How to Manage User Accounts and Roles

https://campus.barracuda.com/doc/75694399/

Watch the User Management video:

User Accounts

There are two types of accounts on the Barracuda Cloud Archiving Service:

- **Local Accounts** – These accounts reside only on the Barracuda Cloud Archiving Service and are created from the **Users > User Add/Update** page in the administration interface.
- **Active Directory Accounts** – Add users through Active Directory authentication and associate a role and whose mail can be viewed with an AD user or group. Once LDAP or Azure AD is configured on the Barracuda Cloud Archiving Service, users can log in using their regular network credentials to view and create flags for messages in their personal archive.

Roles

Local accounts are created with one of the following roles:

- **User** – Able only to view messages accessible to the account, either because the username for the account is also that of the sender or recipient of a message, or because it has been given explicit access to view an email address via Alias Linking.
- **Auditor**– Able to create and activate policies, and view, search, and export any messages to/from the domains to which they have access. Additionally, Auditors can save and name an Advanced search for re-execution at a later time from the Saved Searches tab. To create a "Domain Auditor" (an auditor with access to only a subset of the domains on your Barracuda Cloud Archiving Service), set the role to Auditor and specify at least one domain. If no domains are specified, then all messages in the entire Barracuda Cloud Archiving Service are accessible. No auditor account has access to any system or network configuration information on the

Barracuda Cloud Archiving Service.

- **Admin** – Able to view all items from any user, not just those listed for the account. Also able to create and activate policies, and can make other system or network changes.

The assigned role can be changed at a later date from the **Users > Accounts** page, but only the last assigned role is active.

Add Local Users

Use the following steps to manually create or update a user account:

1. Go to the **Users > User Add/Update** page.
2. Enter the user's **Email Address** and enter the **User Display Name**.
3. If you have configured users via active directory, click **Populate** to retrieve all aliases associated with LDAP or Azure AD for the entered email address.
4. Enter the account password and select the user role for the account.
5. If you select the user role **Auditor** enter the following additional details:
    - Enter a domain for which the auditor can view messages and other Outlook items, and click **Add.** Any messages that includes an email address in the listed domains in either the **From**, **To**, or **CC/Bcc** fields, or any items that belong to a user in the specified domains, display in search results. To allow the auditor to view all items from all domains, leave this field blank.
    - In the **Saved Search** drop-down menu, select a defined Saved-Search to automatically apply to all searches performed by this auditor. Note that the parameters in the Saved Search take precedence over any domain limitations that may be specified above, as well as over any attempts by the auditor to *Search As* any other account.

