How to Create a New Administrator Account

https://campus.barracuda.com/doc/96026581/

Administrator accounts specify which configuration areas and tasks administrative users can access and change on a standalone Barracuda CloudGen Firewall or Barracuda Firewall 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

Users can view or edit settings and services on the Barracuda CloudGen Firewall 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**

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

Firewall	**Access to configuration tab**	Yes	Yes	No	Yes	Yes	No
	Modify configuration	Yes	No	No	Yes	No	No
	Access to trace tab	Yes	No	No	Yes	No	No
	Remove entries from cache	Yes	No	No	Yes	No	No
	Terminate connections	Yes	Yes	No	Yes	No	No
	Create dynamic rules	Yes	Yes	No	Yes	No	No
	Kill a process	Yes	Yes	No	Yes	No	No
	Modify connections	Yes	Yes	No	Yes	No	No
	Modify traces	Yes	No	No	Yes	No	No
	Toggle traces	Yes	No	No	Yes	No	No
	View rules	Yes	No	No	Yes	No	No
Box Menu	**Software Item**	**Manager**	**Operator**	**Mail**	**Security**	**Audit**	**Cleanup**
Logs	**Access to configuration tab**	Yes	No	No	Yes	Yes	Yes
	Delete resource logs (*box_*)	Yes	No	No	No	No	Yes
	Delete service logs	Yes	No	No	No	No	Yes
	Read resource logs (*box_*)	Yes	No	No	Yes	Yes	Yes
	Read service logs	Yes	No	No	Yes	Yes	Yes
Box Menu	**Software Item**	**Manager**	**Operator**	**Mail**	**Security**	**Audit**	**Cleanup**
Mail	**Access to configuration tab**	Yes	No	Yes	No	Yes	No
	Modify configuration	Yes	No	No	Yes	No	No
	GUI commands	Yes	No	Yes	No	No	No
	View stripped attachments	Yes	No	Yes	No	Yes	No
	Retrieve stripped attachments	Yes	No	Yes	No	No	No
	Delete stripped attachments	Yes	No	Yes	No	No	No
Box Menu	**Software Item**	**Manager**	**Operator**	**Mail**	**Security**	**Audit**	**Cleanup**
Access Control Service	**Access to configuration tab**	Yes	No	No	Yes	No	No
	Modify configuration	Yes	No	No	Yes	No	No
	Enable commands	Yes	No	No	Yes	No	No
	Block sync	Yes	No	No	Yes	No	No
Box Menu	**Software Item**	**Manager**	**Operator**	**Mail**	**Security**	**Audit**	**Cleanup**
SSH	**admintcpdump**	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. This account name is used to log into the firewall.
   > 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 Firewall 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 Firewall 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 Firewall 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 CloudGen Firewall or Barracuda Firewall Control Center box and view or edit the services according to their assigned roles.