

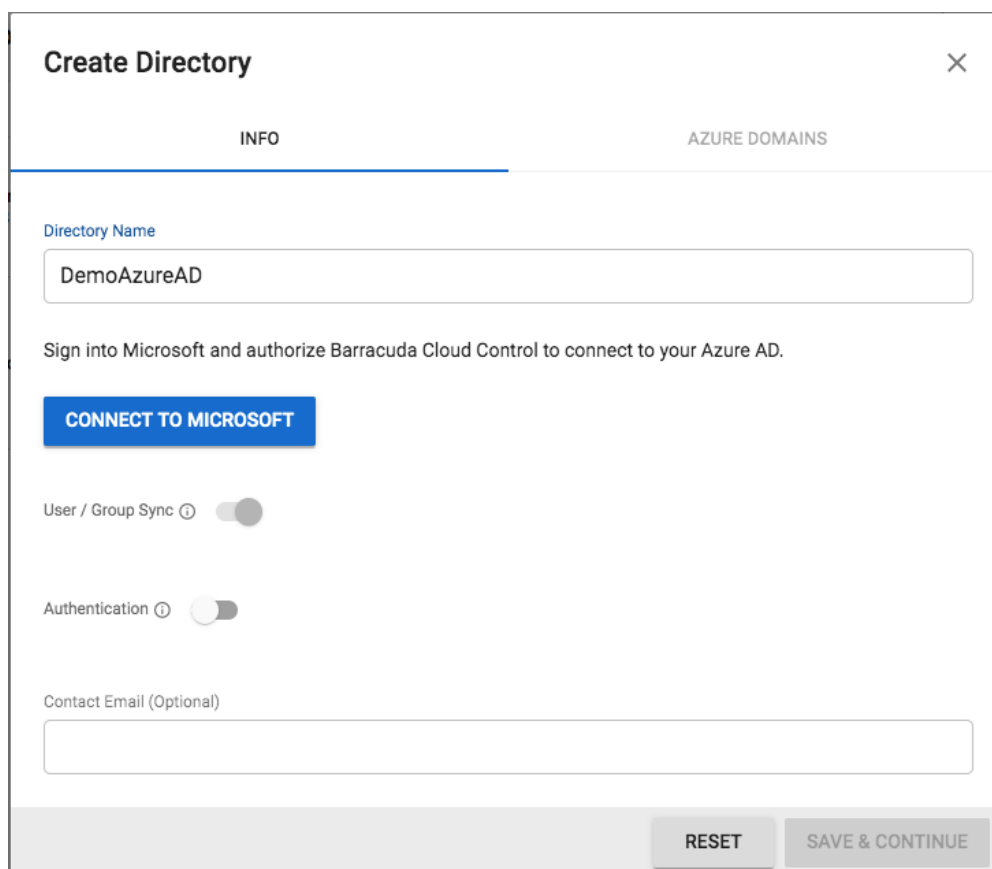
Microsoft Azure Active Directory Support for Single Sign-On

<https://campus.barracuda.com/doc/86540771/>

Microsoft Azure Active Directory (Azure AD) enables single sign-on/authentication for devices, apps, and services for users located almost anywhere. If you want to synchronize Barracuda Content Shield (BCS) users with your Azure AD instead of with your local LDAP/AD, follow the steps in this article. Barracuda supports associating device identities with Azure AD using the Hybrid Azure AD (Hybrid AAD) join method for federated domains.

This article assumes that the Hybrid Azure AD join has already been set up and configured. In order for the Barracuda Web Filtering Component (WFC) of the Barracuda Content Shield Suite to identify users and sync relevant policies at the endpoint, Azure AD needs to be configured on Barracuda Cloud Control (BCC). To do so, follow these steps:

Step 1. Log into your BCC account using your BCS credentials. Click **Add Directory**, and then select *Azure Active Directory*. A pop-up window opens as shown below:



Create Directory [X]

INFO | AZURE DOMAINS

Directory Name
DemoAzureAD

Sign into Microsoft and authorize Barracuda Cloud Control to connect to your Azure AD.

CONNECT TO MICROSOFT

User / Group Sync

Authentication

Contact Email (Optional)

RESET | SAVE & CONTINUE

Step 2. Enter the relevant directory name and click **Connect to Microsoft**. You will be redirected to log in with your Microsoft account. After logging in, you should see the following screen to grant access permissions to Barracuda Networks. Click **Accept**.



qacudatme1@cudatme.com

Permissions requested Accept for your organization

Barracuda Networks

[App info](#)

This app would like to:

- ✓ Read and write user files
- ✓ Read user files
- ✓ Have full control of all site collections
- ✓ Read and write items and lists in all site collections
- ✓ Read and write items in all site collections
- ✓ Read items in all site collections
- ✓ Read and write managed metadata
- ✓ Read managed metadata
- ✓ Read and write items and lists in all site collections
- ✓ Have full control of all site collections
- ✓ Read items in all site collections
- ✓ Read and write items in all site collections
- ✓ Read and write files in all site collections
- ✓ Read files in all site collections
- ✓ Read user mail

After the Azure AD has been added on BCC, it will show up in the **Directories** section of your BCC account page.

