

LDAP Active Directory and Azure Active Directory

<https://campus.barracuda.com/doc/76284893/>

You can configure Barracuda Cloud Control to synchronize users with LDAP Active Directory or Azure Active Directory as described in the sections that follow.

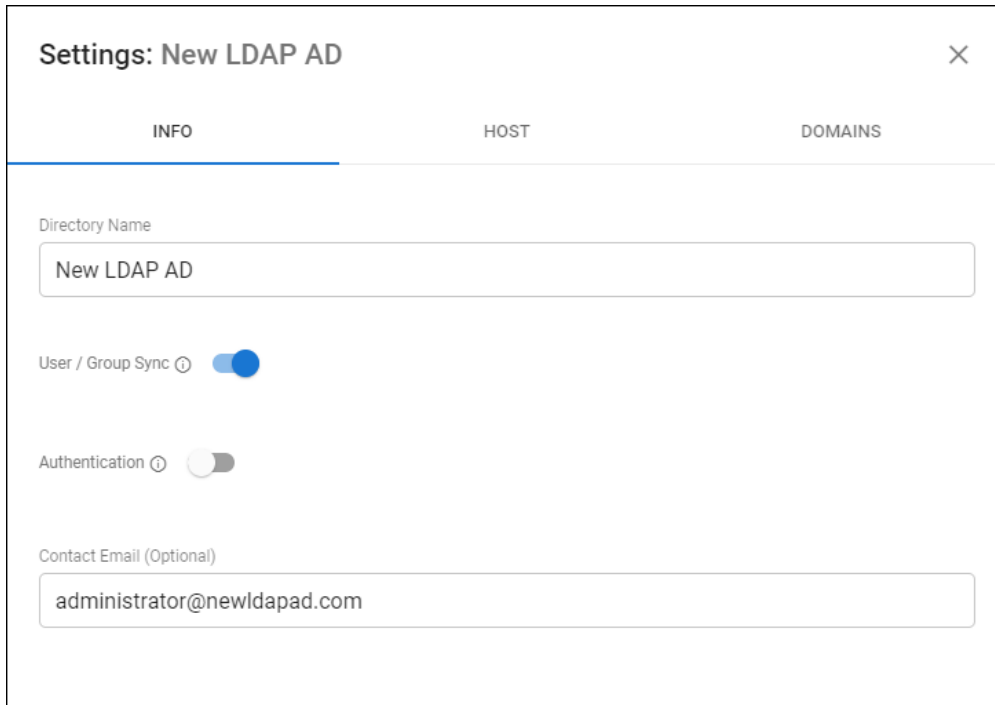
To ensure uninterrupted access to LDAP from the Barracuda Cloud, you must allow incoming connections from the following IP addresses.

- 35.170.131.81
- 54.156.244.63
- 54.209.169.44

View Existing Directories and Groups

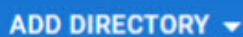
Complete the following steps to view existing directories and groups in Barracuda Cloud Control:

1. From the **Admin** tab in Barracuda Cloud Control, click **Directories**. The Directories table includes a row indicating whether or not **Authentication** has been set to **On** or **Off**.
2. Click **View groups** to display the groups associated with a configured directory.
3. You can synchronize the listed groups to ensure that user information is up-to-date by clicking **Sync groups**.
4. Click **Edit** for a specified group to modify the settings for the host or domain. When you have finished making changes, click **SAVE**.



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.

