Barracuda NG Admin

https://campus.barracuda.com/doc/41116034/

The Barracuda NG Admin application is used to administer Barracuda NG Firewalls and Barracuda NG Control Centers. As a standalone Microsoft Windows application, Barracuda NG Admin is multi-administrator capable and provides instant access to your Barracuda NG units. Unlike web-based administration portals, Barracuda NG Admin allows you to manage multiple Barracuda NG Firewalls from a single interface that remains independent from web browser incompatibilities. You can download Barracuda NG Admin on the Barracuda Networks website: log into the Barracuda Customer Portal, navigate to the **Support** page and click **Access downloads for products**. In the Barracuda NG Firewall product section, select the download category **Administration App (NG Admin)** and download the latest Barracuda NG Admin version.

It is important to use the latest version of Barracuda NG Admin, which includes the newest features. Performing configuration changes using a version of Barracuda NG Admin older than the Barracuda NG Firewall could result in a loss of configuration data.

In this article:

System Requirements

- Windows 7 (32-bit or 64-bit) or Windows 8/8.1 (32-bit or 64-bit)
- Microsoft .NET Framework 4.0 or later
- 30 MB free disk space
- 1 GB RAM
- 1 GHz CPU

Connecting to a Barracuda NG Firewall or NG Control Center

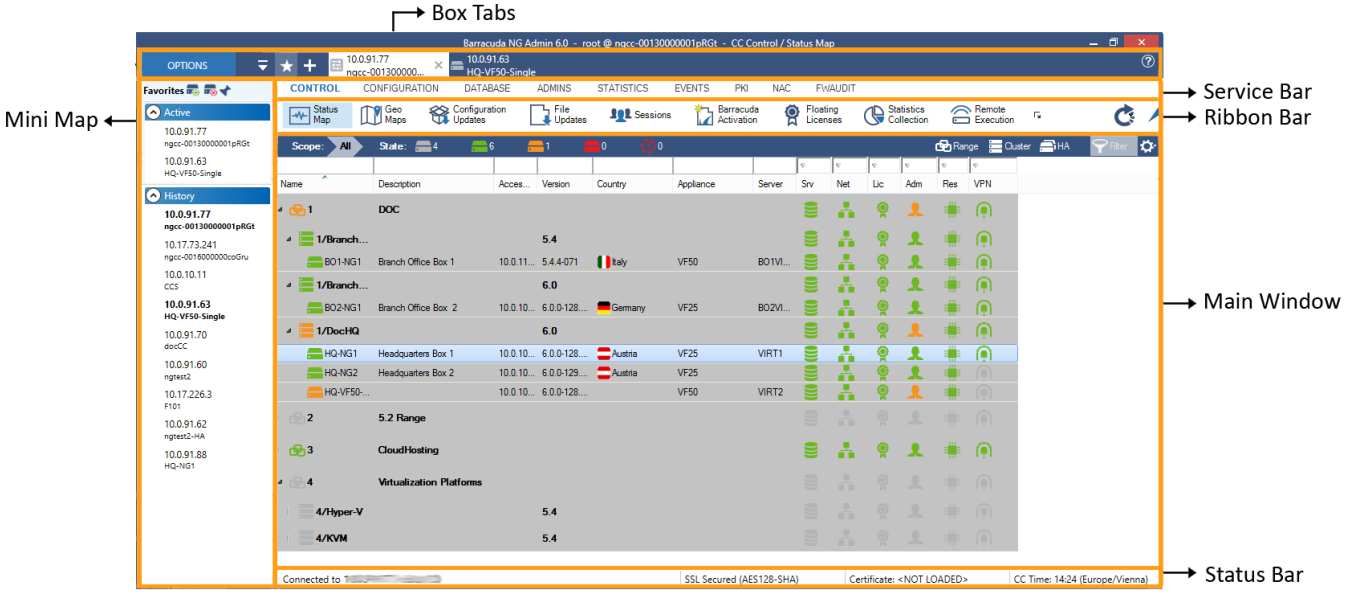
1. Start Barracuda NG Admin.
2. In the **Login** window select the login type:
   - **Box** – Select **Box** to connect to a Barracuda NG Firewall or the box level of a NG Control Center.
   - **Control Center** – Select **Control Center** to log in to the Barracuda NG Control Center.
3. Enter the **Management IP**:
   - Hardware appliances – Enter the default management IP address: 192.168.200.200 or the

management IP address configured by the administrator.
  - Virtual appliances – Enter the IP address configured by the administrator during deployment.
  - Public Cloud – Enter the elastic IP address (AWS) or the VIP/RIP (Azure) assigned to your Barracuda NG Firewall by the public cloud service provider.
4. Enter the login credentials. The default values for all hardware and virtual Barracuda NG Firewalls and NG Control Center, are:
   - **Login**: `root`
   - **Password**: `ngf1r3wall`

     NG Firewalls deployed in AWS use the Instance ID as the default password.
5. Click **Login**
6. If the **Authentication Check,** click **Trust Key**. The authentication check is only displayed on the first login.

The Barracuda NG Admin User Interface

The Barracuda NG Admin user interface is divided into several functional sections. Although the content of functional sections of a Barracuda NG Firewall differs from the Barracuda NG Control center, position and basic functions are identical. The screenshot below shows the Barracuda NG Admin connected to a Barracuda NG Control Center.



