# Account Administrator Actions

https://campus.barracuda.com/doc/69960205/

Users with account administrator rights can take the following actions:

- Add, modify, or remove users on the account (**Home > Admin > Users**)
- Edit and View LDAP group members (**Home > Admin > Groups**)
- Set up LDAP Authentication to store and administer Barracuda Cloud Control user accounts via your organization's LDAP servers (**Home > Admin > Options**)
- Specify whether multi-factor authentication (MFA) is required for all users on the account (**Home > Admin > Options**)
- Select the default time zone for all users on the account (**Home > Admin > Options**)
- View all login activity and system modifications (**Home > Admin > Audit Log**)
- Purchase or start a free trial of Email Protection (**Home > Admin > Email Protection**)

## Add a User

You can use LDAP authentication to store and administer Barracuda Cloud Control user accounts via your organization's LDAP servers. Also see Understanding User Roles and Permissions.

> Before adding users to Barracuda Cloud Control via your organization's LDAP servers, verify that users are enabled, are members of the domain, and that the mail attribute is set for each user.

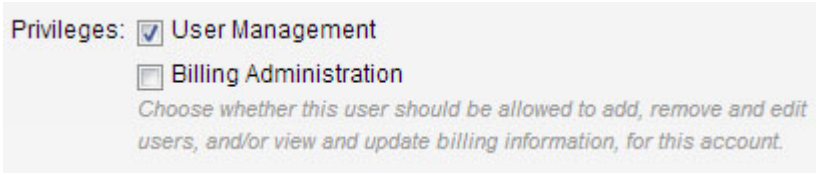
To create a new Barracuda Cloud Control user, the administrator must first add the user to your Barracuda Networks account, and set permissions for that user within the account. For that user, these permissions apply to all Barracuda Networks products and services connected to your Barracuda Networks account. You then create permissions for the user within Barracuda Cloud Control, defining whether the user can view and run reports, manage other Barracuda Cloud Control users, connect products through Barracuda Appliance Control, etc.

> To connect Barracuda Networks products through Barracuda Appliance Control, a user *must* have **User Management** privileges in Barracuda Cloud Control, and the account administrator must enable **Appliance Control** under **Product Entitlements** for that user.

## Add Users

To add a user to Barracuda Cloud Control,

1. Log into http://login.barracudanetworks.com/ as the account administrator.
2. Click **Home > Admin > Users**; the **Users** page displays.
3. Click **Add User**; the new user options display.
4. In the **User Details** section, enter the following details:
    1. **Name** – Enter the user's first and last name.
    2. **Email** – Enter the user's email address to be used as the login username. The user is sent an email to this address with instructions on configuring their password.
        > If your organization is using LDAP authentication to store and administer Barracuda Cloud Control user accounts via your organization's LDAP servers, users are required to use their LDAP credentials to access Barracuda Cloud Control.
    3. **Starting Page** – Select the page to display upon login.
5. Use the **Multi-Factor Authentication** section to manage MFA settings. For details, refer to Multi-Factor Authentication in Barracuda Cloud Control.
6. Select user **Privileges**:
    1. **User Management** – User can add, remove, and edit user accounts.
    2. **Billing Administration** – User can update account billing information.




## Add Product Entitlements

1. In the **Product Entitlements** list, turn on the subscribed to Barracuda Networks products and services that this user can access when they log into the account.
    > **Product Entitlements**
    > For details on setting Barracuda Backup permissions, refer to the section *Barracuda Backup Permissions* below. For details on setting Barracuda Appliance Control permissions, refer to the section *Barracuda Appliance Control Permissions* below.
    > See also: Understanding Entitlement Permissions and Roles.
2. Click **Save User**. If you selected **Backup** or **Appliance Control** in the **Product Entitlements** list, you can now configure permissions using the instructions below.

#### Configure Barracuda Appliance Control Permissions

1. Click the user's name in the **Users** table, and then click **Configure Permissions** directly below

**Appliance Control**:


2. The **BASIC > User Management** page displays in the **Barracuda Appliance Control** web interface. The **Users** table displays user details.

