# Account Management

https://campus.barracuda.com/doc/54266624/

## User Management

A user can perform the following configurations:

- Create and Manage a Tag
- Add a User
- Assign a Role to the User
- Add a Group
- Configure LDAP
- View Audit Logs

## Creating and Managing Tags

Barracuda WAF Control Center enables you to create tags that groups different connected Barracuda WAF appliances into logical groups. Tags are created to organize all the connected appliances based on location, company, department, and so on. For example, If you want to group two or more WAF appliances based on their location, you can create a tag with the name "AUS-WAF" where "AUS" stands for "Australia".
Tags are added to connected appliances to easily identify and manage appliance groups. The tag groups can be viewed by appliance name and serial number or by tag name.

Tags display the tag groups by tag name. In this view, you can search for tags, add an existing tag, create a new tag, or delete a tag.

Associations display the tag groups by appliance serial number and name. In this view, you can search for tags, add an existing tag, create a new tag, or delete a tag.

#### Create New Tags and Associate them to an Appliance

1. Navigate to **ADVANCED>Tags** page.
2. From the **Tags** section, click the **Actions** drop-down list and then select **Create New Tag**.
3. In the **Create New Tag** dialog box, enter the following details.
    1. **Name** - Type a name for the tag.
    2. **Type** - Select Node to associate the tag to. Currently, Barracuda WCC supports only one Type-"Node" that indicates WAF NODES/SYSTEM.
    3. **Associations** - Select one or more appliances (WAFs) for which the tag is to be associated. Based on the selection of Type display, associations may vary accordingly.

4. Click **Save**.

#### Create New Tags for an Appliance

1. Navigate to **ADVANCED>Tags** page.
2. From the **Associations** section, under **Custom Tags**, click + for the appliance for which you want to add a tag.
3. From the **Select a Tag** drop-down list, click **Create New Tag.**
4. Type a name for the tag in the box provided next to the **Create New Tag** drop-down list, and then click **Add Tag**.

#### Rename Tags

1. Navigate to **ADVANCED>Tags** page.
2. From the **Actions** drop-down list, select **Change Name**. The **Rename Tag** dialog box is displayed.
3. In the **Tags Change Name** box, type a new name for the tag and then click **Save**.

## Adding a User

To create a new user, log into the Barracuda WAF Control Center web interface as the Barracuda WAF Control Center Account Admin, and then complete the following steps:

1. Click on the account admin name in the left pane.
2. Go to the **BASIC > User Management** page, and click **Add User**; the **Add User** page appears.
3. Enter the following details for the new user:
    1. **Email Address** – Enter the user's login email address.
    2. **Full Name** – Enter the user's first and last name.
    3. **Preferred Time Zone** – Select the default time zone used to display stats and report data for this user.
4. In the **User Permissions** section:
5. Assign permission to the user by selecting a role from the **User Role** drop-down list. The following options are available in the **User Role** list:
    1. **View Dashboard only** – User can view connected device statistics based on Access settings on the **BASIC > Dashboard** page.
    2. **View Reports**, **Logs**, and **Dashboard only** – User can view connected device statistics on the **BASIC > Dashboard** page, and track events such as login, connecting, or disconnecting specific devices by user, account, name, and date/time on the **BASIC >**

**Audit Log** page. You may wish to assign this role to a support person or office manager to provide performance and traffic reports for each product type.

3. **All Actions** – Use this role to create a Barracuda WAF Control Center administrator account; user can create users and assign permissions, connect/disconnect devices, view device Dashboard, and view tasks and task errors based on **Access** settings.
4. **Account Admin** – Use this role to create a Barracuda WAF Control Center account admin; user can configure and manage the Barracuda WAF Control Center, update security definitions, and view tasks and task errors. **Note**: See ***Permissions by Role*** for additional details on user roles.

