinations of the Time Frames mentioned above and Report Frequency.

	Time Frame	This Week	This and Last Week	This Month	This and Last Month
Frequency					
Hourly		• **Generate**: Each hour of the current week on the hour. • **Start**: This Monday at 00:00. • **Include**: Data from start time to the current hour. • **Automatically stop**: The following Monday at 00:00.	• **Generate**: Each hour of the previous week and the current week. • **Start**: The previous Monday at 00:00. • **Include**: Data from start time to the current hour. • **Automatically stop**: The following Monday at 00:00.	• **Generate**: Each hour of the current month. • **Start**: The first day of the current month at 00:00. • **Include**: Data from start time to the current hour. • **Automatically stop**: The first day of the following month at 00:00.	• **Generate**: Each hour of the previous month and current month. • **Start**: The first day of the previous month at 00:00. • **Include**: Data from start time to the current hour. • **Automatically stop**: The first day of the following month at 00:00.

Daily	• **Generate**: Each day of the current week at the hour you chose. • **Start**: This Monday at 00:00. • **Include**: Data from start time to the hour you chose. • **Automatically stop**: The following Monday at 00:00.	• **Generate**: Each day of the previous week and current week at the hour you chose. • **Start**: The previous Monday at 00:00. • **Include**: Data from start time to the hour you chose. • **Automatically stop**: The following Monday at 00:00.	• **Generate**: Each day of the current month at the hour you chose. • **Start**: The first day of the current month at 00:00. • **Include**: Data from start time to the hour you chose. • **Automatically stop**: The first day of the following month at 00:00.	• **Generate**: Each day of the previous month and current month at the hour you chose. • **Start**: The first day of the previous month at 00:00. • **Include**: Data from start time to the hour you chose. • **Automatically stop**: The first day of the following month at 00:00.
Weekly	• **Generate**: Once for the current week on the day and hour you chose. • **Start**: This Monday at 00:00. • **Include**: Data from start time to the day and hour you chose. • **Automatically stop**: Only one report generated.	• **Generate**: Once for the previous week and current week on the day and hour you chose. • **Start**: The previous Monday at 00:00. • **Include**: Data from start time to the day and hour you chose. • **Automatically stop**: Only one report generated.	• **Generate**: Each week of the current month o n the day and hour you chose. • **Start**: The first day of the current month at 00:00. • **Include**: Data from start time to the day and hour you chose. • **Automatically stop**: After the last week of the month at the day and hour you chose.	• **Generate**: Each week of the previous month and current month on the day and hour you chose. • **Start**: The first day of the previous month at 00:00. • **Include**: Data from start time to the day and hour you chose. • **Automatically stop**: After the last week of the month at the day and hour you chose.
Monthly	• **Generate**: Once for the current week on the date and hour you chose. • **Start**: This Monday at 00:00. • **Include**: Data from start time to the date and hour you chose. • **Automatically stop**: Only one report generated.	• **Generate**: Once for the previous week and current week on the date and hour you chose. • **Start**: The previous Monday at 00:00. • **Include**: Data from start time to the date and hour you chose. • **Automatically stop**: Only one report generated.	• **Generate**: Each week of the current month on the date and hour you chose. • **Start**: The first day of the current month at 00:00. • **Include**: Data from start time to the date and hour you chose. • **Automatically stop**: After the last week of the month at the date and hour you chose.	• **Generate**: Each week of the previous month and current month on the date and hour you chose. • **Start**: The first day of the previous month at 00:00. • **Include**: Data from start time to the date and hour you chose. • **Automatically stop**: After the last week of the month at the date and hour you chose.

Administration

Handle Administrative tasks on the **BASIC > Administration** page.

Changing Your Password

Use the **Password Change** section to change the password for the account currently in use.

Passwords should be 5 to 20 characters and can include letters, numbers, and special characters (including periods, hyphens, and underscores).

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.

Setting Your Time Zone

Use the **Time** section to change the timezone on your system.

Specifying Web Interface Settings

Specify the web interface settings for the web interface of your Barracuda Reporting Server.

