Role-Based Administration

Introduction

Role Based Administration (RBA) restricts access to system resources based on the roles assigned to users within an organization. The Barracuda Web Application Firewall is shipped with predefined roles, each with distinct operational and configuration privileges. In addition to predefined roles, the Barracuda Web Application Firewall allows you to create custom roles and define access 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.

Roles and Privileges

Roles

A role is a set of privileges or permissions for the available system resources, created for a specific job function. The **admin** role is allowed to create, modify, and delete roles. A role can be assigned to multiple users within an organization. Assigning a role to a user confers the set of privileges for the system resources included in the role definition. All users who assume that role can operate in the same environment and access the same resources. For example, an administrator assigned to the **audit-admin** role is only allowed to view logs on the system and is prevented from accessing any other objects.

Predefined Roles

The following table lists a predefined set of roles provided by the Barracuda Web Application Firewall. A predefined role cannot be modified or deleted.

Role	Description of Allowed Functions Associated with Role
admin	The super-administrator • All system operations Note: Only admin can create and assign roles
audit-manager	• Viewing Logs
certificate-manager	• Uploading certificates • Creating certificates • Uploading Trusted certificates
service-manager	• Adding a server • Creating URL ACLs • Configuring website translation rules • Adding URL and parameter profiles • Configuring traffic management rules **Note**: service-manager can create/delete services, add/delete service-groups

policy-manager	• Managing default and customized security policies • Modifying security policies **Note**: policy-manager can create/delete security policies
network-manager	• Advanced IP address configuration • Configuring SNAT and ACL's • Network troubleshooting
monitoring-manager	• View logs • Configuring email notifications • Exporting system logs, application logs and FTP access logs • Generating and scheduling reports
guest	• View all configurations **Note**: guest may not modify the configuration

Create a New Role

In addition to the factory shipped roles, the Barracuda Web Application Firewall enables you to create new roles. You can specify the privileges for these roles, and then assign them to users.

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **Administrator Roles** section, click **Add Administrator Role**.
3. In the **Add Administrator Role** window, enter a role name and specify the permissions for the role.
4. Click **Create Role**.

For more information, refer to the online **Help**.

Privileges

A *privilege* is an access right or permission for a system resource. Privileges are used to control access to the system. You can grant privileges to a role, and then assign the role to one or more users. There are two distinct categories of privileges:

- Object Privileges
- Screen and Operation Privileges

Object Privileges

The following table lists the key configuration objects that are classified in role based administration:

Object	Description	Privileges
Services	Exhibits all services that are configured on the Barracuda Web Application Firewall.	**Read**: Enables the user to view the configuration of an object, but prohibits modifying the object. **Write**: Enables the user to view and modify the configuration of an object, but prohibits deleting the object. **Read All:** Enables the user to view and modify the configuration of all objects, but prohibits modifying objects. **Write All:** Enables the user to view and modify the configuration of all objects, but prohibits deleting the objects.
Security Policies	Exhibits all default and customized security policies.	
Authentication Services	Exhibits all authentication services such as Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial In User Service (RADIUS).	
API Privilege	Allows all the users having this role to access the Barracuda REST APIs.	

Screen and Operation Privileges

The Barracuda Web Application Firewall provides several distinct operations. These operations include tasks such as shutting down the system, changing the system time and date, backing up the system configuration, etc. You can grant permission to perform these operations to a role. A role can only execute operations for which it has permission, and is prevented from executing any other operation in the system. For example, when users are granted **appearance** operation permission, they can change the system name and reset the image used in the web interface.

To select an operation, ensure the corresponding secondary tab is selected in the **Web Interface Privileges** section. If you do not select the secondary tab, the corresponding operations become inaccessible. The **admin** user should determine the screens viewable by a user by selecting the secondary tabs.

Creating Users

Local Users

Local administrators or users are authenticated internally in the Barracuda Web Application Firewall. 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.

External Users

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 Web Application Firewall enables you to configure an external authentication service, 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.

Note: When an external user is no longer part of the LDAP or RADIUS database, the user must be manually deleted from the Barracuda Web Application Firewall so external authentication fails.

1. Go to the **ADVANCED > Admin Access Control** page.

2. To assign roles to local administrators:

    1. In the **Administrator Accounts** section, click **Add Local Administrator**.
    2. In the **Admin Access Control** window, enter the credentials, select the role, and enter the email address for the user.
    3. Click **Add**. The local user then appears in the table in the **Administrator Accounts** section.

3. To assign roles to external users:

    1. In the **External Authentication Services** section, select your external authentication service from the list.
    2. In the **Admin Access Control** window, enter the information for the authentication service and select the default role for users who are authenticated with the service.
    3. Click **Add**. The service then appears in the table in the **External Authentication Services** section.

Dual Authentication

Dual Authentication is supported in the Barracuda Web Application Firewall for enhanced security. It adds an additional layer of security to your basic log-in procedure. This can be enabled for all the administrators who manage the Barracuda Web Application Firewall.

You can enable Dual Authentication in **ADVANCED > Admin Access Control** page.

Before you enable Dual Authentication ensure that you have created two authentication services - an LDAP authentication service and a RADIUS or RSA SecurID authentication service.

1. Navigate to **ADVANCED > Admin Access Control** and in the **Administrator Account Settings** section, provide the following details.

2. **Dual Authentication -** When set to **Enable**, WAF verifies the credentials provided by the user on both LDAP and RADIUS server**.**

3. **Use RSA SecurID** - This field is displayed only when the dual authentication is enabled. When Use RSA SecurID is set to Yes, on the login page, you are presented with an additional **Passcode** field along with Username and Password. You must provide the RSA SecurID token together with PIN in this field. The admin/local users can leave this field blank when logging into WAF.