Add Users through Active Directory Authentication

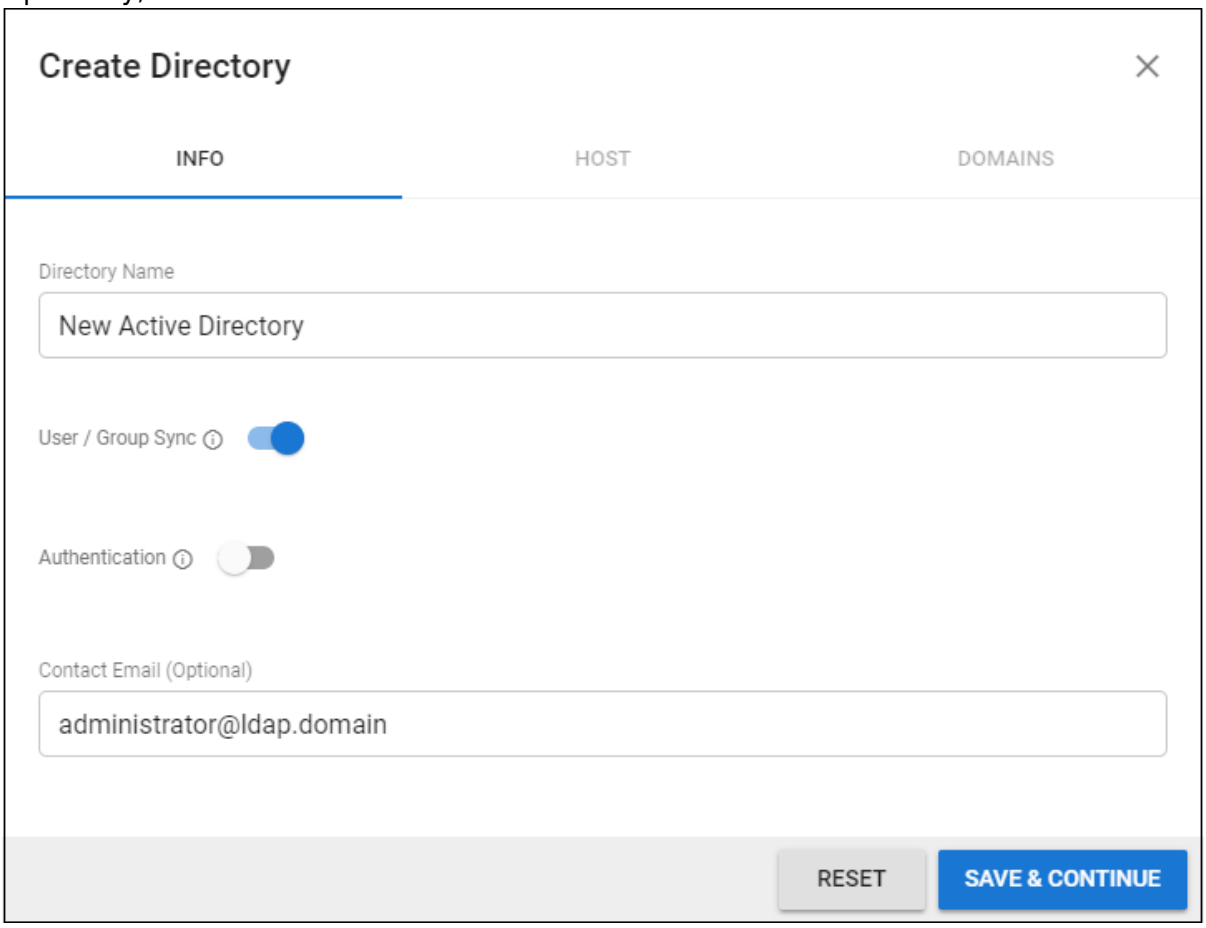
Add LDAP Active Directory

Use the following steps to set up Barracuda Cloud Control LDAP authentication:

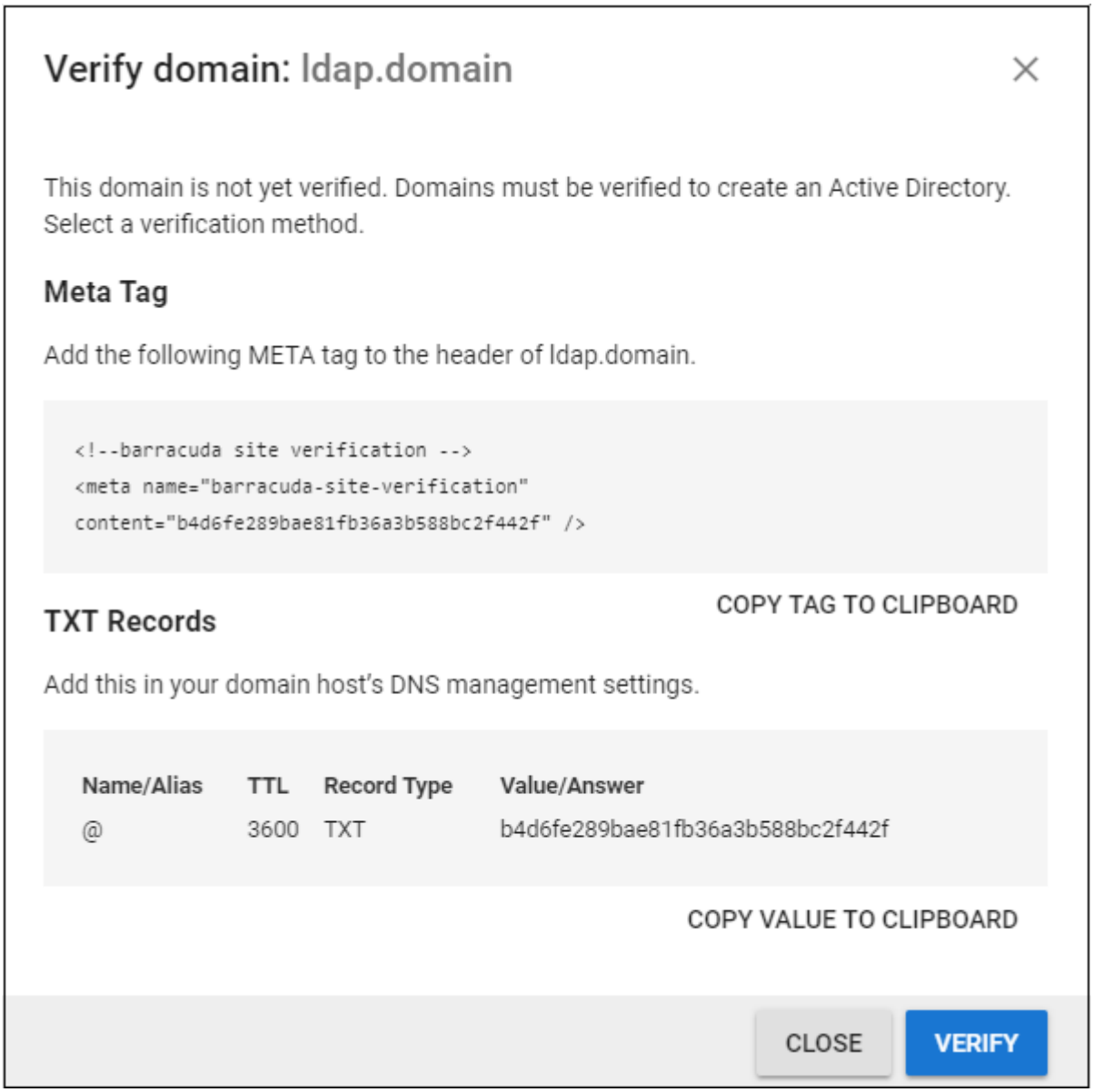
1. Log in to https://login.barracudanetworks.com/ as the account administrator, and go to **Admin > Directories**.
2. Click **Add Directory > LDAP Active Directory**; the **Create Directory** wizard displays. In the **Info** page, specify the following details:
    1. Enter a name to represent the directory in the **Directory Name** field.
    2. Toggle **User / Group Sync** to **On** to synchronize with AD.
    3. Toggle **Authenticate** to **On** to allow users to authenticate using their LDAP AD

