

Single Sign-On with Microsoft Entra ID (OAuth)

<https://campus.barracuda.com/doc/93880574/>

Customers with a configured Microsoft Entra ID in Barracuda Cloud Control can now log into Barracuda Cloud Control using their Microsoft Entra ID credentials. This means that customers using multi-factor authentication (MFA) with Microsoft Entra can now use that same process for signing into Barracuda Cloud Control. This provides users with a secure, smooth login experience to Barracuda Cloud Control.

Upon signing into Barracuda Cloud Control, Microsoft Entra users will be redirected to Microsoft for authentication. After users are authenticated with Microsoft, they are signed into Barracuda Cloud Control.

What is Single Sign-On?

With Microsoft Entra ID Single Sign-On (SSO), users sign in once using their primary organizational account to securely access web and SaaS applications. SSO enables users to authenticate applications using their single organizational account.

The SSO environment protects defined resources (websites and applications) by requiring the following steps before granting access:

1. Authentication: Authentication verifies the identity of a user using login credentials.
2. Authorization: Authorization applies permissions to determine if this user may access the requested resource.

Users are signed into Barracuda Cloud Control automatically if they are already signed into Microsoft Entra. This reduces the number of times a user must enter their credentials into their applications, increasing their productivity. To learn more, see the Microsoft article [What is single sign-on \(SSO\)](#).

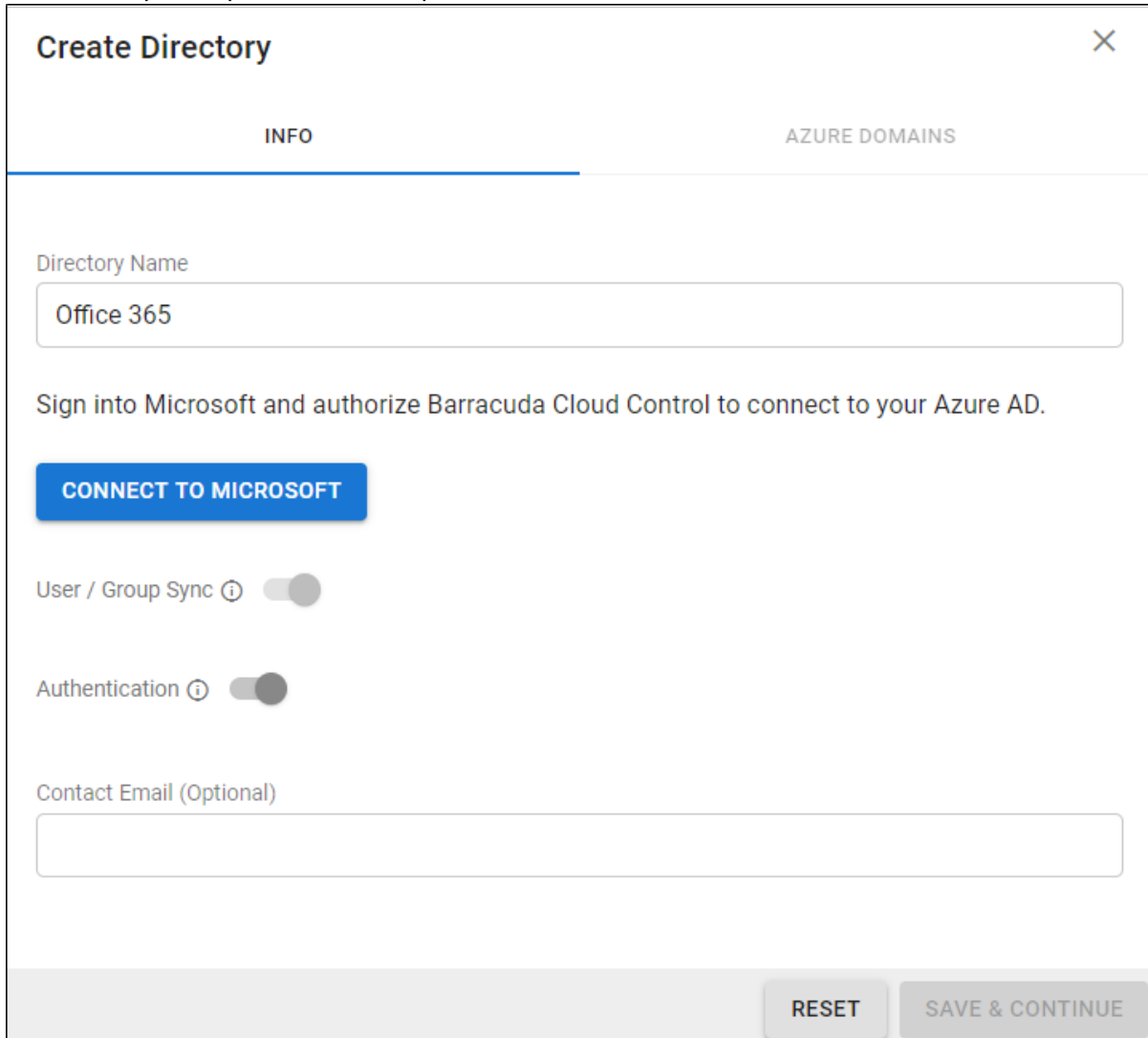
How to Configure Single Sign-On with Microsoft Entra ID

