Control Center Admins

Administrative accounts allow multiple users to simultaneously manage the Barracuda NextGen Control Center and its managed Barracuda NextGen F-Series Firewalls. Initially, every Control Center is managed by the user *root* who has unlimited access rights. The user *root* has the ability to grant system access to other administrators who, depending on the assigned user rights, are allowed or denied to perform certain operations. This is done by creating administrative profiles. Administrative profiles can be configured to use local or external authentication. The profile settings both specify the scope that an administrator can access (e.g., range or cluster) and define permissions and restrictions specified in the administrative roles that are assigned to the profile. Administrative roles define which services an administrator is allowed to use on the Control Center and the managed firewalls. The configuration level specifies which areas in the config tree an administrator has read and/or write access to. The lowest (or best) configuration level that can be assigned to an administrator is 1 (like the user *root*). When an admin user creates a new administrative profile, the new user can, at best, receive the configuration level plus one of the creating admin.

Administrative Roles

The Barracuda NextGen Control Center provides a set of predefined administrative roles that can be modified if required and applied to an admin profile (e.g., Manager, Editor, etc.). Administrative roles define which services administrators are allowed to use on the Control Center and the managed firewalls and which operations the administrator is allowed to perform within the different services (e.g., terminate VPN tunnels, etc.). When creating an administrative profile, you can assign multiple administrative roles to a Control Center administrator account.

For more information, see How to Configure Administrative Roles.

Administrative Profiles

When introducing an administrator on the Control Center, create an administrative profile and assign access privileges, permissions, and restrictions.

An administrative profile consists of the following settings:

- **Account Settings** – Account settings define various parameters of an administrator account, such as username, authentication method, password expiration policy, shell access level, etc. You can authenticate administrators via local or external schemes (e.g., MS Active Directory, RADIUS, LDAP, etc.). External authentication enables the Control Center and the firewalls to verify the credentials of an administrator against any supported authentication server. Administrators can use their external authentication (e.g., MSAD) password for logging into the F-Series environment. Optionally, the administrator can also receive access rights to the operating system layer (shell login).
- **Administrative Scope** – By assigning elements like a range or cluster, the administrative scope implicitly defines the systems that the administrator can access. The administrative scope also restricts the administrator's view on the Control Center (e.g., status map, config tree, etc.) and access to certain F-Series Firewalls that are managed by the Control Center.
- **Configuration Levels** – The configuration level defines the read and write access a user has on configuration nodes in the Control Center config tree. When creating an administrative profile, you have to apply a configuration level to the administrative user. In addition, you can specify or change configuration levels in the config tree. To read or edit a configuration node in the config tree, the administrative user must have a configuration level that is lower than the node's read and write level.

For more information, see How to Configure Administrative Profiles.

Creating CC Admins to Manage Other CC Admins

By default the CC admins using the predefined administrative roles are not allowed to administer other CC (sub-

)admins.The following criteria must be met in order for an CC admin to be able to mange other admins:

- The administrative role of the CC admin must include the **Manage Admins** permission.
- The configuration level of the CC admin must be lower than the configuration level of the CC sub-admins that are to be managed.
- The administrative scope of the CC admin must be explicitly defined and be at least the same than the CC sub-admins that are to be managed.

Box Level Control Center Admins

Barracuda NextGen Control Center box level admins must be created separately on the box level of the Control Center and be configured as if on a stand-alone F-Series Firewall.

For more information, see How to Create a New Admin Account.