

Step 2 - Configure Directory Services

<https://campus.barracuda.com/doc/46891774/>

Google Directory Service integration is currently not supported for Barracuda Cloud Archiving Service.

You must configure LDAP or Azure AD for group expansion and user attributes in the Barracuda Cloud Archiving Service.

Active Directory Limitations

Barracuda Networks does not support using default AD groups, such as Domain Users, when applying entitlements for user access. Due to limitations within AD, these groups may not contain all users or any users at all.

Verify User Status

Before adding users to the Barracuda Cloud Archiving Service 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.

Incoming Connections

To ensure uninterrupted access to LDAP server from the Barracuda Cloud, you must allow incoming connections from the following IP ranges:

- 209.222.80.0/21
- 64.235.144.0/20
- 35.170.131.81
- 54.156.244.63
- 54.209.169.44

Secure LDAP


Barracuda Networks recommends connecting your LDAP connection using SSL (LDAPS). As the information will be transmitted between Barracuda Networks' cloud servers and your Cloud email service, you must ensure that the connection is secure. Contact your IT Administrator if you need help setting up LDAPS in your network.

Use AD authentication to store and administer Barracuda Cloud Archiving Service user accounts via your organization's LDAP or Azure AD.

When you first set up the Barracuda Cloud Archiving Service, a warning notice displays across the top of the web interface notifying you that you must configure AD through Barracuda Cloud Control and enable groups. Before you continue, you are **required** to either set up AD and wait for a sync to

complete, or select to proceed without AD. Barracuda Networks strongly recommends setting up local AD.

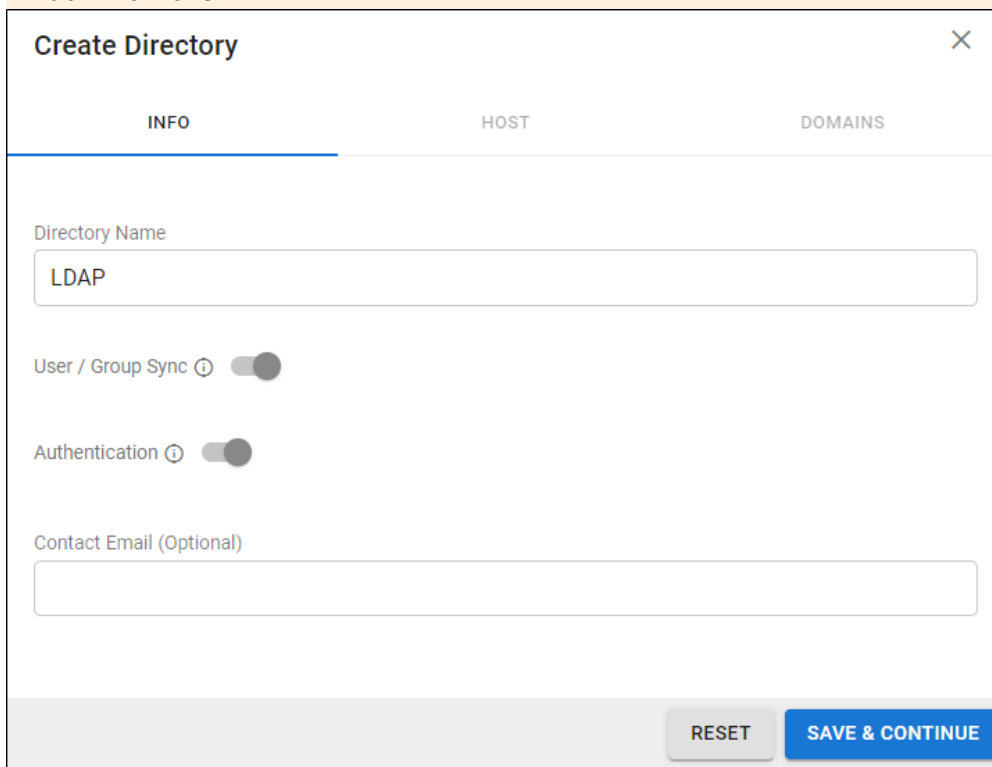
Create a Barracuda Cloud Control Directory

1. Log into <https://login.barracudanetworks.com/> as the account administrator, and go to **Home > Admin > Directories**.
2. Click the **Add Directory** button.