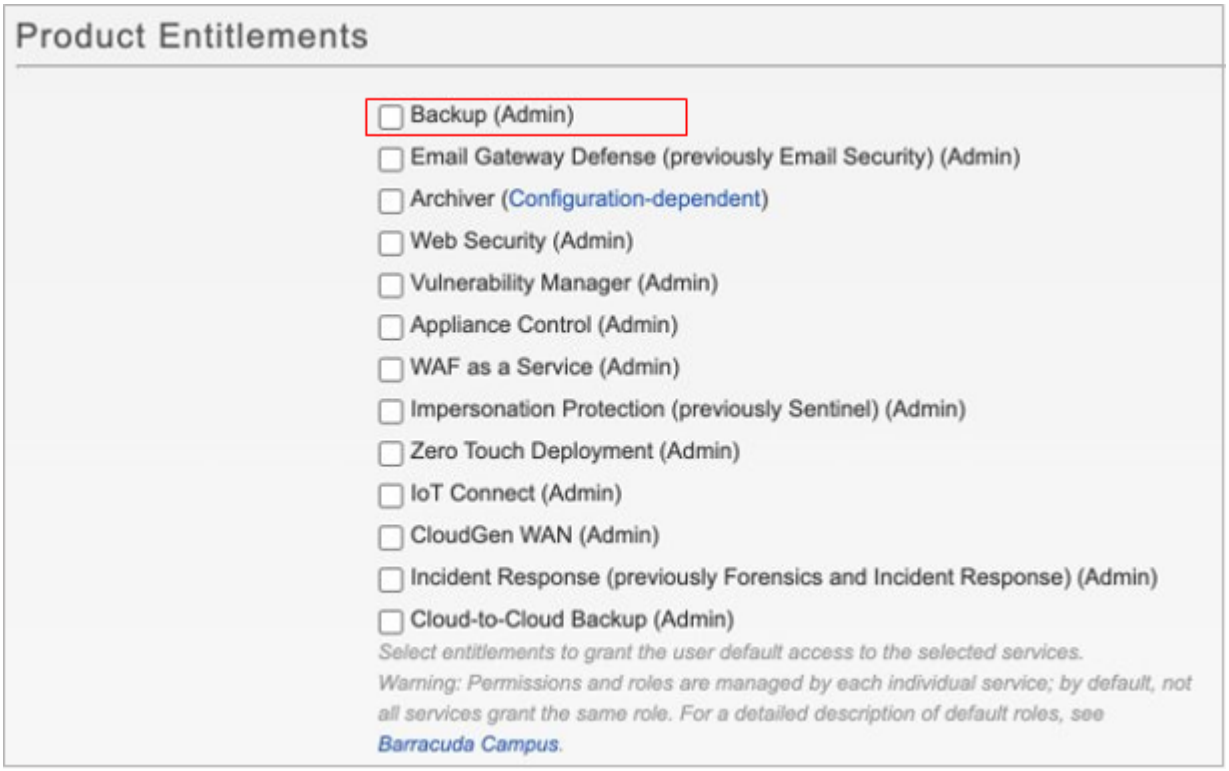
   If you granted a user **User Management** permissions in Barracuda Cloud Control, the **User Role** displays as **Account Admin**, otherwise, the **User Role** displays as **No Permissions**.

3. Click **Edit User** in the **Administrator Actions** column for the new user. The **Edit User** page displays.
4. Select the **Preferred Time Zone** to display all data viewed by the account. All statistics and report data viewed by the user are converted into the selected time zone.
5. From the **User Role** drop-down menu, select the level of permissions for the user.
6. Select one or more connected devices to which the user has access.
7. Use the **Group Permissions** section to add the user to a group and automatically set permissions based on the group settings.

