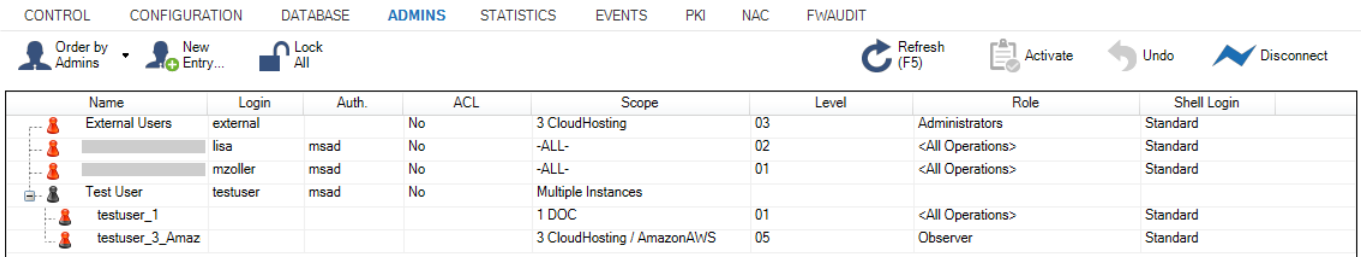
CC ADMINS Tab

https://campus.barracuda.com/doc/48202858/

Administrators are managed on the **Admins** page of the Barracuda NextGen Control Center. This article explains the Barracuda NextGen Firewall F-Series Administration Concept (AC) and provides information on the functionalities of the Barracuda NextGen Control Center **ADMINS** tab.



Barracuda NextGen Firewall F-Series Administration Concept (AC)

When creating administrator profiles, consider the following prerequisites:

1. Create administrative roles (**Global Settings > Administrative Roles**). For information on admin user creation, see: How to Configure Administrative Profiles.
2. Define node properties. For more information, see CC CONFIGURATION Tab.
3. Create the required administrators to fit the concept. To create a new admin under the **ADMINS** tab, click **New Entry** in the ribbon bar and configure the settings. The user then appears in the column.

Default User Rights

Distinguishing between a standalone Barracuda NextGen Firewall F-Series and a system within a Barracuda NextGen Control Center cluster, Administration Concept (AC) offers different services for each system. Every Barracuda NextGen Firewall F-Series has the user 'root' who has unlimited rights in the entire system. In addition, the 'support' user is granted access to the system via the operating system only.

If you need to work on the Barracuda NextGen Admin management interface, you can introduce so-called 'root aliases'. Within the management layer, the status of these users is on equal terms with the status of 'root'. On the other hand, there are no root aliases on operating system layer allowing system access to other users than the system users 'root' and 'support'. Root and root alias also differ in the authentication mode. For authenticating the alias, either a RSA 1024-bit key or a password can be used, whereas root is only authenticated with a password.

- Because all these users are counted among system users, the default access notification

scheme that is configured for each particular service automatically applies to them.

Default user rights overview:

User	Access via Barracuda NextGen Admin	SSH	Console Login	Characteristics
root	yes, password or key	RSA keys, password	yes, password	
support	no	password	password	default Linux user, UID=9999
root alias	yes, password or key	RSA keys, password	no	optional, deactivation possible

The MD5 password hashes of 'root' and 'support' [*UID=9999, group support*] are stored in */etc/shadow* (operative instance for system access) and in */opt/phion/config/configroot[active]/boxadm.conf* (global configurative instance, operative instance for system access). Any authentication data of the root aliases is stored in these two files. *libpwdb*has been manipulated to disable password changes on the command line via passwd for all users.

libpwdb is required by the PAM module *pam_pwdb.so* and is used by default if the method for password changes requiring authentication via the admin DB has not been implemented. The implemented procedure provides for configurational and operational coherence of the authentication data entities.

System access of the 'support' user is recommended for serial access on the box because it is only of restricted use. In addition to the basic services described above, the scope and the performance of the pAC is significantly broadened and enhanced in combination with a multi-administrator CC. Administrators are managed in the Barracuda NextGen Control Center and are reported to the Barracuda NextGen Firewall F-Series systems within their executive scope. For high availability purposes, the administrators 'master' and 'ha' equivalent to 'root' are introduced:

- **ha** – 'ha' is used for data synchronization of two HA partner systems (for example, fw-sync).
- **master** – 'master' is used for configuration updates, status updates, etc.

The Admins Column

The columns under the **ADMINS** tab display the following information:

- **Name** – This column displays the full username.
- **Login** – The login name of the administrator.
- **Auth.** – The authentication method.
- **ACL** – Information about the access control list that applies to the user.

- **Scope** – Defines the administrative scope.
- **Level** – Defines the configuration level of the user.
- **Role** – Defines the adminitrative role of the user.
- **Shell Login** – Defines the shell login method of the user.

You can arrange this list by clicking the **Order by Admins** icon in the ribbon bar if required.

Figures

1. cc_adm.png