Getting Started

https://campus.barracuda.com/doc/41116123/

If you are deploying a Barracuda NG Control Center with the CC Wizard, see NG Control Center Getting Started with the CC Setup Wizard.

When deploying a Barracuda NG Firewall, basic settings need to be made before the system can be used in production. There are some differences, depending on the deployment option you choose (hardware, virtual, or public cloud).

Before you Begin

Make sure you completed the steps listed in the deployment articles, depending on which platform you are deploying the Barracuda NG Firewall on:

- **Hardware** – Complete Hardware deployment and the included Quick Start Guide. The Quick Start Guide is included in the box for every Barracuda NG Firewall. Your PC must be connected to the management port of the NG Firewall and use an IP address in the 192.168.200.0/24 range. Do not use 192.168.200.200 because this IP address is the default management IP address of the Barracuda NG Firewall.
- **Virtual (Vx)** – Complete the deployment steps in Virtual Systems (Vx) for your hypervisor.
- **Public Cloud** – Complete the steps in Public Cloud Hosting for your public cloud provider.

Step 1. Prepare the Client

To connect to the Barracuda NG Firewall, you must use the Barracuda NG Admin application. The application is a standalone, portable executable. Always use the latest version of NG Admin. You can download it from the Barracuda Customer Portal.

For more information on the system requirements and NG Admin, see Barracuda NG Admin.

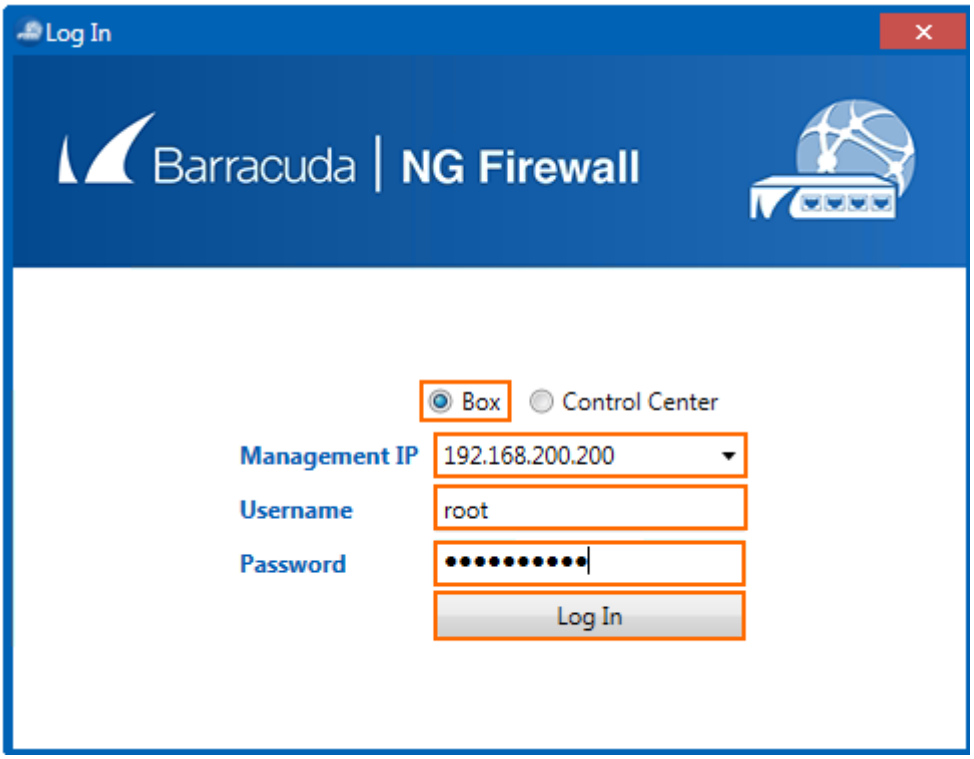
Step 2. Log into the Barracuda NG Firewall

Connect to your Barracuda NG Firewall using Barracuda NG Admin:

