How to Configure Administrator Access

https://campus.barracuda.com/doc/48202082/

The Barracuda Load Balancer ADC is shipped with predefined administrator roles, each with distinct operational and configuration privileges. These roles can be assigned to users to perform specific job functions. The **admin** role, by default, is assigned to the administrative user who has permission for role management and also has access to all of the functionality of the Barracuda Load Balancer ADC.

Administrator Account Settings

On the **ADVANCED > Admin Access Control** page in the **Administrator Account Settings** section, you can configure a password security policy to ensure that administrators and users create secure passwords. You can also configure a policy to lock administrator accounts after a specified number of failed login attempts. For more information on password policy and account lockout policy settings, refer to the online **Help**.

Configure the Password Policy

Click **Password Policy Settings** to configure the following:

- **Policy** - You can select either **Default** or **Custom**. Select **Custom** to modify the password policy.
- **Minimum Characters** - Specify the minimum number of characters needed for the password (the default value is 8).
- **Contains** - Specify the types of characters that must be present in each password:
  - **At Least One Upper Case Character**
  - **At Least One Lower Case Character**
  - **At Least One Special Character**
  - **At Least One Digit**
- **Expires In** - Time until password expires:
  - **3 Months**
  - **6 Months**
  - **1 Year**
  - **Never**
  - **Other** - Specify between 30 and 999 days.
- **Notify Before Expiry** - Time before notifying the user that his or her password is about to expire.
  - **1 Week**
  - **2 Weeks**

Configure the Account Lockout Settings

To prevent unauthorized access to the Barracuda Load Balancer ADC, click **Account Lockout Settings**. Use these settings to specify when a user will be locked out from the Barracuda Load Balancer ADC based on the number of times they have failed to enter their login credentials correctly.

- **Maximum Failed Login Attempts** - Specify the acceptable number of failed login attempts (default is 5).
- **Failed Login Time Threshold** - Specify the time in minutes in which consecutive failed login attempts are counted (default is 15).
- **Lock User Account** - Specify the time in minutes to lock the admin account if the user fails to login more than the **Maximum Failed Login Attempts** value in less that the time specified by the **Failed Login Time Threshold** (default is 15).

If an account is locked after the maximum failed login attempt limit has been reached, an **Admin** user can clear the account lock in the **Administrator Accounts** section by clicking **Clear Lockout** next to the user.

Administrator Roles

The following table lists a predefined set of roles provided by the Barracuda Load Balancer ADC. A predefined role cannot be modified or deleted. You can open a pop-up window with a detailed description of the access granted to a particular role by clicking **Details**. Each role is allowed to complete specific operations on the Barracuda Load Balancer ADC and is denied access to specific user interface screens. These predefined roles cannot be modified.

You can assign roles to users either by configuring an external authentication service (LDAP or RADIUS) or on an individual basis by configuring a local administrator. When a user attempts to log in, the Barracuda Load Balancer ADC first tries to authenticate the user credentials against configured local administrators, then queries the configured external authentication service. Once authenticated, the user inherits privileges from the associated role.

Role	Allowed Functions
Admin	The super administrator • All system operations **Note**: Only admins can assign roles
Service Manager	• Configuring services • Configuring security policies
Security Manager	• Configuring security policies

Network Manager	• IP configuration • IP operations (ping, telnet, TCP dump, etc) • Network troubleshooting
Reporting Manager	• Viewing and exporting logs • Scheduling and exporting reports
Guest	• View all configurations **Note**: Guest cannot modify the configuration

External Authentication Services

External administrators or users are part of an external authentication service like the Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial In User Service (RADIUS). The Barracuda Load Balancer ADC enables you to configure external authentication services, allowing authenticated external users to access the system. An external user cannot be created, but is synchronized internally from the LDAP or RADIUS server when the user is successfully authenticated with the configured directory services. You can override the default role association for an external user by editing the user.

Configure LDAP or RADIUS External Authentication Services

The Barracuda Load Balancer ADC can use both LDAP and RADIUS external authentication services to validate users attempting to login and administer the appliance. When a new user with valid credentials (as determined by checking the LDAP or RADIUS database) logs in, the Barracuda Load Balancer ADC also creates a local account for that user. This gives you additional flexibility with regards to these users in that you can alter their local account role independently of the configuration for LDAP or RADIUS external authentication service.

To configure an LDAP or RADIUS external authentication service, complete the following steps:

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **External Authentication Services** section, select **LDAP** or **RADIUS** from the drop down menu. The **Add LDAP Service** or **Add RADIUS Service** popup window opens.
3. Configure the external service as required. See the online help for details about each configuration option.
4. Assign a default role to all of the users associated with a specific LDAP or RADIUS service by selecting a role from the **Default Role** drop down menu.

If the administrator changes the default role, the new role is assigned to the associated LDAP or RADIUS users, unless a user's role is explicitly configured by the administrator in the **Administrator Accounts** section.

Add LDAP Service Group Mapping

You can assign users associated with a specific LDAP group to one of the predefined user roles on the Barracuda Load Balancer ADC. The LDAP users would gain access to the features and functionality associated with that role. Groups are evaluated based on the specified role priority (1 is the highest priority and 10 the lowest).

A user logging into the Barracuda Load Balancer ADC for the first time (the user has not yet been added to the user database) whose group on the LDAP server does not match any of the predefined roles on the Barracuda Load Balancer ADC is assigned the default role configured for the external LDAP server.

If you change the configuration for the default role of an external server, the role assignment for all the users of this external server is also changed.

For more information on roles, see Administrator Roles.

> If a user's role is mapped to one or more roles based on group mapping, the role with the higher priority is assigned to the user. If a user does not belong to any of the mapped groups, the user assumes the default role configured for the LDAP server.

Change the Default Role for an External User

When a default role is associated with the LDAP or RADIUS authentication service, all external users authenticated through the LDAP or RADIUS database are assigned to that role. For example, consider the default role, **Security Manager**, for the configured LDAP server. An external user authenticated through that LDAP database is assigned **Security Manager** role and can perform only security management tasks. The **Admin** user can change the default role assigned to a user if required.

To change the role assigned to a user:

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **Administrator Accounts** section, identify the desired user.
3. Click **Edit** next to the user. The **Edit Administrator Account** window appears.
4. Select a role for the user from the **Role** drop-down list.
5. Add an **Email Address** and click **Update**.

Administrator Accounts

You can specify local administrators on the Barracuda Load Balancer ADC. These users are authenticated internally by the appliance. The **Admin** user can create local users and associate each user with an administrator role. If you delete a local administrator account, that user is denied access to the system.

When evaluating any user logging in to Barracuda Load Balancer ADC, preference is given first to the local account, then LDAP, and then RADIUS. If the user's password does not match the password in the local account, no attempt is made to check if the user has a valid account on the LDAP or RADIUS server and a *password does not match* error is displayed.

If there are two or more users who share the same username, the user logging in first is considered the valid user who is populated in the administrator accounts. Other users with that username are considered invalid.

To add a local administrator, complete the following steps:

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **Administrator Accounts** section, click on **Add Local Administrator**.
3. Specify a **User Name**, **Password**, and **Email Address** to the new user.
4. Select a role for the new user from the **Role** drop down menu. For more information, see Administrator Roles.