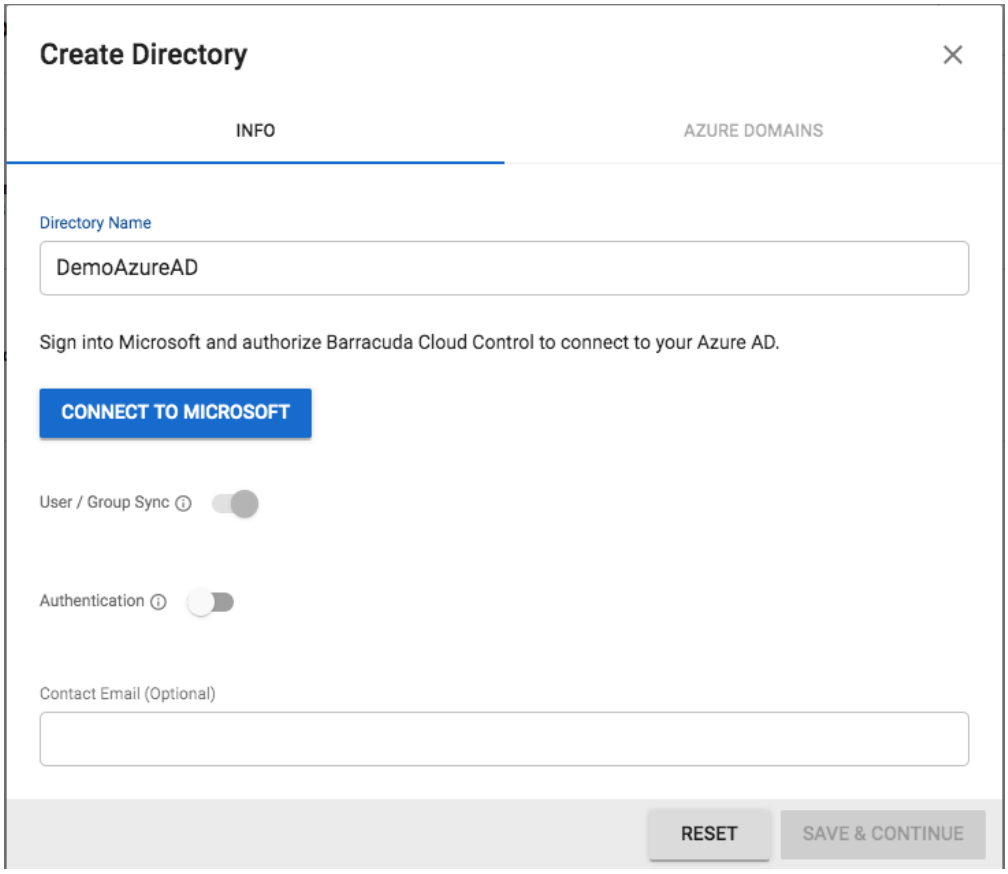
Microsoft Azure Active Directory Support for Single Sign-On

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

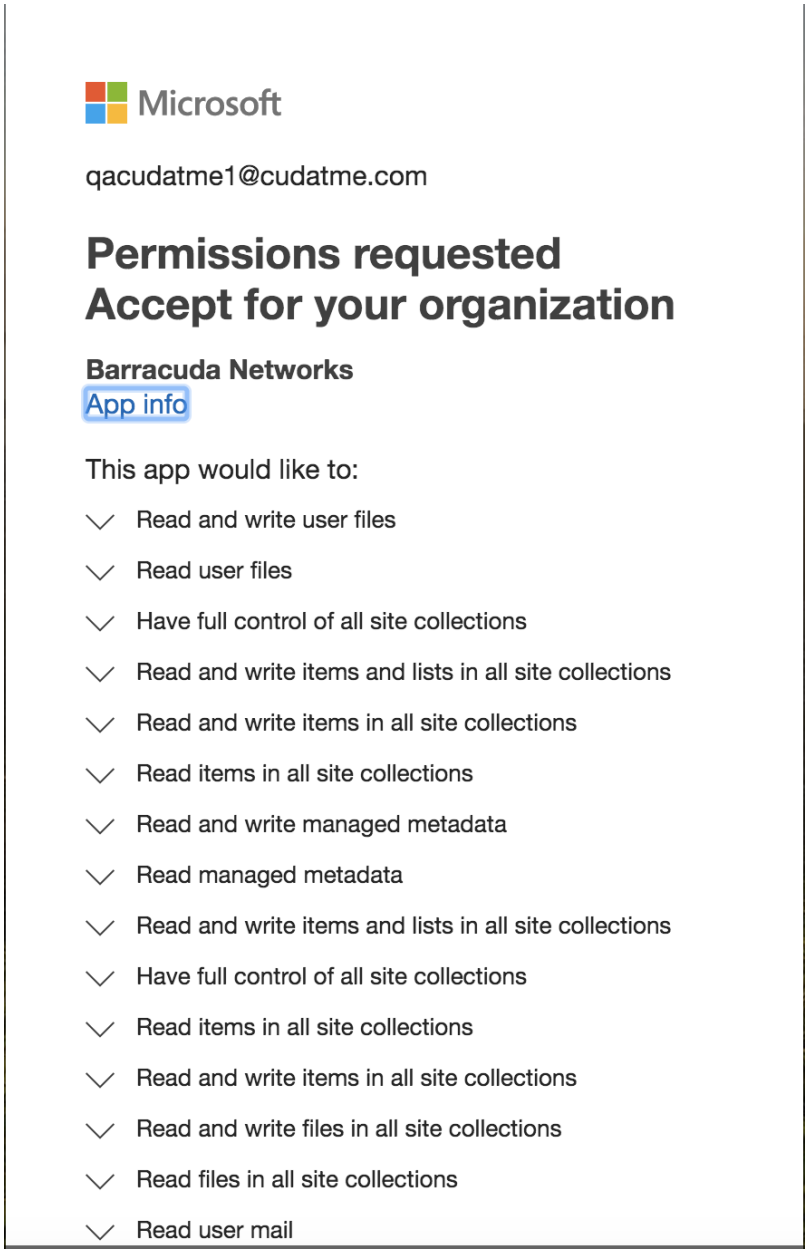
Microsoft Azure Active Directory (Azure AD) enables single sign-on/authentication for devices, apps, and services for users located almost anywhere. If you want to synchronize Barracuda Content Shield (BCS) users with your Azure AD instead of with your local LDAP/AD, follow the steps in this article. 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:

