

How to Change the Root Password and Management ACL

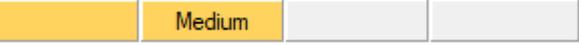
<https://campus.barracuda.com/doc/98210587/>

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 must 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-alphanumeric symbols, except white spaces. Barracuda Firewall Admin rates the password strength according to the entered characters. A password strength of strong or best is recommended for the root password.

The complexity of the password depends on the usage of a mixture of the allowed characters, numbers, and non-alphanumeric symbols. These types of characters are weighted differently, and the occurrence of each character or symbol from a certain category in the password contributes individually to the strength of the final password. While typing, the strength of the password is permanently recalculated. The result is indicated in the user interface with 4 colored rectangles, where each stands for a certain strength:

Password Strength	User Interface Symbol
Weak	Strength 
Medium	Strength 
Strong	Strength 
Best	Strength 

The expiration interval of the password and a theoretical lockout threshold depends on the corporate compliance of rules for renewing the password and is subject to administrative measures to be taken as required. If necessary, the firewall can be configured to ask the user for entering a new password during the next login.

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**.

Enforce a Password Change

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **System Access**.
3. In the left menu, click **Switch to Advanced** for **Configuration Mode**.
4. Click **Lock**.
5. In the **Root Password** section, select the check box for **Enforce password change** so that the password must be changed during the next login.
6. Click **Send Changes** and **Activate**.

Management Access Control Lists

Misconfigurations of the Access Control lists cause Barracuda Firewall 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 allow-list networks that are allowed to connect via Barracuda Firewall Admin to the CloudGen Firewall or Control Center. Only these allow-listed 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 is denied.

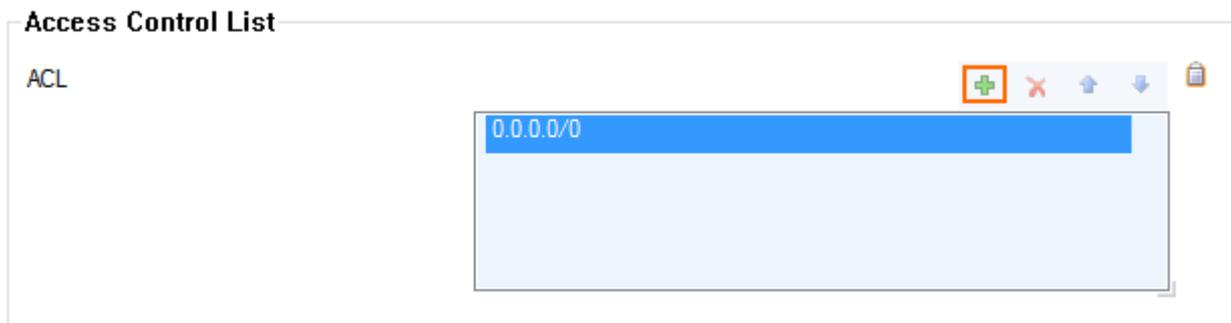
By default, access is allowed from an arbitrary address. Changing the ACL does not terminate active admin sessions. To enforce ACL changes, manually terminate active sessions on the **FIREWALL > Sessions** page.

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.

Configure Management Access Control Lists

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](#).

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. soc_2_weak_password.png
2. soc_2_medium_password.png
3. soc_2_strong_password.png
4. soc_2_best_password.png
5. acls.png

© Barracuda Networks Inc., 2024 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.