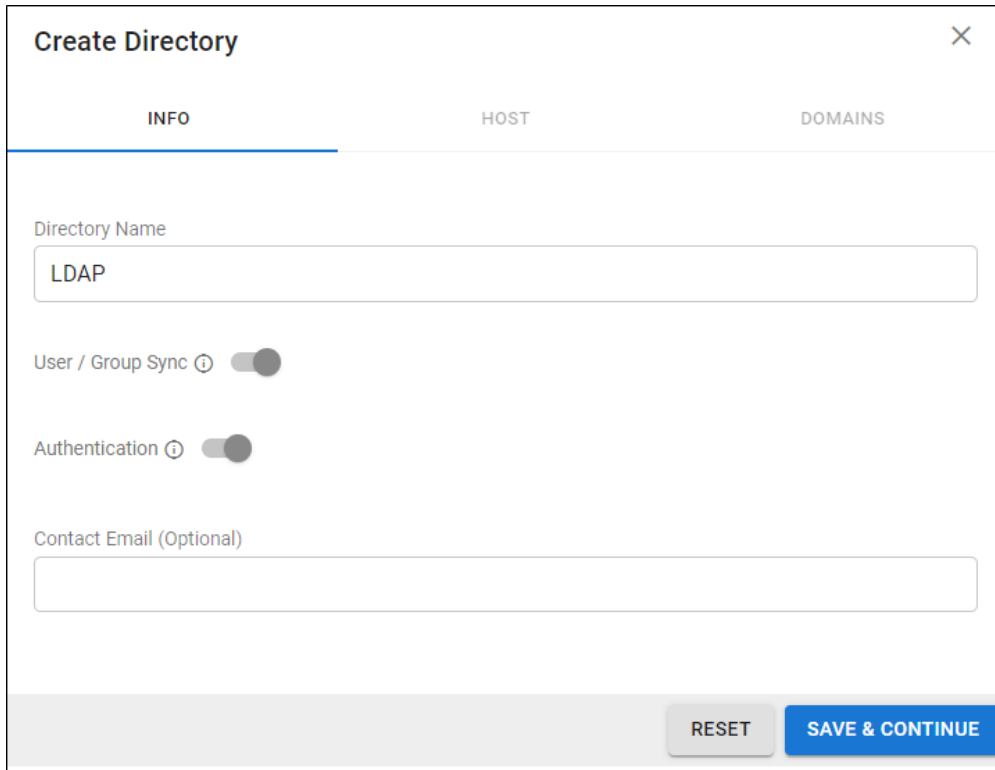


3. Select one of the following sections to add a new LDAP or Azure active directory.

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.



Create Directory [X]

INFO HOST DOMAINS

Directory Name

LDAP

User / Group Sync ☐

Authentication ☐

Contact Email (Optional)

RESET SAVE & CONTINUE

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

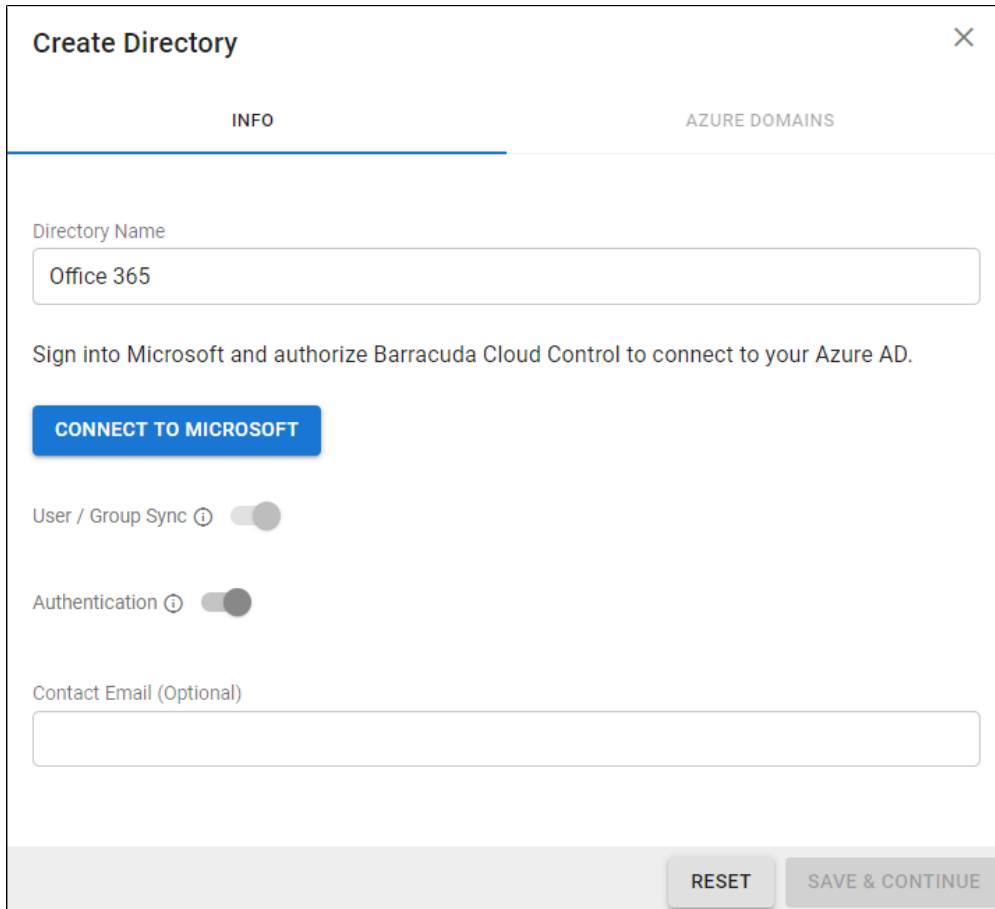
COPY VALUE TO CLIPBOARD

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**.

Re-authorize an Azure Active Directory

Complete the following steps to reauthorize an existing Azure AD directory:

1. Click the **Edit** option for the Azure AD directory you need to reauthorize from the **Admin > Directories** page.
2. Click **RE-AUTHORIZE**.
 - If Barracuda Networks' permissions were revoked from the LDAP account, you can use re-authorization to authenticate the linked Azure account and grant the permissions again.
 - If the list of domains on the Azure account has been updated, you can use re-authorization to update the corresponding list of domains in AuthDB.

The original administrator who initially authorized the Barracuda Networks permissions to the account does not have to be the one who re-authorizes the account. Another administrator on the same Azure account can complete this task. A non-administrator user on the same Azure account or any user on a different Azure account may not be used. The user who performed the most recent authorization is displayed above the **RE-AUTHORIZE** button.

Figures

1. bcc-new-ldap-ad.png
2. addLdap.jpg
3. addLdapInfo.png
4. addLdapHost.png
5. verifyLdapDomain.png
6. 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.