3. Select one of the following sections to add a new LDAP or Azure active directory.

Add a New LDAP Active Directory

1. Select **LDAP Active Directory**.
2. On the **INFO** tab, specify a new **Directory Name**.
3. Activate the **Authentication** option to have users authenticate using their LDAP credentials. If you disable this option, users authenticate with Barracuda Cloud Control.

Barracuda Networks strongly recommends creating an additional administrator account using an independent domain that does not use Active Directory (AD) authentication. This allows you access to your Barracuda Networks product account if your AD server goes down or fails.



The 'Create Directory' dialog box is shown with the 'INFO' tab selected. It contains the following fields and controls:

- Directory Name:** A text input field containing 'LDAP'.
- User / Group Sync:** A toggle switch that is currently turned on.
- Authentication:** A toggle switch that is currently turned on.
- Contact Email (Optional):** An empty text input field.
- Buttons:** 'RESET' and 'SAVE & CONTINUE' buttons at the bottom right.

4. Click **SAVE AND CONTINUE**.
5. On the **HOST** tab, specify the following for the LDAP host:
 - **LDAP Host IP address**
 - **LDAP Host Port** – Use Port **389** for LDAP and LDAPTLS or Port **636** for LDAPS.
 - **Base Domain Name (DN)** – Any user or group that exists with the search base that will sync to Barracuda Networks. For example, DC=domain,DC=com.
 - **Bind DN** – Enter the bind domain name for a service account with read permissions to the active directory.
 - **Password** – Password associated with the service account.
 - **Connection Security** – Select **SSL**, **TLS**, or **None**. For more information, see [New Requirements for LDAP Authentication](#).
6. (Optional) To add additional servers, click **Add LDAP Host**.
7. If your LDAP server uses a self-signed certificate, toggle on the **Allow Self-Signed Certificate** setting.
8. Click **TEST CONNECTION** to check connectivity to the host. If the connection fails, verify your settings are correct and that you have allowed the Barracuda Networks IP in your firewall. Contact [Barracuda Networks Technical Support](#) for additional troubleshooting.
9. If the connection succeeds, it displays as Connected. Click **SAVE AND CONTINUE**.

Create Directory: LDAP

✓ INFO

HOST

DOMAINS

Host

127.0.0.1

Port

389

Add LDAP Host

Base DN

dc=domain,dc=com

Bind DN

CN=ldap,OU=Service Accounts,OU=Users,DC=domain,DC=com

Password

.....

Connection Security

☐ SSL ☐ TLS ☒ None

☐ Allow Self-Signed Certificate

TEST CONNECTION

BACK

RESET

SAVE & CONTINUE

10. On the **DOMAINS** tab, add the domains associated with your users.
11. For each domain that you add, click **Verify** and following the instructions to verify the domain.

Verify domain: domain.org ✕

This domain is not yet verified. Domains must be verified to create an Active Directory. Select a verification method.

Meta Tag

Add the following META tag to the header of domain.org.

```
<!--barracuda site verification -->
<meta name="barracuda-site-verification"
content="d1b49df076ab989d77d1caf052a2567c" />
```

COPY TAG TO CLIPBOARD

TXT Records

Add this in your domain host's DNS management settings.