credentials. When toggled **Off**, users must authenticate using their Barracuda Cloud Control credentials.

4. Optionally, enter the administrator contact email address:



3. Click **Save & Continue**.
4. In the **Host** page, enter the following details for your LDAP host:
    1. **LDAP Host IP address**
    2. **LDAP Host Port**
    3. **Base domain name**
    4. **Username**
    5. **Password**
    6. Select the **Connection Security** as **STARTTLS**, **LDAPS**, or **None**.
5. Click **Add Domain**; the domain is added to the **Domains** field. Click **Verify**.
6. Click **Test** to verify connectivity. If the connection is successful, **Connected** displays. If the connection fails, verify the entered LDAP host details. Click **Continue.**
7. In the **Domains** page, click **Add domain** to add the domain to the AD configuration. Complete this step for each domain you want to add.
8. To verify you own the domains you plan to include in your AD configuration, select the manner in which to verify the domains:
    - Copy a META tag to your domain header, *or*
    - Add a TXT record to your host's DNS management settings



9. Click **Verify**. Once the domain is verified, it is added to the **Directories** table in the **Admin > Directories** page in Barracuda Cloud Control.

Add Azure Active Directory

See also: Azure AD with Active Directory Federation Services

Use the following steps to set up Barracuda Cloud Control Azure AD authentication:

1. Log in to https://login.barracudanetworks.com/ as the account administrator, and go to **Admin > Directories**.
2. Click **Add Directory > Azure Active Directory**; the **Create Directory** wizard displays. In the **Info** page, enter a name to represent the directory in the **Directory Name** field.

3. Click **Connect to Microsoft** to sign in to Microsoft and authorize Barracuda Cloud Control to connect to your Azure AD account.
4. Once authorization is complete, toggle **User / Group Sync** to **On** to synchronize with Azure AD.
5. Toggle **Authenticate** to **On** to allow users to authenticate using their Azure AD credentials. When toggled **Off**, users must authenticate using their Barracuda Cloud Control credentials.
6. Optionally, enter the administrator contact email address. Click **Save & Continue**.
7. Once verification is complete, your Azure AD domains display in the wizard. Click **Done**.

Edit Users

Use the following steps to modify user settings:

1. Go to the **Users > Accounts** page:
    1. Click **Delete** to remove an account.
    2. Click **Edit** to modify the user; the **Users > User Account Create/Update** page displays.
2. Update the user settings, and click **Save Changes**.

Figures