- **Web Interface HTTP Port** – Port used by a web browser to gain access to the product's web interface (Recommended value: 8000).
- **Session Expiration Length** – Time of inactivity, in minutes, before users are required to log on again to access the web interface. **Minimum value**: 1 minute. **Default setting**: 20 minutes.
- **Update Dashboard Every 30 Minutes** – Select **Yes** to automatically refresh the dashboard so you can see the most recent information.
  - If you select **Yes**, as long as you leave the dashboard up as the active screen, you will not be logged out of the dashboard and it will continue to display updated information every 30 minutes. When you switch to a different tab, if the **Session Expiration Length** has passed, you will be logged out.
  - If you select **No**, the **Session Expiration Length** will apply to the **Dashboard** along with the rest of the tabs.

Viewing Connected Devices

Use the **Connected Devices** section to specify the Shared Secret for devices you want to connect, to view devices that are connected to the Barracuda Reporting Server, and to specify their Log Retention Period.

Connected Devices

As part of your configuration process, you set up Barracuda devices, such as Barracuda Web Security Gateways, to point to the Barracuda Repo rting Server. If they connect correctly, the device connections will appear in this section.

- **Shared Secret** – Enter the **Shared Secret** for each device for which you want to collect reports. On every device you want to connect, enter this same Shared Secret.
  - For the Barracuda Web Security Gateway, enter the Shared Secret on the **BASIC > Reports** page and complete the steps in the **Barracuda Reporting Server** section.
- **Device Name** – To have a unique name, the Device Name consists of "Hostname" + "Domain Name" for the connected device.
- **IP Address** – The address of the connected device.
- **Log Retention Period –** Specify how long you want to retain logs for this Web Security Gateway: **1 month**, **3 months**, **6 months**, **9 months**, or **12 months**. One month is defined as 31 days.

Once the hard disk space limit is reached, the oldest logs are automatically deleted first. As much as possible, your data will be preserved. To ensure your data is preserved, back it up often.

Reducing the Log Retention Period deletes all logs older than the new retention period specified. For example, changing the Log Retention Period from 6 months to 1 month deletes all logs older than 1 month. If needed, back up logs before reducing the Log Retention Period.

Increasing the Log Retention Period adds new logs to the existing collection, up to the period specified.

Shutting Down or Restarting the System

Caution
Using these controls temporarily interrupts all Barracuda Reporting Server operations.

- **Shutdown –** Shuts down and powers off the Barracuda Reporting Server.
- **Restart –** Reboots the Barracuda Reporting Server.

Creating, Configuring, and Using Alerts

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.

Scheduled Reports are generated and sent automatically. An email alerts you when they are ready. 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 these formats: HTML, PDF, Text, or CSV.

Refer to Administration for details on setting up email notifications.

Refer to Reporting for details on scheduling reports.

Understanding Data Retention and Storage Capacity

Managing retention policies

As an administrator, you can manage retention policies on a per-appliance basis. By default, the retention policy is 6 months on each appliance. Data older than 6 months is automatically deleted. The Barracuda Reporting Server enables you to control how much data you are saving to the Barracuda Reporting Server and reporting log. Thus, if you have a large amount of data being sent from a single Barracuda Web Security Gateway, or if you have several Barracuda Web Security Gateway devices connected to your Barracuda Reporting Server, you will not run out of space. If you need additional storage, make frequent backups of your configuration and data and connect to Barracuda Backup.

To change the retention policy:

1. Navigate to the **BASIC > Administration** page.
2. Scroll down to the **Connected Devices** section.
3. For the device you want to change, select a different **Log Retention Period**. Repeat this step for additional appliances, if needed.
4. Click **Save Changes**.

Notes:

- When storage capacity is reached, oldest logs are deleted first. Your data will be preserved as much as possible, but some data will be lost.
- Reducing the log retention period deletes all logs older than the new retention period specified (e.g., changing from **6 months** to **1 month** deletes all logs older than 1 month). Consider backing up logs before reducing the retention period.
- Increasing the Log Retention Period adds new logs to the collection, up to the period specified.

