How to Change the Root Password and Management ACL

https://campus.barracuda.com/doc/48203259/

The root password is used for the superuser **root**. The user **root** can log into the basic subsystems and OS. Unless set during deployment, the default root password is **ngf1r3wall**. The root password should be changed immediately after the first login. Do not use the root user for daily configuration tasks; instead, use a firewall admin account.

Password requirements

Passwords can consist of small and capital characters, numbers, and non alpha-numeric symbols except **#**, **&, §** and **spaces**. Barracuda NextGen Admin rates the password strength according to the entered characters. A password strength of strong or best is recommended for the root password.

Change the root password

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **System Access**.
3. Click **Lock**.
4. In the **Root Password** section, enter the password for the root user.
5. Click **Send Changes** and **Activate**.

Management Access Control Lists

Misconfigurations of the Access Control Lists cause NextGen Admin to not be able to communicate with the firewall. The only way to revert this change is to log into the physical console of the system and follow the instructions from Barracuda Networks Technical Support to manually recover connectivity.

The management ACL specifies which IP addresses can access the system. Use the management access control list to whitelist networks that are allowed to connect via NextGen Admin to the F-Series Firewall or Control Center. Only these whitelisted networks are allowed access to the IPv4 or IPv6 management IPs on TCP ports 22 (secure shell) and 800-820. Access from all other addresses to these port/addresses are denied.

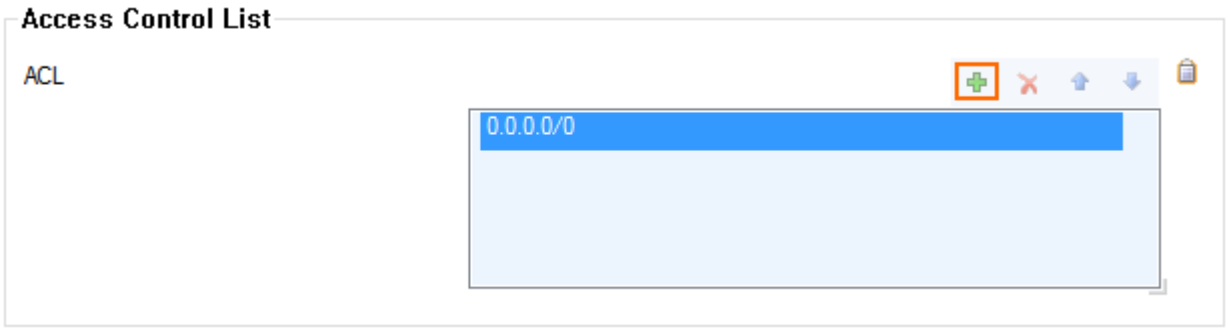
By default, access is allowed from an arbitrary address. Changing the ACL does not terminate active admin sessions. To enforce ACL changes, manually terminate active sessions on the **FIREWALL > Sessions** page.

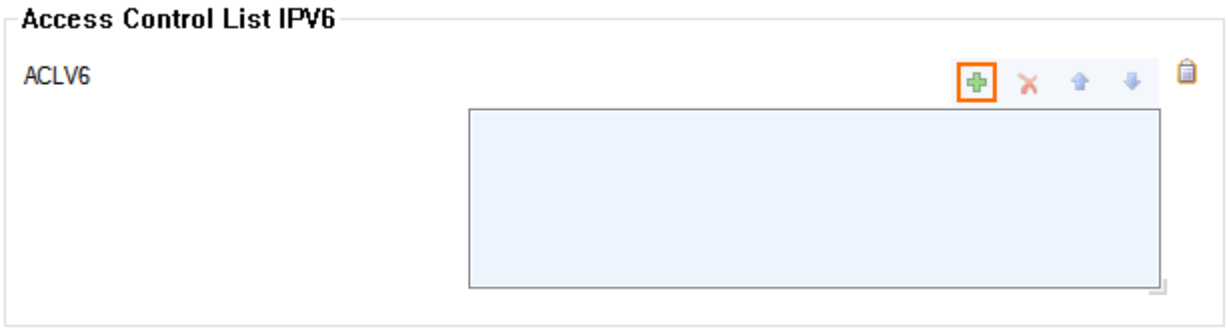
When deploying a CloudGen Firewall in Azure, the ACL is enforced only when the interface is changed from dhcp to ethx and assigned a static IP address. For more information, see Reserved, Static and Public IP Addresses in the Azure Cloud using ASM.

If you configure only IPv6 networks, verify that an IPv6 management IP address is available. For more information, see How to Add an IPv6 Management IP Address.

Configure Management Access Control Lists

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **System Access**.
3. Click **Lock**.
4. In the **Access Control Lists** section, click **+** and add IPv4 networks and/or IP addresses to the **ACL for IPv4** list.
5. Click **+** and add IPv6 networks and/or IP addresses to the **ACL for IPv6** list.





6. Click **Send Changes** and **Activate**.

Figures

1. acls.png