6. After selecting the user role, all Barracuda Web Application Firewall devices connected to the Barracuda WAF Control Center gets displayed under the account admin name. Select the units to which the user needs to be granted permission. When a unit is selected, the user gains access to that unit, and granted permission selected in **User Role**. If the check box next to the account admin name is selected, the user gains access to all the Barracuda Web Application Firewall devices connected to the Barracuda WAF Control Center. Note that the **Account Admin** role always has access to all connected devices.
7. If you have defined user groups, you can select group membership for this user. Use the **BASIC > Group Management** page to set group permissions and specify unit access for each group. By using **Groups**, you can easily set the same permissions for multiple users without having to manage each user individually.
8. Configured LDAP user groups displays in the **LDAP Permissions** section.
9. Click **Add User** to add the new user. An email is sent to the user's email address with their login username and password. Once added, the user account displays in the **Users** table on the **BASIC> User Management** page.

Once logged into the Barracuda WAF Control Center, users can manage their own account information using the **BASIC > My Account** page.

#### Administrator Actions

Once you create a user, the user account details display in the **Users** table on the **BASIC > User Management** page. From this table, the **Account Admin** can perform the following actions:

- **Reset Password** – Resets the user's password; a new password is automatically generated and sent to the user's email address.
- **Edit User** – Modify the user's time zone, role, and device access.
- **Deactivate/Activate** – Suspend or restart a Barracuda WAF Control Center user account. Deactivated users can no longer log into the Barracuda WAF Control Center.

If you attempt to deactivate the last **Account Admin** on the account, a warning displays noting that by deactivating the only Account Admin you will deactivate the account for all users. If necessary, the Barracuda WAF Control Center Account Administrator can recover the account.

## Assigning a Role to the User

When you add new users, you assign a user role, which specifies their level of permissions. The following table lists permissions by role:

| Role | Permissions |
|---|---|
| **View Dashboard Only** | Users with this role can:<br>• View status including asset reports in the **BASIC > Dashboard** page.<br>• View existing reports in the **BASIC > Reports** page. The user cannot generate custom reports. |
| **View Reports, Logs and Dashboard Only** | Users with this role can:<br>• View status including asset reports in the **BASIC > Dashboard** page.<br>• View and generate reports in the **BASIC > Reports** page.<br>• View audit logs in the **BASIC > Audit Log** page. This page is unavailable if the system is in proxy mode.<br>• Generate reports in the **BASIC > Reports** page. This page is unavailable if the system is in proxy mode.<br>• View tasks and errors in the **BASIC > Task Manager** page. The user can also clear errors. |
| **All Actions** | Users with this role can:<br>• View status including asset reports in the **BASIC > Dashboard** page.<br>• View and generate reports in the **BASIC > Reports** page.<br>• View all certificates in the **BASIC > Certificates** page.<br>• Create, import, use, download, edit, and delete templates in the **BASIC > Templates** page.<br>• View and check updates in the **BASIC > Updates** page.<br>• Connect/disconnect devices, and resolve identifier conflicts in the **BASIC > Connect Products** page.<br>• Modify their password, update the time zone, and change the account information in the **BASIC > My Account** page.<br>• Configure Active Directory server details, test LDAP settings, and add user groups in the **BASIC > Configure LDAP** page.<br>• View audit logs in the **BASIC > Audit Log** page. This page is unavailable if the system is in proxy mode.<br>• Generate reports in the **BASIC > Reports** page. This page is unavailable if the system is in proxy mode.<br>• View tasks and errors in the **BASIC > Task Manager** page. The user can also clear errors. |