Box Tabs

The box tabs display the IP address and hostname of your Barracuda unit. An icon also indicates whether this is a Barracuda NG Firewall or a Barracuda NG Control Center. When logged into more

than one system, further box tabs become available from where you can switch between the currently connected units. The tab for the selected unit is always highlighted. Clicking open tabs allows you to switch between connected units.

Click the **Options** tab on the top left to access the Barracuda NG Admin settings menu, where you can configure general settings for the Barracuda NG Admin application, such as the behavior of connections and configuration elements. For more information, see NG Admin Settings.

Minimap

When opened, the minimap provides an optional list view of all connected Barracuda NG Firewalls or NG Control Centers. To access or close the minimap, click on the star icon in the box tabs column. Click the blue pin icon on top of the map to leave it open during the session - to 'unpin' it, click it again. The minimap is divided into the following sections:

- **Active** – Expanding this section shows the IP addresses and hostnames of all Barracuda NG Firewalls and Barracuda NG Control Centers that are currently connected with an active session. Clicking on an entry opens the currently accessed page of the selected unit.
- **History** – Expanding this section provides a history view of all units that were recently accessed. Clicking on an entry offers the login screen for the selected unit.

To manually add a Barracuda NG Firewall or Barracuda NG Control Center to the minimap, click the **Add Boxes to the Minimap** (green plus) icon on the top of the map and add the unit. The **Enter manually** option in the context menu lets you enter the details of the unit you wish to add. To remove an entry from the minimap, or to clear the history, click the **Remove Boxes from the Minimap** (red minus) icon and select which part of the entries you wish to remove.

Service Bar

The service bar is the main navigation and operation utility of the Barracuda NG Admin user interface and provides a tab for each main section of the Barracuda NG Firewall or Barracuda NG Control Center. Additional services introduced on the Barracuda NG Firewall, e.g., Mail Gateway or VPN, add further tabs to this bar from where you can access settings and sub-sections depending on the configured service.

On the Barracuda NG Firewall, the Barracuda NG Admin interface service bar contains the following tabs:

- **DASHBOARD** – Provides a general system overview of your Barracuda NG Firewall or NG Control Center (box level).

- **CONFIGURATION**– Contains the operative configuration tree for the Barracuda NG Firewall or NG Control Center.
- **CONTROL** – On the Barracuda NG Firewalls, this tab shows information about virtual server and services, current network status, running processes, system and license status, etc.
- **FIREWALL** – Provides real-time and historical information on network traffic and application traffic passing the Barracuda NG Firewall.
- **VPN** – Provides access to VPN real-time information for Site-to-Site and Client-to-Site VPN connections, if configured.
- **LOGS** – Contains information related to system and service logs.
- **EVENTS**– Contains information related to events that are created on the Barracuda NG Firewall.
- **STATISTICS** – Contains information related to statistics generated on the Barracuda NG Firewall.
- **SSH** – Login to the command line interface of the Barracuda NG Firewall. (see also: Command-Line Interface).

On the Barracuda NG Control Center, the Barracuda NG Admin interface service bar contains the following tabs:

- **CONTROL** – On the Barracuda NG Control Center, the **CONTROL** tab provides an overview of all connected units.
- **CONFIGURATION**– Contains the configuration sections for the Barracuda NG Control Center.
- **DATABASE** – Provides details and quick access to available ranges, clusters, boxes, servers, and services of the Barracuda NG Control Center.
- **ADMINS** – Provides access to the section for the administrator's list.
- **STATISTICS**, **EVENTS** – These tabs contain pages related to logs, statistics, and events.
- **FWAUDIT** – Provides access to the section for the Firewall Audit service.

Ribbon Bar

Located directly under the service bar, the ribbon bar provides icons for each section relevant to the selected service bar tab. To access a section, open a tab in the service bar and select an icon from the ribbon bar to open the corresponding settings page. In some cases, you might have to expand the icons section in the ribbon bar to gain access to all sections. In the top right corner, the ribbon bar provides icons to specify system refresh settings. Clicking the last icon disconnects the unit. When disconnected, this icon changes to **Connect**.

Main Window

The main window contains the configuration and information part of Barracuda NG Admin. Depending on the tabs and icons selected from the service and ribbon bars, the main window displays

information that is relevant to the selected item and might also contain further tabs and subsections.

Status Bar

The status bar at the bottom of the Barracuda NG Admin user interface displays information about the certificate status, the SSL connection, and the time zone specified within the box time settings. A license state warning indicator appears if the license of a Barracuda unit enters a critical state, e.g., in case Grace mode goes into effect, if an installed license is expired, or in Demo mode.

> When your license status enters Grace mode, you have 15 days to validate your license. If not licensed after this time, traffic forwarding and VPN will no longer work.

The license state warning indicator is displayed as follows:

- Text only – Installed license is valid, but Grace mode will go into effect in 60 days.
- Yellow background – Installed license is valid, but Grace mode will go into effect in 30 days.
- Orange blinking – Installed license is in Grace mode.
- Red blinking – Installed license is either invalid or Grace mode is expired.

The status of the warning indicator refreshes at box login, when the status page is refreshed, if **License Warning** is clicked, or after a new configuration is activated (see also: Licensing).

Barracuda NG Firewall Configuration

On the **Config** page, you can configure all settings and services of the Barracuda NG Firewall or Barracuda NG Control Center. The config tree contains all configuration sections, listed in hierarchical levels, from where you can add and access virtual servers, firewall services, and, if on a Barracuda NG Control Center, create and configure ranges, clusters, and add your Barracuda NG Firewalls. For more information, see Configuration Tab.

Figures