

## How to Create a New Admin Account

<https://campus.barracuda.com/doc/53248462/>

Admin profiles specify which configuration areas and tasks administrative users can access and change on a stand-alone Barracuda NextGen Firewall F-Series or Barracuda NextGen Control Center on box level. Admin users can log into the system using the credentials specified in their profile and view or edit the services and settings defined in the administrative roles assigned to them.

### Administrative Roles

Admin users can view or edit settings and services on the Barracuda NextGen Firewall F-Series according to their assigned roles.

Box Menu	Software Item	Manager	Operator	Mail	Security	Audit	Cleanup
Virus Scanner	Access to configuration tab	Yes	No	No	Yes	No	No
	Modify Configuration	Yes	No	No	Yes	No	No
	Update Pattern	Yes	No	No	Yes	No	No
	Disable/Enable Pattern Update	Yes	No	No	Yes	No	No
Box Menu	Software Item	Manager	Operator	Mail	Security	Audit	Cleanup
Config	Access to configuration tab	Yes	No	No	Yes	Yes	No
	Create a DHA box	Yes	No	No	No	No	No
	Create a PAR file	Yes	No	No	No	No	No
	Create a repository	Yes	No	No	No	No	No
	Create a server	Yes	No	No	No	No	No
	Create a service	Yes	No	No	No	No	No
	Kill configuration sessions	Yes	No	No	No	No	No
	HA synchronization	Yes	No	No	Yes	No	No
Box Menu	Software Item	Manager	Operator	Mail	Security	Audit	Cleanup

<b>Control</b>	<b>Access to configuration tab</b>	Yes	Yes	No	Yes	No	No
	<b>Activate new network configuration</b>	Yes	Yes	No	No	No	No
	<b>Block a server</b>	Yes	Yes	No	No	No	No
	<b>Block a service</b>	Yes	Yes	No	No	No	No
	<b>Time control</b>	Yes	No	No	No	No	No
	<b>Delete Wild Route</b>	Yes	Yes	No	No	No	No
	<b>Import license</b>	Yes	No	No	No	No	No
	<b>Kill sessions</b>	Yes	Yes	No	No	No	No
	<b>Firmware Restart</b>	Yes	Yes	No	No	No	No
	<b>Reboot/Shutdown Box</b>	Yes	Yes	No	No	No	No
	<b>Remove license</b>	Yes	No	No	No	No	No
	<b>Restart network configuration</b>	Yes	Yes	No	No	No	No
	<b>Show license</b>	Yes	Yes	No	No	No	No
	<b>Start a server</b>	Yes	Yes	No	No	No	No
<b>Stop a server</b>	Yes	Yes	No	No	No	No	
<b>Box Menu</b>	<b>Software Item</b>	<b>Manager</b>	<b>Operator</b>	<b>Mail</b>	<b>Security</b>	<b>Audit</b>	<b>Cleanup</b>
<b>DHCP</b>	<b>Access to configuration tab</b>	Yes	Yes	No	No	No	No
	<b>Modify Configuration</b>	Yes	No	No	Yes	No	No
	<b>GUI commands</b>	Yes	Yes	No	No	No	No
<b>Box Menu</b>	<b>Software Item</b>	<b>Manager</b>	<b>Operator</b>	<b>Mail</b>	<b>Security</b>	<b>Audit</b>	<b>Cleanup</b>
<b>Events</b>	<b>Access to configuration tab</b>	Yes	Yes	No	Yes	Yes	Yes
	<b>Confirm events</b>	Yes	Yes	No	No	No	Yes
	<b>Delete events</b>	Yes	No	No	No	No	Yes
	<b>Mark events as read</b>	Yes	Yes	No	No	No	Yes
	<b>Set events to silent</b>	Yes	Yes	No	No	No	Yes
	<b>Stop alarm</b>	Yes	Yes	No	No	No	Yes
<b>Box Menu</b>	<b>Software Item</b>	<b>Manager</b>	<b>Operator</b>	<b>Mail</b>	<b>Security</b>	<b>Audit</b>	<b>Cleanup</b>