| | |
|---|---|
| **Account Admin** | Users with this role can:<br>• View status including asset reports in the **BASIC > Dashboard** page.<br>• View and generate reports in the **BASIC > Reports** page. This page is unavailable if the system is in proxy mode.<br>• View all certificates in the **BASIC > Certificates** page.<br>• Create, import, use, download, edit, and delete templates in the **BASIC > Templates** page.<br>• View and check updates in the **BASIC > Updates** page.<br>• Connect/disconnect devices, and resolve identifier conflicts in the **BASIC > Connect Products** page.<br>• Modify their password, update the time zone, and change the account information in the **BASIC > My Account** page.<br>• Add, edit, and delete users groups, and import LDAP users from a selected group for synchronization in the **BASIC > Group Management** page.<br>• Add, edit, and deactivate users on the account, reset user passwords, and import LDAP users from a selected group for synchronization in the **BASIC > User Management** page.<br>• Configure Active Directory server details, test LDAP settings, and add user groups in the **BASIC > Configure LDAP** page.<br>• View audit logs in the **BASIC > Audit Log** page. This page is unavailable if the system is in proxy mode.<br>• View tasks and errors in the **BASIC > Task Manager** page. The user can also clear errors. |

#### Effective Permissions

A user can be assigned different permissions in different groups, along with a different permission assigned to the same user under **User Management**. In such cases, the Barracuda WAF Control Center chooses the maximum permission role assigned to the user and grants access to the selected devices i.e., the lower level user role will be overridden by the higher-level user role. For example, consider a user is assigned:

- “View Dashboard Only” in ***Group1*** for the devices WAF1 and WAF2,
- “Account Admin” in ***Group2*** for the devices WAF2 and WAF3
- “View Reports, Logs and Dashboard Only” permission for the user in the **BASIC > User Management** page.  The devices selected for the user are WAF1 and WAF3.

Here:

- In WAF1, the user is assigned with “View Reports, Logs and Dashboard Only” role and “View Dashboard Only” role in ***Group1***. The maximum permission assigned to the user is “View Reports, Logs and Dashboard Only”, so the user gains access to WAF1 with View Reports, Logs and Dashboard Only permission.
- In WAF2, the user is assigned with “View Dashboard Only” and “Account Admin” roles in ***Group1*** and ***Group2*** respectively.  In this case, the “Account Admin” role is granted the maximum permission than the other role (“View Dashboard Only”), so the user gains access to

WAF2 with “Account Admin” permissions.
- In WAF3, the user is assigned with “View Reports, Logs and Dashboard Only” role and “Account Admin” role in ***Group2***. The Account Admin role is granted with the maximum permission than the other role (“View Reports, Logs and Dashboard Only”), so the user gains access to WAF2 with “Account Admin” permissions.

## Adding a Group

Use the **BASIC > Group Management** page to set group permissions and specify unit access for each group. By using **Groups**, you can easily set the same permissions for multiple users without having to manage each user individually. When you log in to the Barracuda WAF Control Center as the Barracuda WAF Control Center Account Admin, the **Groups** table on the **BASIC > Group Management** page displays details for all local and LDAP user groups for the account. Note that LDAP must be enabled on the **BASIC > Configure LDAP** page before you can create an LDAP user group.

To add a group, log into the Barracuda WAF Control Center web interface as the Barracuda WAF Control Center Account Admin, and then complete the following steps:

1. Click on the account admin name in the left pane.
2. Go to the **BASIC > Group Management** page, and click **Add Group**. The **Add Group** window appears.
3. In the **Add Group** section, do the following:
    1. Enter a name to identify the group in the **Group Name** field.
    2. From the **Role** drop-down list, select a permission for the group.
        1. **View Dashboard only** – Users can view connected device statistics based on Access settings on the **BASIC > Dashboard** page
        2. **View Reports**, **Logs**, and **Dashboard only** – Users can view connected device statistics on the **BASIC > Dashboard** page, and track events such as login, connecting, or disconnecting specific devices by user, account, name, and date/time on the **BASIC > Audit Log** page. You may wish to assign this role to a support person or office manager to provide performance and traffic reports for each product type.
        3. **All Actions** – Use this role to create a Group with Barracuda WAF Control Center administrator account permissions; users in this group can create users and assign permissions, connect devices, view device Dashboard, and view tasks and task errors based on **Access** settings.
        4. **Account Admin** – Use this role to create a Group with Barracuda WAF Control Center account admin permissions; users in this group can configure and manage the Barracuda WAF Control Center, update security definitions, view tasks and task errors. See **Permissions by Role** for additional details on selecting group roles.
4. The **Access** list displays all Barracuda Web Application Firewall devices currently connected to the Barracuda WAF Control Center by group. Select the units to which the group user(s) needs

