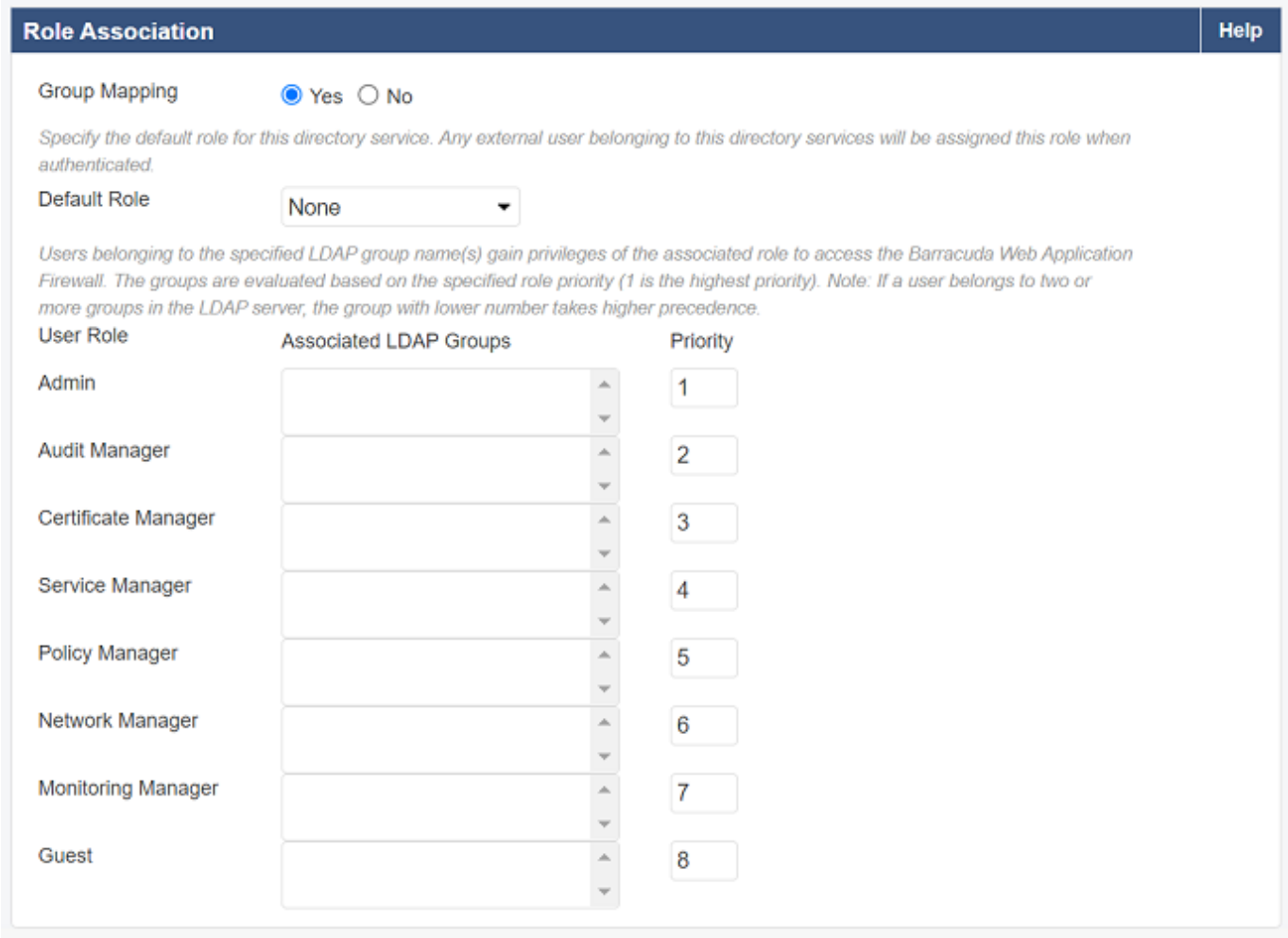
External Database Users

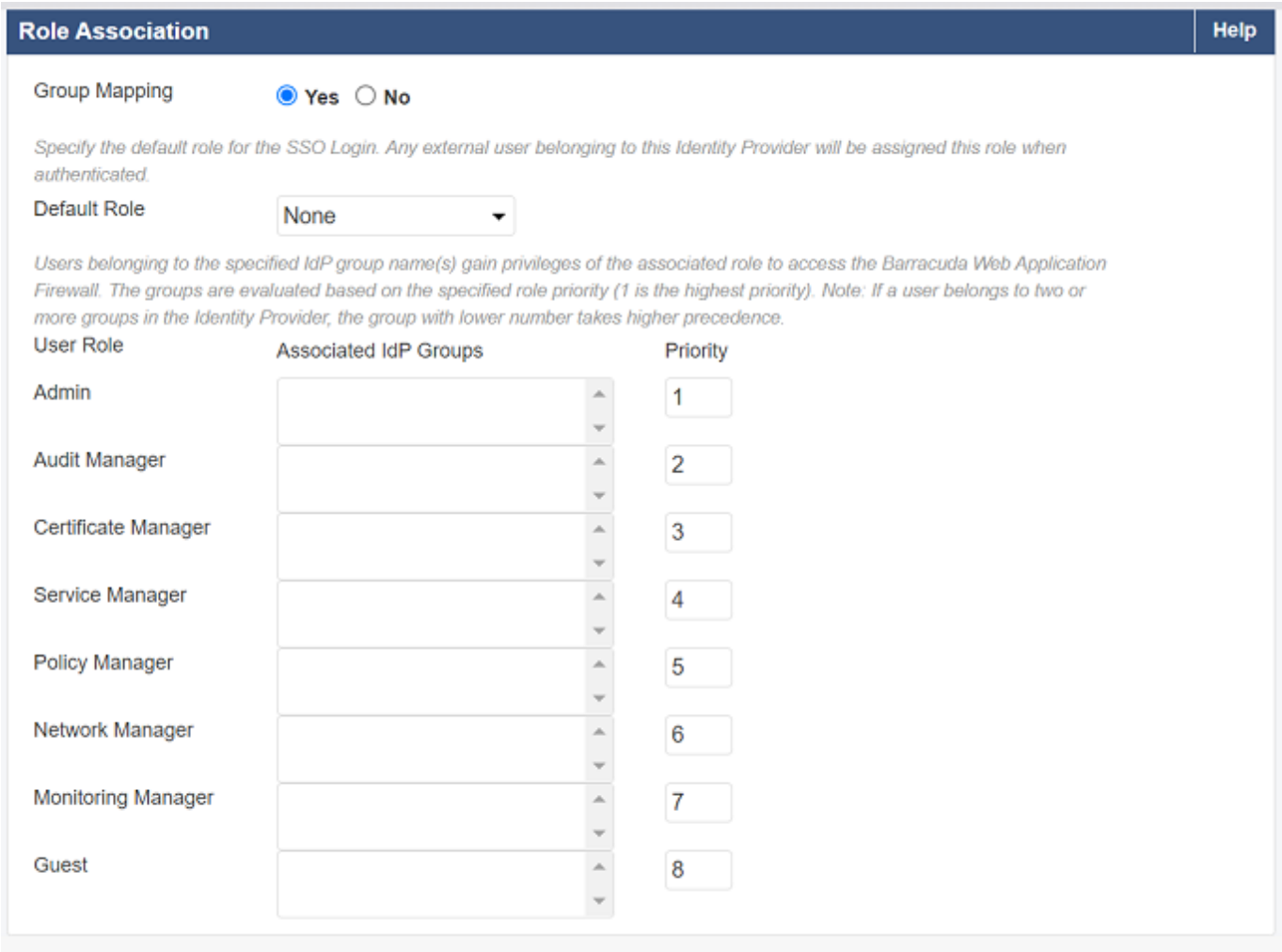
https://campus.barracuda.com/doc/95263131/

External administrators or users are part of an external authentication service like the Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), or Security Assertion Markup Language (SAML). 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, RADIUS, or SAML server when the user is successfully authenticated with the configured directory services. Users belonging to the specific LDAP group name(s) will obtain the privileges of the associated role to access the Barracuda Web Application Firewall. The groups are evaluated based on the specified role priority (1 is the highest priority).

Role Association for LDAP Groups:



Role Association for IdP Groups:



- If the user belongs to two or more groups in the LDAP server, the lower number always takes the highest precedence.
- When an external user is no longer part of the LDAP, RADIUS, or SAML database, the user must be manually deleted from the Barracuda Web Application Firewall so external authentication fails.

Assign Roles to External Users

1. Go to the **ADVANCED > Admin Access Control** page.
2. In the **External Authentication Services** section, select your external authentication service from the list.
3. 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.
4. Click **Add**. The created service gets displayed in the **External Authentication Services** section.

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 the Certificate-Manager role and can perform only certificate management tasks. The "Admin" user can change the default role assigned to a user if required.

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**.

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.

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

Figures