Storage Capacity

To view storage used for the logs from each connected Barracuda Web Security Gateway:

1. Navigate to **BASIC > Dashboard**.
2. In the **Connected Devices** area, click **Details**.
3. For each connected device, you will see the storage space used for its stored logs.
   Combined used and available storage on the Barracuda Reporting Server is shown in the donut chart on the dashboard.

If your storage is getting tight, consider reducing the log retention period for one or more connected devices.

Scalability and Redundancy

Scalability and redundancy of the Barracuda Reporting Server enable you to create reports consistently and reliably.

Scalability

The Barracuda Reporting Server can scale to fit your needs.

- Each Barracuda Reporting Server can connect to multiple Barracuda Web Security Gateway devices, regardless of the Barracuda Web Security Gateway model.
- You can back up and archive your logs, with Barracuda Backup and Barracuda Cloud Archiving Service, to create room for additional data.

Redundancy

The Barracuda Reporting Server has built-in redundancy to protect you against potential problems.

- The software has redundancy built into its architecture, based around the concepts of hot data (data most recently accessed or processed) and cold data (data that is no longer hot). This redundancy helps protect your data.
- In the unlikely event that you lose your cold data on the appliance, you can switch out the RAID arrays with a new Barracuda Reporting Server appliance. The Barracuda Web Security Gateway devices save logs for at least 30 days' worth of data, which can be resent to the new Barracuda Reporting Server. You can continue to process data without data loss.
- You can back up your configuration and data often to ensure your data is protected. Refer to Understanding Data Retention and Storage Capacity for details.

Hardware Support

In the unlikely event that you experience problems with your Barracuda Reporting Server appliance, contact Barracuda Customer Support immed iately. You can also refer to Hardware Support in Barracuda Campus.

Maintenance

Maintenance topics include:

- Working with Backups
- Updating Reports and Security Definitions
- Updating Barracuda Reporting Server Firmware
- Working with External Servers
- Finding Support through Help
- Restarting and Shutting Down the System
- Disconnecting Devices

Working with Backups

You can create a backup of various system settings for the Barracuda Reporting Server. You can use these files for backup purposes or to upload them to a separate Barracuda Reporting Server.

Creating a Configuration Backup

To back up a configuration,

1. Navigate to the **ADVANCED > Backups** tab.
2. In the **Configuration Backup** section, click **Backup Now**.
   Barracuda Reporting Server creates a backup of the current system configuration. Save the file to a safe location.

Restoring Configuration

> **Caution**
> Restoring a backup will **overwrite the current configuration** of this Barracuda Reporting Server.
>
> If your machine is currently part of a cluster, do not restore a configuration file onto it, because all cluster information will be lost. If this happens, the units will have to be re-clustered again.

To restore a configuration:

1. If you are performing a restore to upload settings onto a new, unconfigured Barracuda Reporting Server, perform the first three steps in Getting Started:
   - Step 1 - Install the Barracuda Reporting Server
   - Step 2 - Configure the Barracuda Reporting Server
   - Step 3 - Activate the Barracuda Reporting Server
2. Navigate to the **ADVANCED > Backups** tab.
3. Select a backup file to **Restore From**. Click **Choose File** to navigate to the desired backup file on your local disk.
4. Confirm that you have selected the correct backup file and the desired components, then click **Restore** to begin the restoration.

> To fully complete the restore, the Barracuda Reporting Server will reboot. Attempting to use the system without a reboot may result in unexpected behavior.

Creating a Data Backup

Creating a data backup allows access to the data store as an SMB share. Backing up your data ensures that you will always have it, even if it gets deleted from the Barracuda Reporting Server.

To back up the Barracuda Reporting Server reporting data:

1. Navigate to the **ADVANCED > Backups** tab.
2. In the **Data Backup** section, select **Yes**, you want to **Back Up Data via SMB**.
   Recommended setting: **Yes**
   To access an enabled share, use \\<*Barracuda Reporting Server IP Address*>*backup*.
3. Specify the name of the **Workgroup** in which the Barracuda Reporting Server should appear.
   Recommended setting: **WORKGROUP**
4. Specify the **Password** used to connect to the SMB share. The username is **smb**.

Updating Reports and Security Definitions

This is usually configured by the administrator during the initial Barracuda Reporting Server installation.