The following steps must be done by a Barracuda Cloud Control User Administrator. For more information about users and user privileges in Barracuda Cloud Control, see [How to Add Users and Configure Product Entitlements and Permissions](#).

1. Log into [Barracuda Cloud Control](#) as the account administrator, and go to **Home > Admin > Directories**.
2. Click the **Add Directory** button.

[ADD DIRECTORY ▾](#)

3. Select **Azure Active Directory** (now Microsoft Entra ID).
4. On the **INFO** tab, specify a new **Directory Name**. For example, "Office 365".
5. Click **CONNECT TO MICROSOFT** to sign into Microsoft and authorize Barracuda Cloud Control to connect to your Microsoft Entra ID.
 1. Log in with your Microsoft administrator credentials.
 2. Accept the permissions required for Barracuda Cloud Control to access Microsoft Entra ID.



Create Directory ✕

INFO **AZURE DOMAINS**

Directory Name

Office 365

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**

6. Activate/Enable the **Authentication** option to have users authenticate to Barracuda Cloud Control using their Microsoft Entra ID credentials. If this option is disabled, users will not be redirected to Microsoft for authentication and will authenticate with Barracuda Cloud Control.

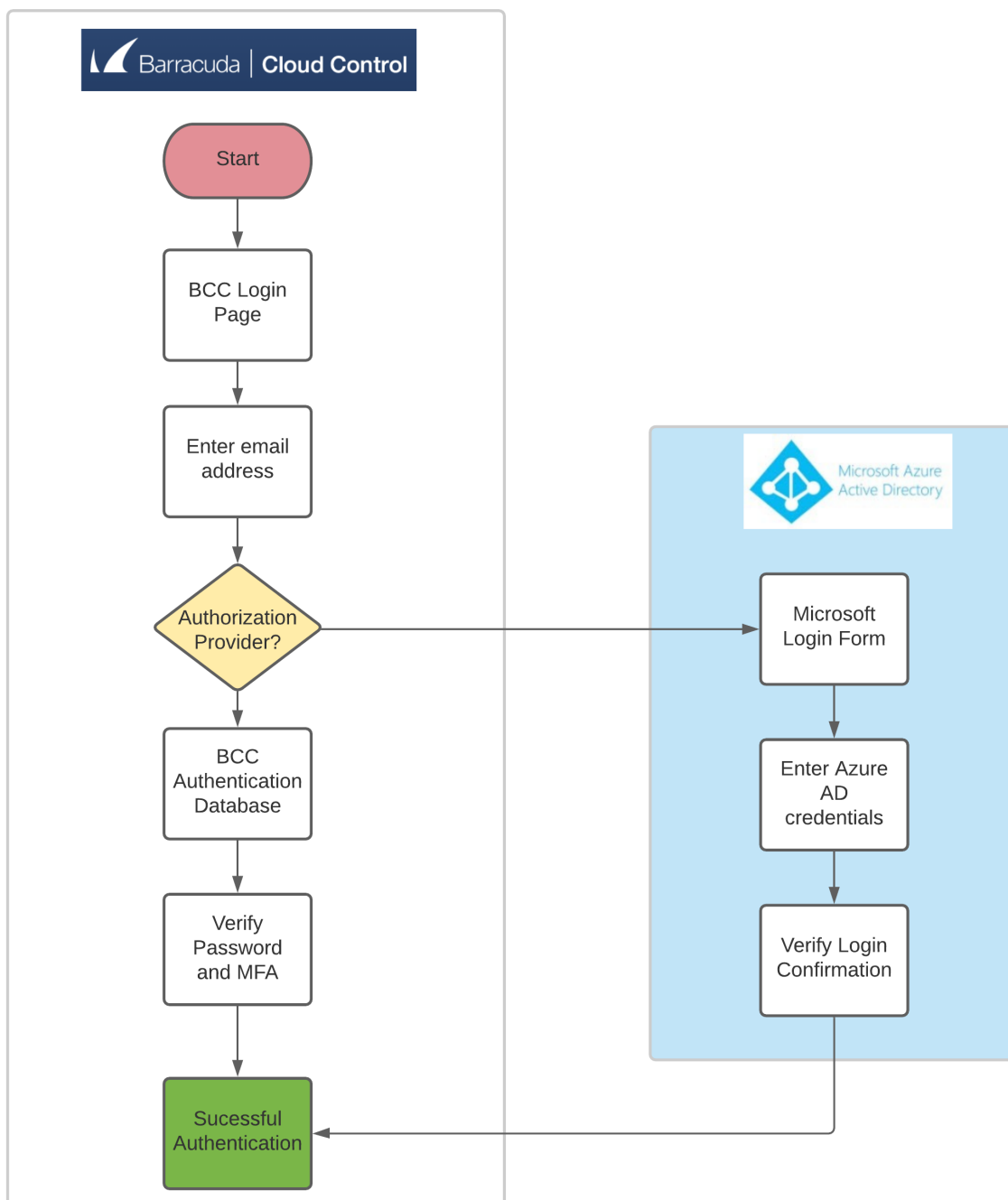
Barracuda Networks strongly recommends creating an additional administrator account using an independent domain that does not use Active Directory (AD) authentication. This allows you access to your Barracuda Networks product account if your AD server goes down or fails.