to be granted permission. When a unit is selected, the user gains access to that unit, and granted permission selected in **Role**. If the check box next to the account admin name is selected, the user(s) gains access to all the Barracuda Web Application Firewall devices connected to the Barracuda WAF Control Center. Note that the **Account Admin** role always has access to all connected devices.

5. All users on the account display in the **Members** section. Select the members you wish to add to the group, and then click **Add Group**.

Once logged into the Barracuda WAF Control Center, users can manage their own account information using the **BASIC > My Account** page.

#### Administrator Actions

Once you create a group, the group details display in the **Groups** table on the **BASIC > Group Management** page. From this table, the **Account Admin** can perform the following actions:

- **Edit Group** – Modify the group role, device access, and members.
- **Delete Group** – Delete the group from the Barracuda Control Server.

## Configuring Lightweight Directory Access Protocol (LDAP)



## Understanding LDAP Authentication

The Barracuda WAF Control Center xxx supports Active Directory (AD) for role based access control. For additional information, log into the web interface as the Barracuda WAF Control Center Account Admin, and click Help on the **BASIC > Configure LDAP** page.

Use LDAP authentication to store and administer Barracuda WAF Control Center user accounts and verify user group membership via your organization's LDAP servers; you must have a verified domain to use LDAP. All users for the verified domain are required to use their LDAP credentials to access the Barracuda WAF Control Center.

Once LDAP authentication is set up and enabled, users added to Barracuda WAF Control Center by the Barracuda WAF Control Center Account Admin are automatically set up to use LDAP authentication, replacing the current user Barracuda WAF Control Center login credentials with their LDAP credentials. New users log in to the Barracuda WAF Control Center using their LDAP credentials and

follow the onscreen instructions to join the appropriate account.

You can add multiple email domains to a single LDAP profile. In scenarios where multiple companies are merged and each retain their email domain; the Barracuda WAF Control Center can work with multiple email domains.

## Configure the Active Directory Server

To configure the Barracuda WAF Control Center to use your AD server for authentication:

1. Log into Barracuda WAF Control Center as the Barracuda WAF Control Center Account Admin.
2. Click on the account admin name in the left pane.
3. Go to the **BASIC > Configure LDAP** page and do the following configuration in the **LDAP Configuration** section:
    1. Set **Enable LDAP** to *Yes*.
    2. In the **Server Alias** field, enter a short name or alias to identify the server.
    3. In the **Server Name/IP** field, enter the IP address or hostname of your Active Directory (AD) server.
    4. In the **LDAP Port** field, enter the port used by your Active Directory (AD) server; the default port number is 389. Ensure that you enter appropriate port number. Example: 636 for SSL port.
    5. In the **Bind DN (Username)** field, enter the distinguished name (DN) of a user in your LDAP directory that has read access to all users in LDAP.
    6. In the **Bind Password** field, enter the password associated with the username specified in the **Bind DN** field.
    7. In the **LDAP Search Base** field, enter the base distinguished name (DN) for the directory. For example, if your domain is test.com, your base DN might be *dc=test,dc=com*.
    8. In the **Username Attribute** field, enter he attribute that contains the user's ID. This is mapped to the mail attribute for use with AD LDAP environments.
    9. From the **LDAP Encryption** drop-down menu, select the type of encryption used by your Active Directory (AD) server.
    10. Click **Test LDAP** to test your LDAP configuration settings.
4. Click **Save** to save your LDAP settings.

## Creating a LDAP Group

To create a LDAP group, perform the following steps:

1. Log into Barracuda WAF Control Center as the Barracuda WAF Control Center Account Admin.
2. Click on the account admin name in the left pane.