cudaTME.com



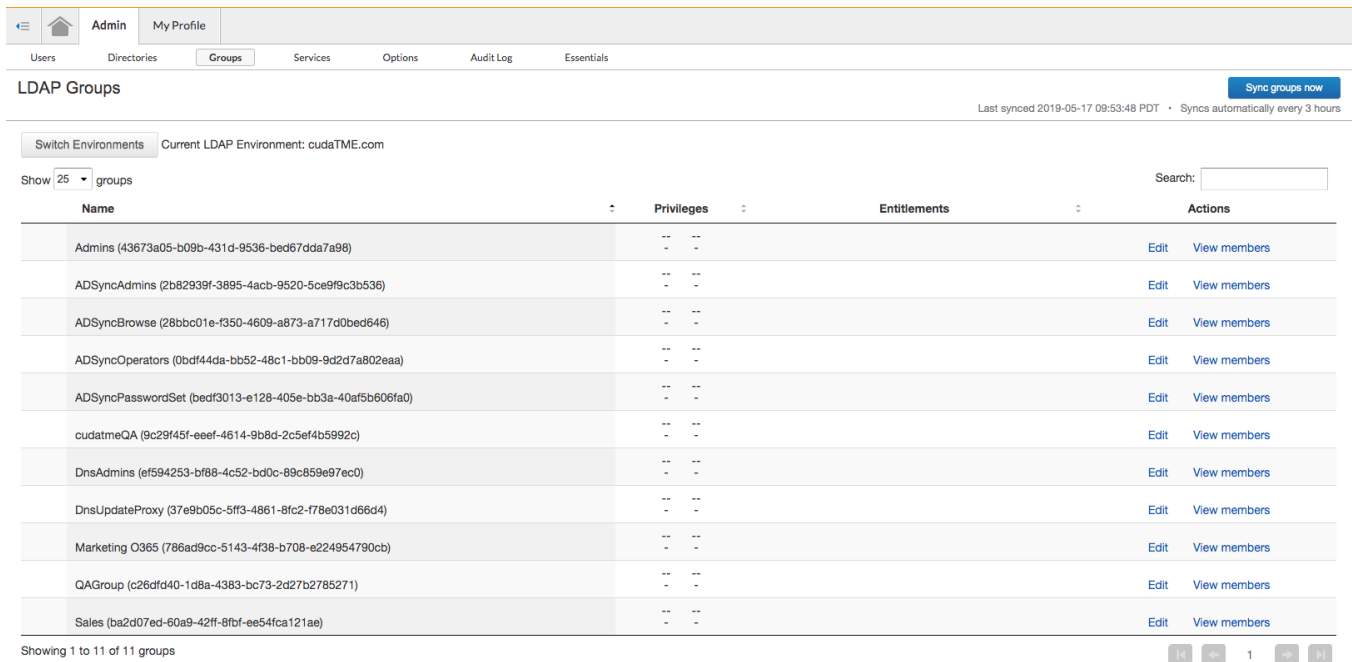
Success
9:53 AM

Off

✓ cudatme.com
✓ cudatme.mail.onmicrosoft.com
✓ cudatme.onmicrosoft.com
[and 1 more](#)

[VIEW GROUPS](#) [EDIT](#)

Step 3. After the automatic Sync is completed, you will see a *Success* message with the time of the last sync. Click **VIEW GROUPS** to verify if the Groups have synchronized successfully as shown below:



LDAP Groups Sync groups now

Last synced 2019-05-17 09:53:48 PDT • Syncs automatically every 3 hours

Switch Environments Current LDAP Environment: cudaTME.com

Show 25 groups Search:

Name	Privileges	Entitlements	Actions
Admins (43673a05-b09b-431c-9536-bed67dda7a98)	-- --		Edit View members
ADSyncAdmins (2b82939f-3895-4acb-9520-5ce9f9c3b536)	-- --		Edit View members
ADSyncBrowse (28bbc01e-f350-4609-a873-a717d0bed646)	-- --		Edit View members
ADSyncOperators (0bdf44da-bb52-48c1-bb09-9d2d7a802eaa)	-- --		Edit View members
ADSyncPasswordSet (bedf3013-e128-405e-bb3a-40af5b608fa0)	-- --		Edit View members
cudaTMEQA (9c29f45f-eeef-4614-9b8d-2c5ef4b5992c)	-- --		Edit View members
DnsAdmins (ef594253-bf88-4c52-bd0c-89c859e97ec0)	-- --		Edit View members
DnsUpdateProxy (37e9b05c-5ff3-4861-8fc2-f78e031d66d4)	-- --		Edit View members
Marketing O365 (786ad9cc-5143-4f38-b708-e224954790cb)	-- --		Edit View members
QAGroup (c26dfd40-1d8a-4383-bc73-2d27b2785271)	-- --		Edit View members
Sales (ba2cd07ed-60a9-42ff-8fbf-ee54fca121ae)	-- --		Edit View members

Showing 1 to 11 of 11 groups 1

Step 4. Make sure that the Barracuda WFC on the endpoint machine is able to detect Users/Groups and apply relevant policies.

1. Log into BCS and go to the **USERS** page.
2. Click **Directory Services** next to **Configure users**.
3. Log out of BCS.
4. Log in as an LDAP user on the client PC, which is joined to the on-premise AD, and verify that user-specific (if configured) policies are applied. You should be able to see the user traffic on the **WEB FILTERING LOGS** page in the Barracuda Content Shield service.

To finalize the Hybrid AAD Connect setup, follow the additional steps described here:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-hybrid-azure-ad-join-post-config-tasks>.

For details on how to setup the Hybrid Azure AD join, see Microsoft documentation at

<https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan> .

Figures

1. Create Directory Azure.png
2. Azure AD Permissions.png
3. AzureAD Directories.png
4. Azure AD LDAP Groups page.png

© Barracuda Networks Inc., 2020 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.