After you are redirected back to Barracuda Cloud Control, your domains are queried and shown on the **AZURE DOMAINS** tab.

7. Click **Save**.

8. After a successful sync of the new directory, users in the directory can now enter their company-provided email address in the Barracuda Cloud Control login page. When Barracuda Cloud Control detects that the email address matches one of the users in the Microsoft Entra ID setup, Barracuda Cloud Control will redirect the user in their web browser to Microsoft to complete authentication and return the user to Barracuda Cloud Control.

User Authentication Flow Chart



Authentication with Barracuda Networks products and Known Issues

At this time, single sign-on support with Microsoft Entra ID is only supported by Barracuda Cloud Control (BCC). All authentication and product access must use the BCC login page and redirect to Microsoft for authentication.

If you access a Barracuda Networks product login page outside of BCC, for example, sentinel.barracudanetworks.com, authentication is only handled using the default BCC authentication method which requires an email address and password. Organizations that have MFA configured with Microsoft will encounter login failures because users do not redirect to Microsoft for authentication, and we are unable to meet Microsoft's MFA requirement. To avoid this issue, log into BCC at <https://auth.barracudanetworks.com/> and then access the desired Barracuda Networks product. If this is not feasible, contact [Barracuda Networks Technical Support](#) to apply a patch on your account that bypasses the MFA requirement from Microsoft and allow you to login with just an email address and password.

Troubleshooting

This table contains troubleshooting information on possible issues and how to fix them.

Failure	Possible Causes	Possible Solutions
Error after returning from Microsoft when connecting to a new Active Directory.	<ul style="list-style-type: none">• User setting up a new Active Directory is not an Administrator in their company's Microsoft Entra ID.• User did not consent to the required permissions when prompted by Microsoft.	<ul style="list-style-type: none">• Ensure user is an Administrator in their company's Microsoft Entra ID.• Ensure user consents to the required permissions when redirected to Microsoft during the connection process.
Error fetching domains after initial connection to Microsoft.	<ul style="list-style-type: none">• Temporary authentication failure from Microsoft.	<ul style="list-style-type: none">• Attempt to reauthorize with Microsoft and retry.
Error returned during syncing of users and groups.	<ul style="list-style-type: none">• User revoked consent within their Microsoft Entra ID portal.• Temporary authentication failure from Microsoft.	<ul style="list-style-type: none">• Attempt to reauthorize with Microsoft on the Directories page.• Force a resynchronization of the AD on the Admin > Groups page.

<p>Error returned during sign-in attempt for Microsoft Entra ID user.</p> <p>Examples of user-facing errors:</p> <ul style="list-style-type: none">• Failed to authenticate with Microsoft, please try again.• Invalid information returned from Microsoft during authentication, please try again.• Failed to finish authentication with Microsoft, please try again.	<ul style="list-style-type: none">• User canceled the authentication request.• Temporary authentication failure from Microsoft.	<ul style="list-style-type: none">• Ensure user fully completes the authentication process when redirected to Microsoft during the login process.• Retry authentication again in a few minutes.
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figures

1. addDirectory.png
2. addAzure.png
3. bcc_azure_auth.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.