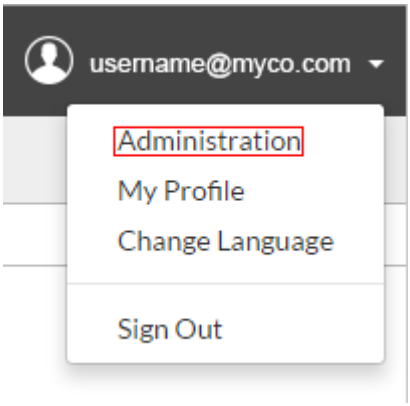
Barracuda Account Administration

https://campus.barracuda.com/doc/69960209/

To access Account Administration:

1. Log into https://login.barracudanetworks.com/ using your administrator credentials.
2. Click the Admin icon (Admin) or, in the top right corner, click the down arrow next to your user name, and click **Administration**:



3. The **Admin** page displays. From here, you can view these tabs, which are described in sections below:

- **Users** and **Groups** tabs – Manage users and LDAP groups;
- **Options** tab – Configure LDAP authentication, multi-factor authentication, and set the default time zone for all users on the account;
- **Audit Log** tab – View user login activity and system modifications;
- **Email Protection** tab – Purchase or start a free Email Protection trial.

Manage Users

Go to the **Home > Admin > Users** page to manage user information and set product entitlements.

For more information on managing users, refer to the following articles:

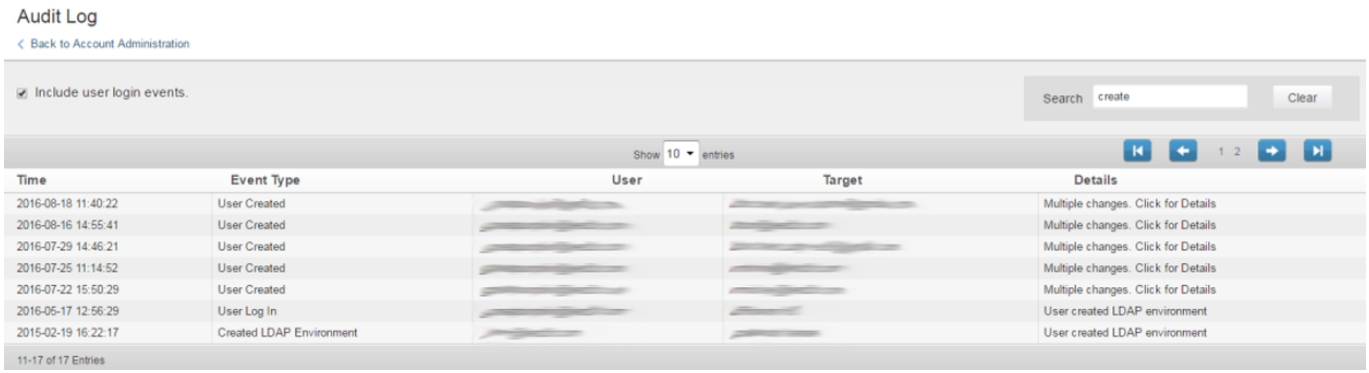
- Understanding User Roles and Permissions
- How to Add Users and Configure Product Entitlements and Permissions
- Understanding LDAP Authentication
- LDAP Active Directory and Azure Active Directory
- How to Modify or Remove Users