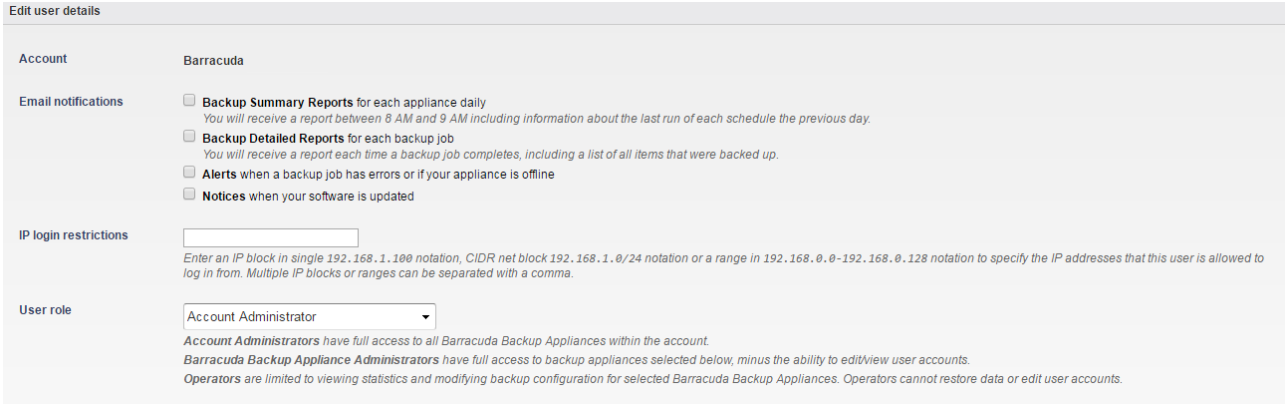
   If you are using LDAP authentication, use **LDAP Permissions** to select LDAP user groups.
8. The **Effective Permissions** display the effective user permissions based on both the selected **User Permissions** (role and device access) and **Group Permissions**.
9. Click **Save** to set the user's Barracuda Appliance Control permissions.

#### Configure Barracuda Backup Permissions

1. Click the user's name in the **Users** table, and then click **Configure Permissions** directly below **Backup**:




2. When you click **Configure Permissions** directly below **Backup**, you can set the following options:




3. **Barracuda Email Notifications**:
    1. **Backup Summary Reports for each appliance daily** – When turned on, a report is sent to this user each day between 8-9am.
    2. **Backup Detailed Reports for each backup job** – When turned on, a report is sent to this user each time a backup job completes.
    3. **Alerts** – When turned on, an alert is sent to this user if an error occurs during a backup job or if the Barracuda Backup Server goes offline.
    4. **Notices** – when turned on, a notice is sent to this user when the Barracuda Backup Server software is updated.
4. **IP login restrictions** – If you want to restrict the IP address from which this user is allowed to log in, enter a value or range of values here.
5. **User Role**:
    1. **Account Administrator** – User has full access to all Barracuda Backup Servers within

the account.
2. **Barracuda Backup Appliance Administrator** – Select the Barracuda Backup appliances to which the user has access based on their permissions. Select Select All Backup Appliances to grant user access to all Barracuda Backup Appliances attached to the account based on their permissions.
3. **Operator** – User can view statistics and modify backup configuration for Barracuda Backup Appliances selected in the Barracuda Backup Appliance Permissions section.

6. **Grant access to** – Select backup appliances this user can access. Select all or a subset of available appliances.
7. Click **Save**.

## Modify a User

To modify a user's account:

1. Log into https://login.barracudanetworks.com/ as the account administrator.
2. Click **Home > Users** ; the **Users** page displays.
3. Click on a username in the table; the **User Details** pane displays where you can modify:
   1. **Name** – Update the name to identify this user.
   2. **Password** – Click to send the user an email with instructions to update their password; you cannot modify the password in this way if you are using LDAP authentication.
   3. **Starting Page** – Select the product or page to display when the user signs in.
4. Multi-Factor Authentication (MFA) options are based on whether MFA is required for all users on the Barracuda Cloud Control account. For more information, see How to Set Up and Manage Multi-Factor Authentication in Barracuda Cloud Control.
5. Change user access **Privileges**; for more information, refer to Understanding User Roles and Permissions.
6. Use the **Product Entitlements** section to change the subscribed to Barracuda Networks products and services that this user can access when they log into the account.
7. Click **Save User** to update the user's account.

## Remove a User

**Warning!**

You must have at least one user attached to an account. Once the last user is removed, the *account is permanently unavailable*.

Removing a user does not disable the user or delete them from Barracuda Networks' authentication back end. The user's entitlements and privileges on the account are removed, and they no longer have access to any products or services on the account from which they were removed. The next time that user logs in, they are prompted to create or join an existing company account. Note that the account admin can deny a join request.

Note: To strictly control user access, consider integrating your company's LDAP authentication with Barracuda Cloud Control. Refer to LDAP Active Directory and Azure Active Directory for details.

To remove a user:

1. Log into https://login.barracudanetworks.com/ as the account administrator.
2. Click **Home > Users** ; the **Users** page displays.
3. Click on the username you want to remove from the account.
4. In the right pane, click **Remove User**.


5. Click **OK** to confirm that you want to remove the user from the account; the user name is removed from the **Users** list.

## Figures