<b>Firewall</b>	<b>Access to configuration tab</b>	Yes	Yes	No	Yes	Yes	No
	<b>Modify Configuration</b>	Yes	No	No	Yes	No	No
	<b>Access to trace tab</b>	Yes	No	No	Yes	No	No
	<b>Remove entries from cache</b>	Yes	No	No	Yes	No	No
	<b>Terminate connections</b>	Yes	Yes	No	Yes	No	No
	<b>Create dynamic rules</b>	Yes	Yes	No	Yes	No	No
	<b>Kill a process</b>	Yes	Yes	No	Yes	No	No
	<b>Modify connections</b>	Yes	Yes	No	Yes	No	No
	<b>Modify traces</b>	Yes	No	No	Yes	No	No
	<b>Toggle traces</b>	Yes	No	No	Yes	No	No
	<b>View rules</b>	Yes	No	No	Yes	No	No
<b>Box Menu</b>	<b>Software Item</b>	<b>Manager</b>	<b>Operator</b>	<b>Mail</b>	<b>Security</b>	<b>Audit</b>	<b>Cleanup</b>
<b>Logs</b>	<b>Access to configuration tab</b>	Yes	No	No	Yes	Yes	Yes
	<b>Delete resource logs (box_)</b>	Yes	No	No	No	No	Yes
	<b>Delete service logs</b>	Yes	No	No	No	No	Yes
	<b>Read resource logs (box_)</b>	Yes	No	No	Yes	Yes	Yes
	<b>Read service logs</b>	Yes	No	No	Yes	Yes	Yes
<b>Box Menu</b>	<b>Software Item</b>	<b>Manager</b>	<b>Operator</b>	<b>Mail</b>	<b>Security</b>	<b>Audit</b>	<b>Cleanup</b>
<b>Mail</b>	<b>Access to configuration tab</b>	Yes	No	Yes	No	Yes	No
	<b>Modify Configuration</b>	Yes	No	No	Yes	No	No
	<b>GUI commands</b>	Yes	No	Yes	No	No	No
	<b>View Stripped Attachments</b>	Yes	No	Yes	No	Yes	No
	<b>Retrieve Stripped Attachments</b>	Yes	No	Yes	No	No	No
	<b>Delete Stripped Attachments</b>	Yes	No	Yes	No	No	No
<b>Box Menu</b>	<b>Software Item</b>	<b>Manager</b>	<b>Operator</b>	<b>Mail</b>	<b>Security</b>	<b>Audit</b>	<b>Cleanup</b>
<b>Access Control Service</b>	<b>Access to configuration tab</b>	Yes	No	No	Yes	No	No
	<b>Modify Configuration</b>	Yes	No	No	Yes	No	No
	<b>Enable Commands</b>	Yes	No	No	Yes	No	No
	<b>Block Sync</b>	Yes	No	No	Yes	No	No

## Create an Administrator Profile

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrators**.
2. Click **Lock**.
3. In the **Administrators** section, click + to add an administrator account.

4. Enter a unique **Name** for the account and click **OK**. The **Administrators** window opens.  
Do NOT use the following names because they are reserved by the system: *master, ha, root, bin, adm, daemon, lp, system, sync, shutdown, halt, mail, operator, nobody, support, uucp*.
5. Enter the **Full Name** of the administrator or a description for the account.
6. In the **Assigned Roles** table, add the appropriate administrative roles for the user. For a description of roles, see the **Administrative Roles** section.
7. If you wish to grant permission for shell level access, select an option from the **System Level Access** list. You can select:
  - **No OS Login** – Shell access is denied.
  - **Standard OS Login** – Allows access on the OS layer via a default user account (home directory: user/phion/home/username).
  - **Restricted OS Login** – Permits access via a restricted shell (rbash) with limitations (e.g., specifying commands containing slashes, changing directories by entering cd, ...). A restricted login confines any saving action to the user's home directory.
8. Select the **Authentication Level** that is required to access a system.
9. If external authentication is required, select the corresponding method from the **External Authentication** field.
10. When using a password, select the corresponding scheme from the **Password Validation** list.
11. Enter the **External Login Name** for the authentication scheme if it is different than the admin account name.
12. Enter the password for the Barracuda NextGen Admin login. When creating an account, the new password must be entered in both the **Current** and **New** fields, even though the password has not yet been created. The password must be confirmed by re-entering it in the **Confirm** field.
13. Import the **Public RSA Key** if required.
14. If required, use the **Peer IP Restriction** table to set an access restriction on IP address and/or subnet level on which Barracuda NextGen Admin runs.
15. From the **Login Event** list, select how a login is recorded. You can select.
  - **Service Default (default)** – refers to the settings made within the Barracuda NextGen Control Center Access Notification (see [How to Configure Access Notifications](#)).
  - **Silent** – suppresses any event notification.
16. Click **Send Changes** and **Activate**.

Your admin user can now log into the Barracuda NextGen Firewall F-Series or Barracuda NextGen Control Center box and view or edit the services according to their assigned roles.

© Barracuda Networks Inc., 2020 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.