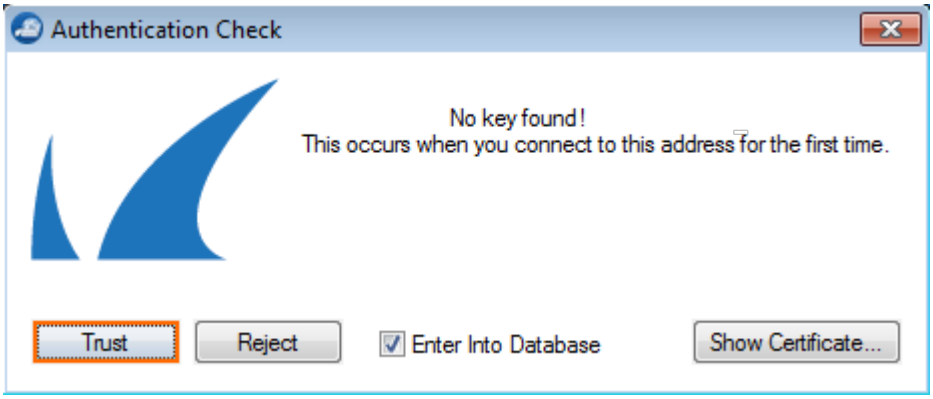
1. Launch Barracuda NG Admin.

2. In the **Log In** window, select **Box**.
3. Enter the **Management IP**, **Username,** and **Password**:

	Management IP Address	Username	Default Password
Hardware	192.168.200.200	root	ngf1r3wall
Virtual (Vx)	Set during deployment	root	ngf1r3wall
Public Cloud - Amazon AWS	Elastic IP pointing to the Barracuda NG Instance	root	Instance ID of your Barracuda NG Instance E.g., **i-0aaaa123**
Public Cloud - Microsoft Azure	**.cloudapp.net** or Virtual IP (VIP) for the cloud service	root	◦ Set during deployment ◦ If not set during deployment: ngf1r3wall



4. Click **Log In**. The **Authentication Check** window opens.
5. Click **Trust**.

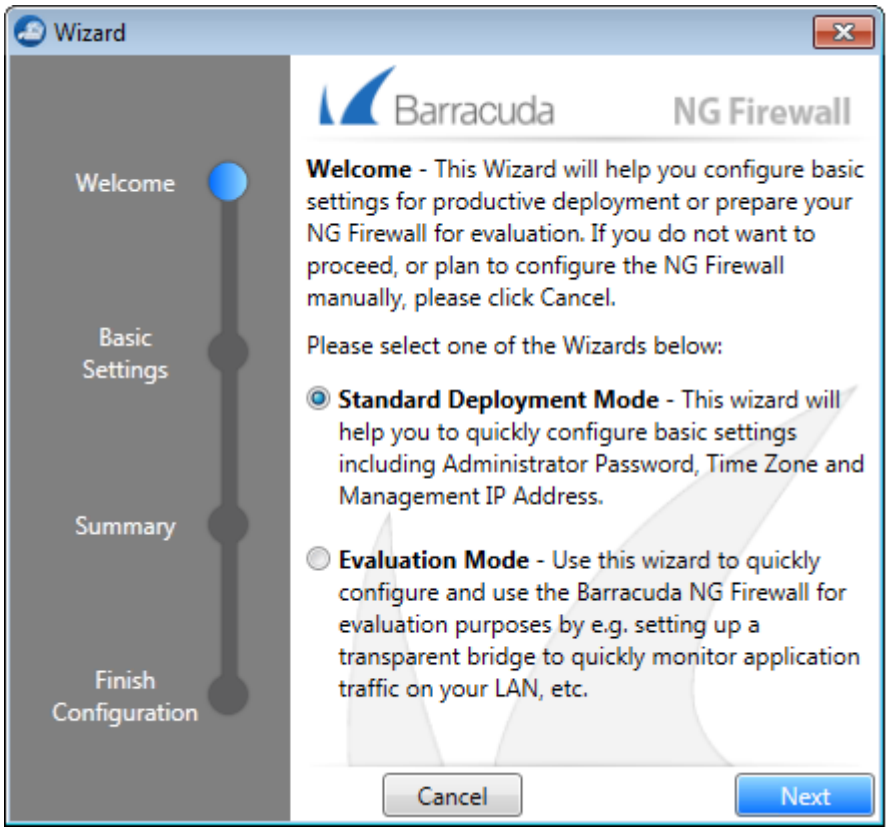


Step 3. Configure Basic Settings

The box wizard can only be used on hardware units. If you are deploying a virtual Barracuda NG Firewall system, you must configure the time zone and change the password manually.