3. Go to the **BASIC > Configure LDAP** page, and verify **Enable LDAP** is set to *Yes*.
4. Go to the **BASIC > Group Management** page, and click **Add Group**. The **Add Group** window appears.
5. In the **Add Group** section, select **LDAP**.
6. Click **LDAP Browser**, and navigate to and select the new LDAP user group.
7. Click **Add Group**.
8. In the **Groups** table, click **Edit Group**.
9. In the **Role** field, specify the level of permissions:
    1. **ViewDashboardOnly** – The users in this group can only view existing reports.
    2. **View Reports**, **Logs**, and **Dashboard Only** – The users in this group can create and view reports, and view logs and statistics.
    3. **All Actions** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
    4. **Account Admin** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
10. From the **Access** list, select the devices that the members of the group can access; you must select at least one device.
11. Click **Save**.

## Adding a Local User Group

To add a local user group, perform the following steps:

1. Log into Barracuda WAF Control Center as the Barracuda WAF Control Center Account Admin.
2. Click on the account admin name in the left pane.
3. Go to the **BASIC > Group Management** page, and click **Add Group**. The **Add Group** window appears.
4. In the **Add Group** section, select **Local**. The **Local User Group** section appears.
5. In the **Local User Group** section, specify values for the following:
    1. **Group Name** - Enter a name for the local user group.
    2. **Role** - specify the level of permissions:
        1. **ViewDashboardOnly** – The users in this group can only view existing reports.
        2. **View Reports**, **Logs**, and **Dashboard Only** – The users in this group can create and view reports, and view logs and statistics.
        3. **All Actions** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
        4. **Account Admin** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
    3. **Access** - select the devices that the members of the group can access; you must select at least one device.
    4. **Members** – Select the group members you want to add to the group.
6. Click **Add Group**.

## View Audit Logs

**Audit logs** are generated whenever users log in or log out of the web interface of the Barracuda WAF Control Center, except in a few rare cases. They are:

The **Login** action is not logged, when:

- Maintenance command is executed by a user or by the Barracuda WAF Control Center, a new login session will be created in maintenance mode, but it won't be logged.

The **Logout** action is not logged, when:

- The Barracuda WAF Control Center is restarted because critical processes have crashed, in which case the current existing sessions won't be logged out.
- The Maintenance command is executed by a user or by the Barracuda WAF Control Center, in which case the current existing sessions won't be logged out.

## Managing Connected Devices

You must have the following login rights to connect and disconnect the Barracuda Web Application Firewall devices to the Barracuda WAF Control Center:

- Barracuda WAF Control Center Account Admin login credentials; and
- Admin login credentials for each Barracuda Web Application Firewall you want to connect to, or disconnect from, the Barracuda WAF Control Center.

#### Connect a Device

To connect the Barracuda Web Application Firewall to the Barracuda WAF Control Center, refer to the steps mentioned in **Step 6 - How to Connect Devices to the Barracuda WAF Control Center**.

#### Disconnect a Device

To disconnect the Barracuda Web Application Firewall from the Barracuda WAF Control Center:

1. Log into the Barracuda WAF Control Center as the Barracuda WAF Control Center Account Admin, and go to the **BASIC> Connect Products** page.
2. In the **Connected Devices** section:
3. Identify the device you want to disconnect.
4. Click **Disconnect** next to the device under **Actions**. The **Remove Device** pop-up window

appears.
5. Click **Remove** to confirm.
6. The device no longer displays in the table or in the left pane.

## Task Manager

Use the **BASIC > Task Manager** page to monitor system tasks. This page provides a list of tasks that are in the process of being performed, and displays any errors encountered when performing these tasks.

If a task takes a long time to complete, you can click the **Cancel** link next to the task name and then run the task at a later time when the system is less busy. The **Task Errors** section lists an error until you manually remove it from the list; errors are not automatically phased out over time.