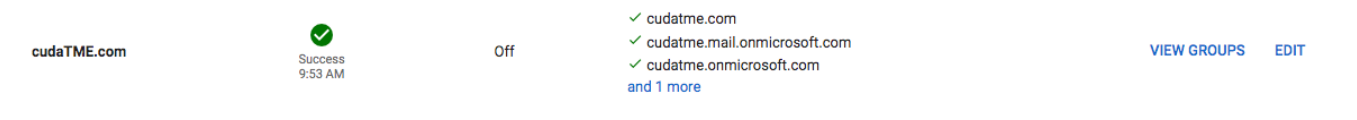
Step 1. Log into your BCC account using your BCS credentials. Click **Add Directory**, and then select *Azure Active Directory*. A pop-up window opens as shown below:



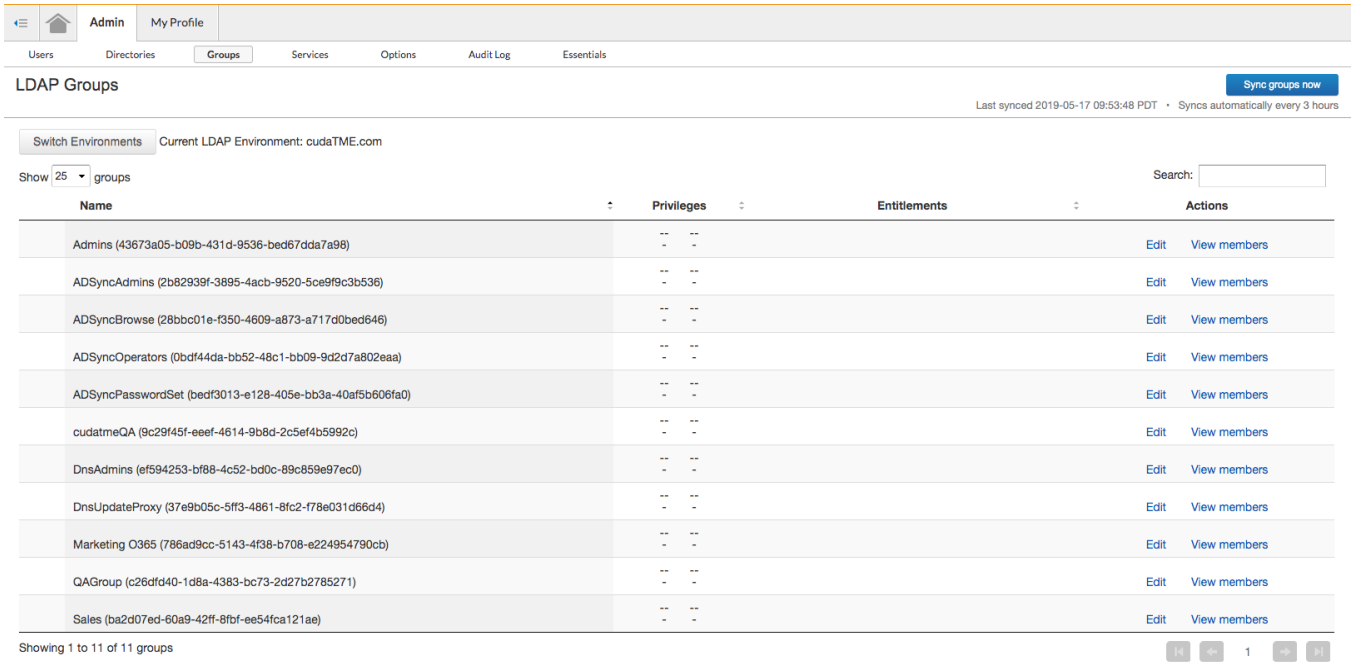
Step 2. Enter the relevant directory name and click **Connect to Microsoft**. You will be redirected to log in with your Microsoft account. After logging in, you should see the following screen to grant access permissions to Barracuda Networks. Click **Accept**.



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



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:



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