Step 3.1 Complete the Wizard for the Barracuda NG Firewall

If you are using a hardware appliance, the wizard helps you configure basic settings during deployment. Follow the instructions for the **Standard Deployment Mode**. Skip this step if you are connected to a Barracuda NG Firewall in the public cloud because these settings were already configured during deployment.



Step 3.2 Configure the Time Zone and Change the Root Password for the Virtual Barracuda NG Firewall

When using a virtual Barracuda NG Firewall, complete the following tasks:

Task	Link
Change the password	How to Change the Root Password and Management ACL
Set the time zone	Step 1 in How to Configure Time Server (NTP) Settings
(optional) Change the management IP address	How to Change the Management IP Address

Step 4. Configure an Internet Connection

If you are deploying a Barracuda NG Firewall that must connect to the Internet via ISP, configure the Internet connection. If your Barracuda NG Firewall can already access the Internet via Management interface, you can skip this step. The Barracuda NG Firewall F10 to F30x already have a preconfigured DHCP interface on port 4.

Complete the configuration for your type of Internet connection:

Internet Connection Type	Link
Static IP address	How to Configure an ISP with Static IP Addresses
DHCP	How to Configure an ISP with Dynamic IP Addresses (DHCP)
xDSL (PPP, PPPoE and PPTP)	How to Configure an ISP with xDSL
UMTS/3G	How to Configure an ISP with UMTS/3G
ISDN	How to Configure an ISP with ISDN

Step 5. Activate and License your Barracuda NG Firewall

To license your Barracuda NG Firewall, the NG Admin application must be able to connect to the Internet directly or via proxy. For hardware appliances you only need to activate the unit; licenses are automatically downloaded and installed afterwards. For virtual and public cloud systems you must enter a license token before activating your unit. If you are licensing a Barracuda NG Firewall that is to be used in a high availability cluster, it is important to activate the secondary unit first. For more information, see How to Activate and License a Barracuda NG High Availability Cluster.

	License Installation	Link
Hardware	1. Fill out the activation form. 2. Licenses are downloaded and installed automatically. 3. For Barracuda NG Firewall F10 - F30X, preconfigured services must be enabled manually.	How to Activate and License a Standalone Hardware Barracuda NG Appliance

Virtual (Vx) + Public Cloud	1. Enter the license token. 2. Fill out the activation form. 3. Licenses are downloaded and installed automatically.	How to Activate and License a Standalone Virtual Barracuda NG Firewall

Step 6. Configure Administrative Settings

Configure the Barracuda NG Firewall to use your preferred DNS and NTP servers. To receive email notifications from selected services, you must configure a recipient email address.

	Link
DNS Servers	How to Configure DNS Settings
NTP Servers	Step 2 in How to Configure Time Server (NTP) Settings
System Email Notification Address	How to Configure the System Email Notification Address

Next Steps

If you are deploying a Barracuda NG Control Center, continue with NG Control Center Manually Getting Started.

Continue with the steps below to set up the system according to your needs.

	Link
Configure **VLANs**, **routing** and add **additional network interfaces**.	Network
Create and configure the **virtual server**.	• Virtual Servers and Services • How to Configure Virtual Servers
Create and configure **services** (e.g., Forwarding Firewall, VPN,...).	• NG Firewall Services • How to Configure Services
Configure external authentication servers.	Authentication
Configure administrator accounts.	Managing Access for Administrators
Create a high availability cluster	High Availability

Figures

1. getting_started_01.png
2. getting_started_02.png
3. getting_started_03.png