Barracuda Central monitors the Internet for new threats and puts out Energize Updates, the latest definitions to protect you from those threats.

To check on and update your Reports Definitions and Security Definitions:

1. Navigate to the **ADVANCED > Energize Update** tab.
2. Look in the **Current Installed Version** to see if you are running the latest version. Click **Release Notes** if you want to see information about that release.
3. In the **Latest Version** area, click **Update** if there is a later version than the one you are currently running. If available, click the **Release Notes** link to read about this release before installing it. The **Update** button is available only when the **Current Installed Version** is older than the **Latest Version**.
4. For Reports Definitions, Security Definitions, or both, select if you want to perform **Automatic Updates**. Selecting **Yes** for both options means that you will always have the most up-to-date definitions.
   Recommended setting: **On**, for both
5. Click **Save Changes** if you changed the settings for **Automatic Updates**.

Updating Barracuda Reporting Server Firmware

Important
Before updating the firmware on your Barracuda Reporting Server, Barracuda recommends reading the Release Notes.

To update the firmware:

1. Navigate to the **ADVANCED > Firmware Updates** page.
2. In the **Firmware Download** section, see if there is a new version available.
3. Read the release notes for this firmware version.
4. If you are certain you want to update the firmware, click **Download** to download the new firmware.
5. When the firmware has been downloaded, click **Apply Now**.

The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call Barracuda Networks Technical Support before reverting back to a previous firmware version.

Working with External Servers

Add and work with external servers, where you store report logs.

Adding an External Server

Use this section to add **FTP** or **SMB** servers for storing report logs. These servers can then be selected from the **Reports** page.

Enter the details for the external server:

- **Server Type** – Select either FTP or SMB.
- **Alias** – *(Optional)* Enter the server alias name.
- **Hostname/IP Address** – Enter the FQDN or IP address of the server.
- **Port** – Enter the **Port** number of the server.
  - Default ports:
    - FTP = 21
    - smb = 445
- **Username/Password** – Enter the server administrator username and password.
- **Folder/Path** – Enter the directory path location, including forward slashes (/).

Click **Add Server** to add the server to the **External Servers** table.

Click **Test Server** to test the server connection.

External Servers

The list of external servers you have defined on this page for reports. Fields in the table include:

- **Alias** – Alias name for the server.
- **Hostname/IP Address** – The FQDN or IP address of the server.
- **Type** – The type of external server, either *FTP* or *SMB*.
- **Port** – Port number for the external server.
- **Folder/Path** – Directory path location.
- **Actions** - Actions you can take on the external server:
  - **Edit** – Make any changes to the server details in the top part of this page. You can test the server again, if needed. Be sure to click **Save Changes** when you have finished.
  - **Remove** – Removes the link between the external server and this Barracuda Reporting Server.

    Note: If you remove an external server, any reports that were pointing to it will be disabled. They will still be listed in the **Scheduled Reports** list on the **Reports** page, but they cannot run without your specifying a new external server.

Finding Support through Help

If you need assistance online, click the Help icon ( ) on the page where you need help. Alternatively, you can search the help system for the topic you need.

To search the help:

1. Navigate to the **ADVANCED > Support** page.
2. In the **Search Help Topics** box, type a word or phrase, then click **Search**.
3. Click a link from the list of **Search Results**.

Alternatively, you can click one of the links in the **Help Topics** section.

Restarting and Shutting Down the System

To restart or shut down the Barracuda Reporting Server:

1. Navigate to the **BASIC > Administration** page.
2. In the System Management section, select:
   - **Shutdown** to power off the unit.
   - **Restart** to reboot the unit.

Disconnecting Devices

To disconnect a device from the Barracuda Reporting Server:

1. In the connected device (Barracuda Web Security Gateway), navigate to the **BASIC > Administration** page and locate the **Barracuda Reporting Server** section.
2. For **Connect to Barracuda Reporting Server**, click **No**.

Note that the **IP Address** and **Shared Secret** information for this Barracuda Web Security Gateway still populates the appropriate fields. The connection information is not deleted. Should you choose to reconnect this device, click **Yes** in Step 2 above.