Assigning Roles to Users

Barracuda Web Application Firewall users are assigned roles which determine the operations they can perform. A user may be either *local* or *external*. Users must be assigned a role when the user account is created. The user can then access the system. When a user attempts to log in, the Barracuda Web Application Firewall 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.

Change the Default Role for External Users

When a default role is associated with the LDAP/RADIUS authentication service, all external users authenticated

through the LDAP/RADIUS database are assigned to that role. For example, consider the default role, **certificate-manager**, for the configured LDAP server. An external user authenticated through that LDAP database is assigned **certificate-manager** role and can perform only certificate 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 **External Authentication Services** 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. Modify Password and Email Address if required and click **Update**.

Admin Password Masking for the Barracuda Web Application Firewall Instances Deployed in Amazon Web Services (AWS)

By default, you can login to the Barracuda Web Application Firewall instance on Amazon Web Services using the following credentials:

Username*: admin*

Password*: AWS instance-ID*

If you want to enable Role Based Administration (RBA) to the Barracuda Web Application Firewall using a remote LDAP authentication service, you can use the backup based BYOL CloudFormation template. The backup based CFT includes the “maskAdminPassword” parameter that masks the admin password, and enables the admin user to login to the Barracuda Web Application Firewall using the LDAP password. If “maskAdminPassword” is enabled in the CFT and the Barracuda Web Application Firewall is bootstrapped, the local administrator cannot access the Barracuda Web Application Firewall with the default credentials (i.e. **Username**: *admin*, **Password**: *AWS instance ID*).

If the backup file does not include the LDAP configuration and maskAdminPassword is enabled in the CFT, the Barracuda Web Application Firewall becomes inaccessible. This is an irreversible activity. Therefore, ensure the backup file includes the LDAP server details configured in **External Authentication Services** in the **ADVANCED > Admin Access Control** page before enabling “maskAdminPassword” in the CFT.

You can mask the admin password and allow LDAP users to access the Barracuda Web Application Firewall web interface with their LDAP credentials (LDAP username and password). The Barracuda Web Application Firewall allows you to associate a LDAP group to a single role or multiple roles. Users belonging to the specified LDAP group name(s) gain privileges of the associated role to access the Barracuda Web Application Firewall web interface. For example, if a LDAP group is associated with the **audit-manager** role. The users of that group are allowed to view logs on the system and are prevented from accessing any other objects.

Currently, admin password masking can be achieved only when bootstrapping is performed using a backup stored in Amazon S3 bucket. See "**Backup Bootstrapping**" in the Bring-Your-Own-License (BYOL) Auto Scaling


article.

Mapping LDAP Groups with User Roles

You can map LDAP groups with user roles in the Barracuda Web Application Firewall. Users belonging to the specified LDAP groups gain privileges of the associated role to access the Barracuda Web Application Firewall web interface. You can map multiple groups to a single user role.

Steps to Configure LDAP Group Mapping

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **External Authentication Services** section, select **LDAP** from the drop-down list.
3. In the **Add LDAP Service** section, enter your LDAP server details.
4. In the **Role Association** section:Click **Save**.
    1. Set **Group Mapping** to **Yes**.
    2. Select a **Default Role** for the users who do not belong to any group specified in **Associated LDAP Groups**. If **Default Role** is set to **None**, users are not allowed to access the system.
    3. Specify the group name(s) in **Associated LDAP Groups** next to each **User Role** and set the priority. **Note**: Priority is applicable to a user ONLY when the user is a member of multiple groups in the LDAP server.

       If a user belongs to multiple groups in the LDAP server, and those groups are mapped to different roles, the user gains the privileges of the higher priority role. For example: Consider a user 'abc' belongs to group1, group2 and group3, where group1 is associated with the **Certificate Manager** role and priority set to 3, group2 is associated with the **Audit Manager** role and priority set to 1, and group3 is associated with the admin role and priority set to 2. In this case, the user 'abc' gains the **Audit Manager** role privileges to access the Barracuda Web Application Firewall web interface.

Configuration example to restrict users from a group for Open LDAP Directory and Active Directory

Group filter configuration to restrict users from a group for Open LDAP Directory:

- **Bind DN**: cn=administrator,cn=users,dc=example,dc=domain,dc=com
- **Bind Password**: password12
- **LDAP Search Base**: dc=example,dc=domain,dc=com
- **UID Attribute**: uid
- **Group Filter**: cn={groupname} or gidnumber={100}

- **Group Name Attribute**: cn
- **Group Member UID Attribute**: memberUid

Group filter configuration to restrict users from a group for Active Directory:

- **Bind DN**: cn=administrator,cn=users,dc=example,dc=domain,dc=com
- **Bind Password**: password12
- **LDAP Search Base**: dc=example,dc=domain,dc=com
- **UID Attribute**: sAMAccountName
- **Group Filter**: cn={groupname}
- **Group Name Attribute**: cn
- **Group Member UID Attribute**: member

RBA differences in UI vs API

1. For editing a sub-resource the user role needs
    1. **Write** permission on that sub-resource and at least a **Read** permission on it's object [via API]
    2. **Write** permission on that sub-resource and **Write** permission on it's object [via UI]
2. Any custom role should have at least **Read** permission on the service the role wants in order to view access or firewall logs, .
3. If a user is creating/adding/editing a new object from the UI, the user role needs to have the following.
    1. a **Write** access directly on that object
    2. accessibility (either **Read**/**Write**) to it's parent object
    3. a **Write Permission** on that tab/screen that the role is creating the object from.
4. Granting permissions to an object from the **Administrator-Roles** API, will automatically grant the same permission for the dependent screen(s) of that object and vice-versa. (when done from the UI).