Groups

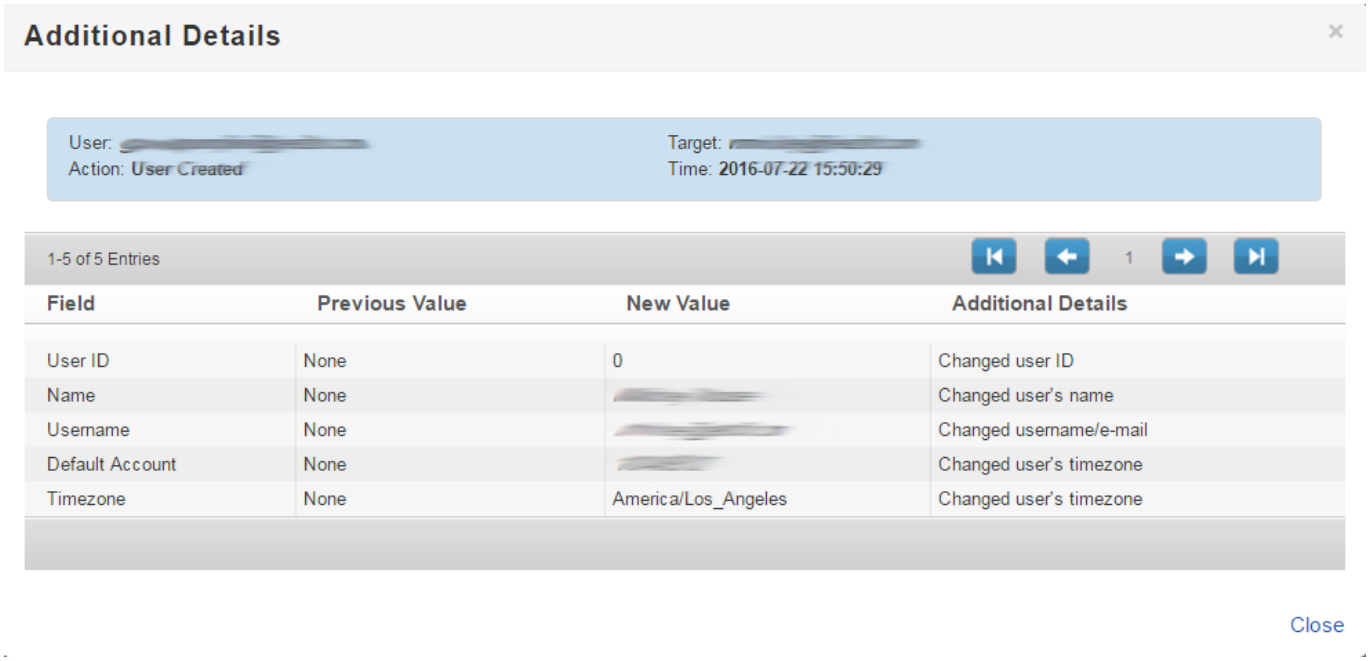
Go to the **Home > Admin > Groups** page to view and manage your LDAP groups. Note that you must enable LDAP authentication before you can view and manage Groups. Refer to LDAP Active Directory and Azure Active Directory and Understanding LDAP Authentication.

Audit Log

Go to the **Home > Admin > Audit Log** page to view all user activity in the system. Scroll through the table to view activity, or enter a search term in the **Search** field to view all matching items. Note that the table updates dynamically as you type. The audit log includes event time, type, the user and target user, and a description of the event. For example, if you are looking for details of when the LDAP environment was created on your account, begin typing in the **Search** field to populate the table:



Click in the **Details** field for any additional details for the selected activity:



Options

Use the **Home > Admin > Options** page to configure account security and authentication:

LDAP Authentication

Use LDAP authentication to store and administer Barracuda Cloud Control user accounts via your organization's LDAP servers; note that you must have a verified domain to use LDAP. All users for the verified domain are required to use their LDAP credentials to access Barracuda Cloud Control. For details refer to the following articles:

- Understanding LDAP Authentication
- LDAP Active Directory and Azure Active Directory

Multi-Factor Authentication

Multi-factor authentication (MFA), also known as two-factor authentication, is a security feature that requires two forms of authentication to access Barracuda Cloud Control. When enabled, MFA provides an extra layer of security to your account. Even if the user's login credentials are stolen, without the trusted device, the attacker is unable to access the account. And if the user's device is taken, the attacker cannot access the account without the login credentials. For details refer to the following articles:

- Understanding Multi-Factor Authentication in Barracuda Cloud Control
- How to Set Up and Manage Multi-Factor Authentication in Barracuda Cloud Control

- How to Add Multi-Factor Authentication Devices in Barracuda Cloud Control
- How to Remove Multi-Factor Authentication Devices from Barracuda Cloud Control

Time Zone Details

Select the default time zone for all users in your account from the **Time Zone** drop-down menu, and then click **Save**.

Figures