To confirm that the device is disconnected:

1. In the Barracuda Reporting Server, navigate to the **BASIC > Administration** page.
2. In the **Connected Devices** section, notice that this device has an  icon next to it, indicating that it has been disconnected properly. The data is not deleted.

   Note that you can change the Log Retention Period of this device, even if it is disconnected. You can decrease the retention period, taking a subset of the data you already have. You cannot lengthen the retention period when a device is connected.

Migrating Scheduled Reports

Refer to Step 5 - Migrate Reports from Connected Devices for information on migrating scheduled reports.

Troubleshooting

Basic Troubleshooting

This section describes issues that you can handle on your own. If you require help from a Support Technician, see the next section in this article.

Error Status for a Connected Device

If a connected device shows a connection error, check the following:

- Network connectivity between the Barracuda Reporting Server and the connected device, and between both devices and the Internet
- Wire connections for any broken or damaged cables.
- The Shared Secret is the same on both the Barracuda Reporting Server and the connected device. Refer to Step 2 - Configure the Barracuda Reporting Server and Step 4 - Connect Devices for details.
- The connected device is set to connect to the Barracuda Reporting Server. Refer to Step 4 - Connect Devices for details.

No Reports Migrated

The are some cases in which the Migrated Scheduled Reports dialog might not display any reports. A message informs you why there are no reports to display.

Possible reasons for not having migrated reports displayed include:

- There were no reports to migrate from the connected device.
- The device was just connected and the migration process has not yet started.
- There is a problem reading the incoming report. Click **View Details**, as described above, if there is an error.
- There is a problem reading all of the incoming reports.
- You have already migrated Scheduled Reports from this device. Scheduled Reports can only be migrated once.

Troubleshooting with Barracuda Support

Connecting with the Barracuda Support Center

If a Barracuda Networks technician needs to troubleshoot and diagnose a potential issue, click **Establish Connection to Barracuda Support Center** to create a secure troubleshooting connection from your Barracuda Reporting Server to the Barracuda Networks Technical Support servers.

To open a support connection:

1. Navigate to the **ADVANCED > Troubleshooting** tab.
2. Click **Establish Connection to Barracuda Support Center**.
   A new window will appear that displays the following:
   - Access token and serial number required by the support technician in order to access your Barracuda Reporting Server
   - Status of connection
   - Button to terminate connection
3. Work with the Support Representative to solve your issue.
4. When your support issue is resolved, click **Terminate Connection to Barracuda Central**.

After the connection is terminated, all existing connections with the support servers are immediately closed and all new connection attempts will be rejected until the connection is re-established from the Barracuda Reporting Server.

Note: This connection lasts only a few hours.

Performing a Network Connectivity Test

To perform a network connectivity test, enter a hostname or IP address, then select a test to run:

- **Ping** – Enter the IP address or hostname to ping and click **Ping** to start the test.
- **Traceroute** – Enter the hostname or IP address to use for the command and click **Traceroute** to start the test. Trace routes are used to determine the network traffic route to navigate to its destination.
- **Dig/NS-lookup** – Enter the IP address or hostname to Dig and click **Dig/NS-lookup** to start the test.

Release Notes

Barracuda Reporting Server Firmware

This is an Early Release, prior to General Release for Barracuda Reporting Server.

The Barracuda Reporting Server provides:

- an aggregate view of data for multiple connected devices
- drill-down capability for a subset of connected devices to see aggregate statistics
- dashboard monitoring for a quick overview of filtering statistics aggregated across all connected devices

The current version supports connecting Barracuda Web Security Gateway devices running firmware version 11.0 or higher.

Possible Issue

- Refresh the dashboard if you have passed the session expiration time.

Barracuda Reporting Server Definition

The Barracuda Reporting Server Definition includes additional quick fixes, outside of firmware, that may include some security fixes.

If there are additional reports that need to be added, the definitions will be distributed to your systems through the Barracuda Reporting Server Definition.

This Early Release has a definition for:

- Advanced Threat Detection (ATD) Reports for Barracuda Reporting Server, if you have ATD activated on your connected Barracuda Web Security Gateway device(s).