

Step 3: How to Configure the Barracuda Load Balancer Web Interface

<https://campus.barracuda.com/doc/3538952/>

Before configuring the web interface, complete [Step 2: How to Configure the Barracuda Load Balancer](#).

In this article:

Configure the Barracuda Load Balancer from the Web Interface

After specifying the IP address of the Barracuda Load Balancer and opening the necessary ports on your corporate firewall, configure the Barracuda Load Balancer from the web interface. Make sure the system being used to access the web interface is connected to the same network as the Barracuda Load Balancer, and that the appropriate routing is in place to allow connection to the Barracuda Load Balancer's IP address via a web browser.

To configure administrative settings on the Barracuda Load Balancer:

1. From a web browser, enter `http://` followed by the IP address of the Barracuda Load Balancer, followed by the default web Interface HTTP Port (:8000).
For example: `http://192.168.200.200:8000`
2. Log into the administration interface using **admin** for both the username and password.
3. Go to the **BASIC > IP Configuration** page and perform the following steps:
 1. Enter the following information in the **WAN IP Configuration** section:
 - **IP Address**. The address associated with the port that connects the Barracuda Load Balancer to the WAN.
 - **Subnet Mask**. The subnet mask assigned to the WAN interface of the Barracuda Load Balancer.
 - **Default Gateway**. The default router for network traffic not destined for the local subnet.
 - **Allow administration access**. Set to **Yes** if you want to allow administration access using this IP address. The web interface port has a default of 8000 but can be changed on the **BASIC > Administration** page.
 2. If the Barracuda Load Balancer is in Bridge-Path mode, or if only Direct Server Return mode is being employed, then go to Step [3c](#).
If you are configuring a passive Barracuda Load Balancer in a cluster, then go to Step [3c](#).
If the system becomes active and if it is in Route-Path mode, it will assume the LAN IP

address and netmask that are configured on the originally-active Barracuda Load Balancer. See *High Availability Deployment*.

Enter the following information in the **LAN IP Configuration** section:

- **LAN IP Address and LAN Netmask.** The address that connects the Barracuda Load Balancer to the LAN. This is only used for two-armed Route-Path mode or, if in one-armed Route-Path mode, for management.
 - **Allow administration access.** Set to Yes if you want to allow administration access using this IP address. The web interface port has a default of 8000 but can be changed on the **BASIC > Administration** page.
3. If desired, enter the following information in the **Management IP Configuration** section:
 - **Management IP Address and Management Netmask.** The management IP address can be used only for administration access and is optional. It should not be on the same network as either the LAN or WAN IP address. On certain 640 models, it is used by the MGMT port on the front of the unit; on most other models, it is used by the Ethernet port on the back of the appliance.
 - **Allow administration access.** Set to Yes. The web interface port has a default of 8000 but can be changed on the **BASIC > Administration** page.
 4. Enter the IP address of your primary and secondary DNS servers.
 5. Enter the default hostname and default domain name of the Barracuda Load Balancer.
 6. If the Barracuda Load Balancer is behind a proxy server, enter the relevant parameter.
 7. Click **Save Changes**.

If you change the IP address that you were using to access your Barracuda Load Balancer, you will be disconnected from the web interface. Use the new IP address to connect and log in again.

8. If you want this Barracuda Load Balancer to operate in Bridge-Path mode, and this is not a backup Barracuda Load Balancer in a cluster, click **Convert** to change the operation from Route-Path to Bridge-Path.
4. Select **BASIC > Administration**, and perform the following steps:
 1. Assign a new administration password to the Barracuda Load Balancer.
 2. Make sure the local time zone is set correctly.

Time on the Barracuda Load Balancer is automatically updated via NTP (Network Time Protocol). It requires that port 123 is opened for outbound UDP traffic on your firewall (if the Barracuda Load Balancer is located behind one).

It is important that the time zone is set correctly because this information is used to coordinate traffic distribution and in all logs and reports. Also, if this system is going to be clustered with another one, both systems must have the same time zone.
 3. If desired, change the port number used to access the Barracuda Load Balancer user interface. The default port is 8000.
 4. Enter the amount of time, in minutes, for the length of your web interface session before you are logged off due to inactivity.
 5. (Optional) Specify your local SMTP server. Enter the email address for your administrator to receive system alerts and notifications
 6. Click **Save Changes**.

Subscription Status

the Barracuda Load Balancer has access to the activation servers, your Energize Update and Instant Replacement subscriptions are most likely active. If not, you will see a warning at the top of every page. You must activate your subscriptions before continuing.

Click on the link in the warning message or use the link on the **BASIC > Status** page to open up the Barracuda Networks Product Activation page in a new browser window. Fill in the required fields and click Activate. A confirmation page displays the terms of your subscription. On the **BASIC > Status** page, you may need to enter the activation code from the Barracuda Networks Product Activation page to activate your Barracuda Load Balancer.

If your subscription status does not change to *Current*, or if you have trouble filling out the **Product Activation** page, contact your Barracuda Networks sales representative.

Update the Barracuda Load Balancer Firmware

Use the following steps to update the firmware:

1. Go to the **ADVANCED > Firmware Update** page.
2. Read the release notes to learn about the latest features and fixes in the new firmware version.
3. Click **Download Now** next to Latest General Release. Click **OK** on the download duration window.
Updating the firmware may take several minutes. Do not turn off the unit during this process. **Download Now** is disabled if the Barracuda Load Balancer is running the latest firmware version.
4. The Barracuda Load Balancer begins downloading the latest firmware version. Click **Refresh** to view the download status, until you see a message stating that the download has completed.
5. Click **Apply Now** when the download completes.
6. Click **OK** when prompted to reboot the Barracuda Load Balancer.
A Status page displays the progress of the reboot. Once complete, the login page appears.

Update the IPS Definitions

If you are configuring a [passive Barracuda Load Balancer in a cluster](#), then you may skip this set of steps.

To apply the newest definitions for the Intrusion Prevention System:

1. Select **ADVANCED > Energize Updates**.
2. Select **Hourly or Daily for Automatically Update**. The recommended setting is Hourly for IPS definitions.
3. Check to see if the current version is the same as the latest general release. If the rules are up-to-date, proceed to the next section. If the rules are not up-to-date, continue to the next step.
4. Click **Update** to download and install the latest available IPS definitions onto the Barracuda Load Balancer.
5. Click **Save Changes**.

Continue with [Step 4: How to Configure Administrative Settings](#).

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.