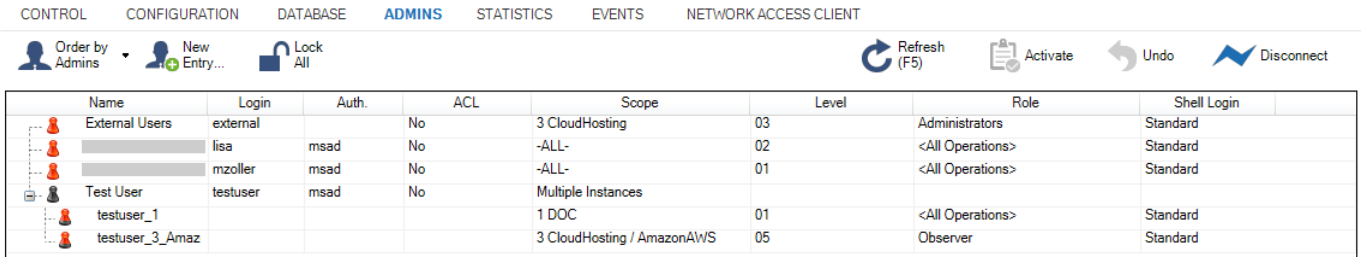
CC ADMINS Tab

https://campus.barracuda.com/doc/79463231/

The **Admins** page of the Barracuda Firewall Control Center lets you create profiles for administrative users and assign configuration access properties and roles. To access the **Admins** page, click the **Admins** tab in the ribbon bar.



The columns on the **ADMINS** page display the following information for created users:

- **Name** – 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** – The administrative scope.
- **Level** – The configuration level of the user.
- **Role** – The administrative role of the user.
- **Shell Login** – The shell login method of the user.

To rearrange this list, click the **Order by Admins** icon in the ribbon bar.

The hierarchical level of an administrative user entry is indicated by the following icons:

Icon	Description
	Administrative user. The orange icon is shown when a new entry is created on the first level.
	The grey icon is shown when an administrative user entry is created that contains one or multiple instances.
	Instance. The striped icon is shown when an entry is created on the second level to grant an administrative user different permissions or roles on further administrative scopes (ranges or clusters).
	Indicates that the entry for this administrative user or instance is locked for configuration.

Creating Administrators

To create administrator profiles, you must first:

1. Create administrative roles (**Global Settings > Administrative Roles**).
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. For more information, see How to Configure Administrative Profiles.

Administration Concept

Every firewall has the user 'root' who has unlimited rights in the entire system. In addition, the user 'support' has access to the system via the operating system only. Different services are available depending on whether you are using a stand-alone firewall or a system managed by a Control Center.

If you need to work on the Barracuda Firewall Admin management interface, you can introduce 'root aliases'. The status of these users is equal to the status of 'root'. However, root aliases do not allow 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 an RSA 1024-bit key or a password can be used. 'Root' is authenticated only with a password.

> Because all these users are considered system users, the default access notification scheme configured for each particular service automatically applies to them.

Default User Rights Overview

User	Access via Barracuda Firewall 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 of only 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 Control Center and are reported to the Barracuda CloudGen Firewall systems within their executive scope. For high availability purposes, the administrators 'master' and 'ha' are introduced and equivalent to 'root':

- **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.

Figures

1. cc_adm.png
2. orange.png
3. grey.png
4. striped.png
5. locked.png