How to Configure Administrative Profiles

Administrative profiles define the authentication setup for admin users and specify which ranges/clusters, services and configuration areas the users can access on a Barracuda NextGen Control Center and its managed Barracuda NextGen Firewall F-Series systems. When c reating an administrative profile assign the administrative scope (e.g., range and cluster) to the user and specify the login details. Then you assign a configuration level to the profile and set the service permissions and restrictions by applying one or several administrative roles. Administrative profiles are extendable, scopes and permissions can be added at any time by configuring further instances.

In this article:

Step 1. Assign the Administrative Scope

Add an administrator account and select the range and cluster to which the user should have access.

1. Open the **ADMINS** tab.
2. Click **New Entry**.
3. Enter a **Name** for the account. This is the user login name.
4. From the **Range** list, select which ranges the admin should be able to access.
   - If you select -**ALL-** , the user has access to all ranges and clusters.
   - If you select **-Linked-Only-**, you can customize the administrative scope by selecting specific range and clusters from the **Links** lists in the **Administrator** window.
5. From the **Cluster** list, select which clusters that the admin can access.
   - If you select **-ALL-** , the administrative scope is widened to all clusters within the selected range.
6. Click **OK**.

The administrative scope is now defined for the user and the **Administrator** configuration window opens for further configuration.

Step 2. Configure Authentication Settings

When using external authentication, you must also configure the authentication scheme that is used on the **Infrastructure Services > Authentication Service** pages for the Barracuda NextGen Control Center's box layer and on all Barracuda NextGen F-Series Firewalls that are managed by the Control Center. For more information, see Authentication.

You can use either local or external authentication for admin users:

Local Authentication

When creating an admin account using local authentication, configure the following settings in the **Administrator** window (To edit an existing admin profile, right click the profile, select **Lock All Instances** and edit it .):

1. On the **Administrator** page, select **Local (No external Authentication)** from the **External Authentication** list.
2. Enter the **Full Name** and **Password** for the user in the **General** section.
3. Click the **Details** tab.
4. Specify the password settings in the **Password Parameters** section.
5. Click **OK**.

6. Click **Activate**.

External Authentication

When creating an admin account using external authentication, configure the following settings in the **Administrator** window (To edit an existing admin profile, right click the profile, select **Lock All Instances** and edit it .):

1. On the **Administrator** page, select the authentication scheme from the **External Authentication** list. E.g., **MS Active Directory**.
2. Click the **Details** tab.
3. Select the applicable authentication method from the **Authentication Level** list.
4. When selecting **Key** or **Password or/AND Key**, you must import the **Public Key**.
5. Click **OK**.
6. Click **Activate**.

Step 3. Configure Access Permissions and Restrictions

Specify the configuration and access level and assign administrative roles to the account. The default levels for config tree nodes are 99 or lower for read access, and 2 or lower for write access. Usually, the write level is lower than the read level.

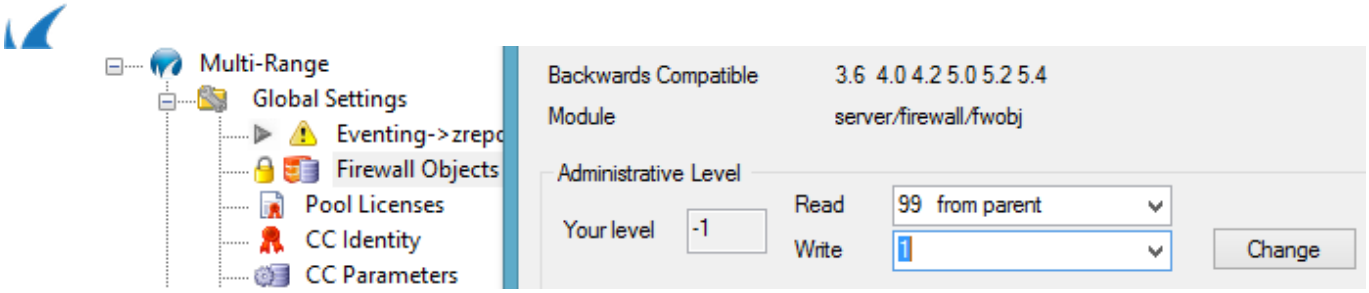
1. In the **Administrator** configuration window, click the **Administrator** tab. (To edit an existing admin profile, right click the profile, select **Lock All Instances** and edit it.)
2. Specify the **Configuration Level** for the user in the **Operative Settings** section. 2 or lower means write access, 99 or lower means read access (see also Control Center Admins).
3. Assign one or several administrative roles,
   - Select the role from the **Roles** list and click **Add**. (For more information on administrative roles, see How to Configure Administrative Roles), or
   - Select the **Allow all Operations** check box to grant permission for all administrative role operations. This overrides all administrative roles that have been assigned to the administrator.
4. To grant permission for shell level access, select an option from the **Shell Level** list. You can select:
   - **No Login** – Shell access is denied.
   - **Standard Login** – A llows access on the OS layer via a default user account (home directory: `user/phion/home/username`).
   - **Restricted 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 users home directory.
5. Click **OK**.
6. Click **Activate**.

Your admin user can now log into the Barracuda NextGen Control Center using the credentials specified in their profile and view or edit the services and settings defined in the assigned administrative roles.

Step 4. (Optional) Define Node Properties

To change configuration levels in the Barracuda NextGen Control Center config tree,

1. Lock the configuration node in the config tree.
2. Right-click the node and select **Properties**.
3. Edit the **Read** and **Write** levels in the **Administrative Level** section.



4. Click **Change**.

By default, the configuration level for an object is taken from its parent node. If you change a level, it is displayed as 'explicit'. When you change the level of a parent node, the levels of all nodes below it are also changed. Be aware that nodes with status 'explicit' must be changed manually.

Create new Admin Instances to Add Scope and Permissions to Existing Profiles

To grant an administrative user different permissions or roles on further administrative scopes (ranges or clusters),

1. Open the **ADMINS** tab.
2. Right-click the user.
3. Click **lock all instances**.
4. Right click the user again and select **create new instance**.
5. Edit the settings as described in the above configuration sections.

   When assigning clusters to an existing administrative profile, do not choose the 'linked only' option as this will generate an error message. Instead, choose a single cluster.

6. Click **OK**.
7. Click **Activate**.

Name	Login	Auth.	ACL	Scope	Level	Role	Shell Login
External Users	external		No	3 CloudHosting	03	Administrators	Standard
Test User	testuser	msad	No	Multiple Instances			
testuser_1				1 DOC	01	<All Operations>	Standard
testuser_3_AmazonAWS				3 CloudHosting / AmazonAW	05	Observer	Standard

The administrative profile is now displayed in a tree structure, showing all instances when expanded.

Figures