Name/Alias	TTL	Record Type	Value/Answer
@	3600	TXT	d1b49df076ab989d77d1caf052a2567c

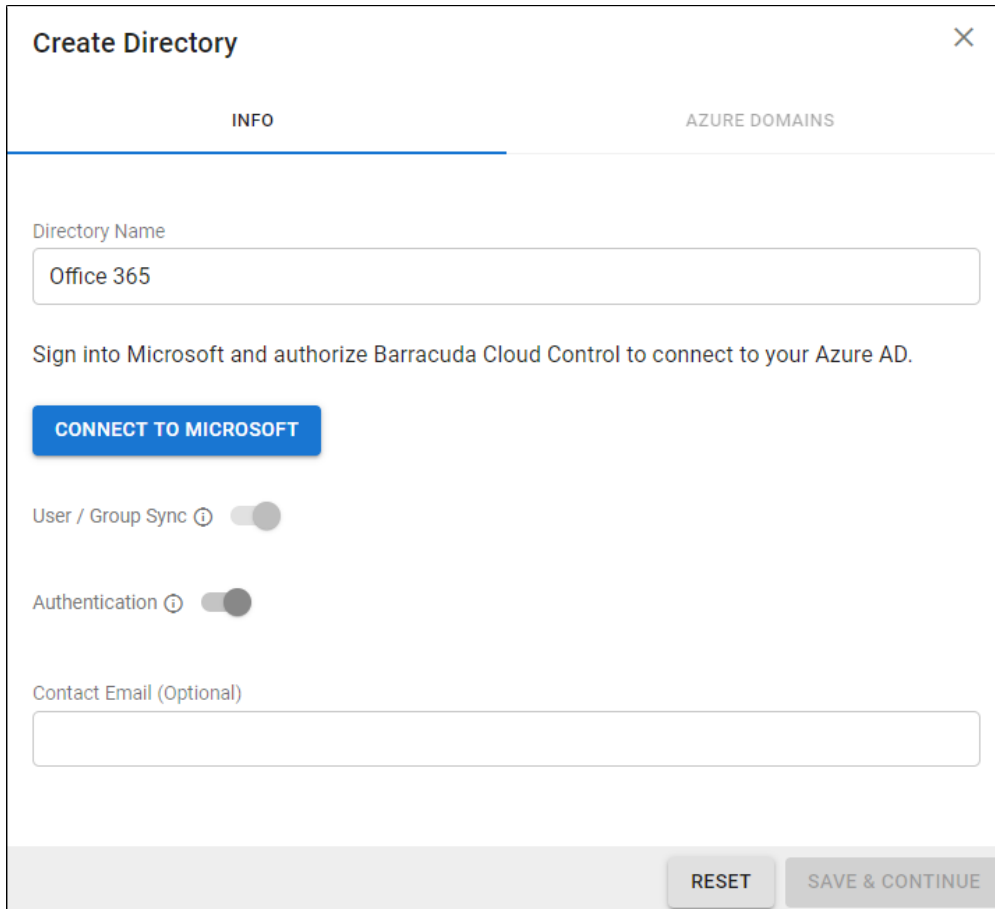
COPY VALUE TO CLIPBOARD

CLOSE VERIFY

12. After each domain is verified, you can sync your users and groups to the Barracuda Cloud Control.

Add a New Azure Active Directory

1. Select **Azure Active Directory**.
2. On the **INFO** tab, specify a new **Directory Name**. For example, "Office 365".
3. Click **CONNECT TO MICROSOFT** to sign into Microsoft and authorize Barracuda Cloud Control to connect to your Azure Active Directory account.
 1. Log in with your Microsoft 365 administrator credentials.
 2. Accept the credentials for the application request.



4. Activate the **Authentication** option to have users authenticate using their Azure credentials. If you disable this option, users authenticate with Barracuda Cloud Control.

Barracuda Networks strongly recommends creating an additional administrator account using an independent domain that does not use Active Directory (AD) authentication. This allows you access to your Barracuda Networks product account if your AD server goes down or fails.

5. After you are redirected back to the Barracuda Cloud Control, click **Save**.

For end-user authentication, refer to [How to Set Up Active Directory Groups for End-User Authentication](#).

Continue with [Step 3 - Launch the Initial Setup Wizard](#) .

Figures

1. addLdap.jpg
2. addLdapInfo.png
3. addLdapHost.png
4. verifyLdapDomain.png
5. addAzureInfo.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.