

Cloudbrink - MS Entra ID Integration

Cloudbrink's [Hybrid Access as a Service](#) has granular role based access controls, enabling administrators to assign different users and groups to needed public and private resources. Rather than requiring customers to manually define these users and groups, Cloudbrink instead integrates with the customer's existing identity provider. This enables organizations and their end-users to utilize existing single sign-on methods, simplifying onboarding and management. This document covers configuring Cloudbrink with Entra ID.

Overview

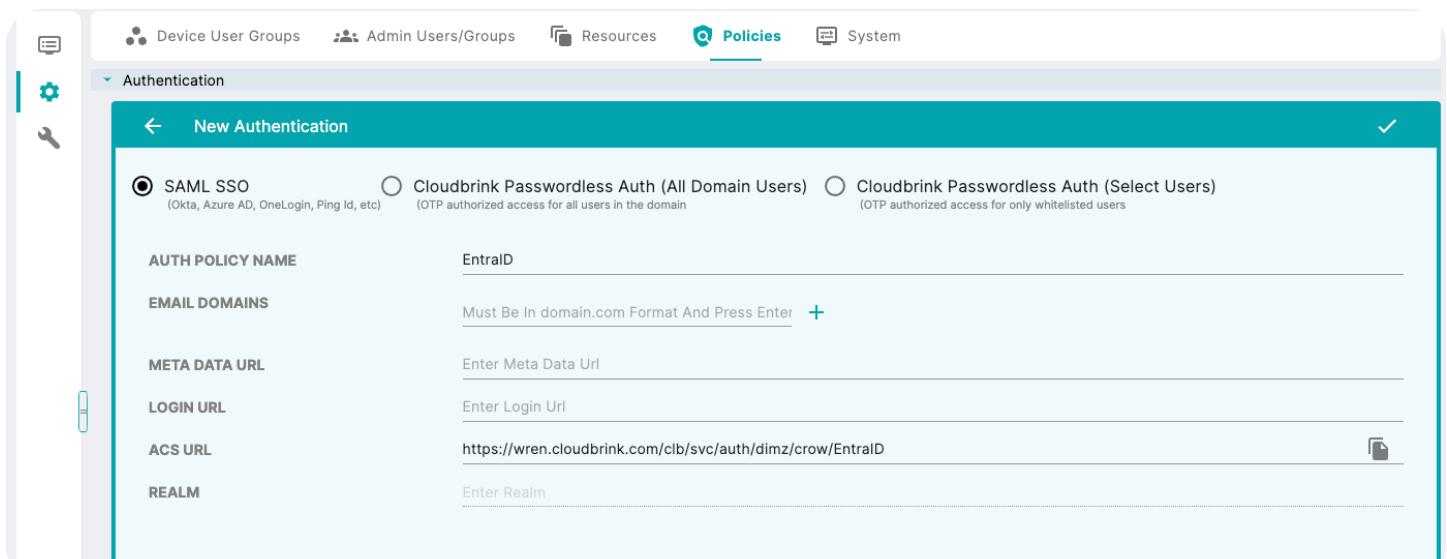
Microsoft Entra Identity, commonly known as Entra ID, is a comprehensive identity and access management solution designed to enhance security and streamline user access across various platforms. Its key benefits include robust authentication mechanisms, centralized identity management, and simplified access controls. Entra ID facilitates secure and efficient user access, reducing the risk of unauthorized access and data breaches. By offering features like multi-factor authentication and single sign-on, it greatly improves the user experience while maintaining high security standards. This makes Entra ID an ideal choice for organizations looking to strengthen their cybersecurity infrastructure and optimize user access management with Cloudbrink.

Prerequisites

- Administrative access into the Cloudbrink Administrators portal
- Administrative access into the Microsoft Entra ID portal
- Cloudbrink Entra ID signing certificate provided from support@cloudbrink.com

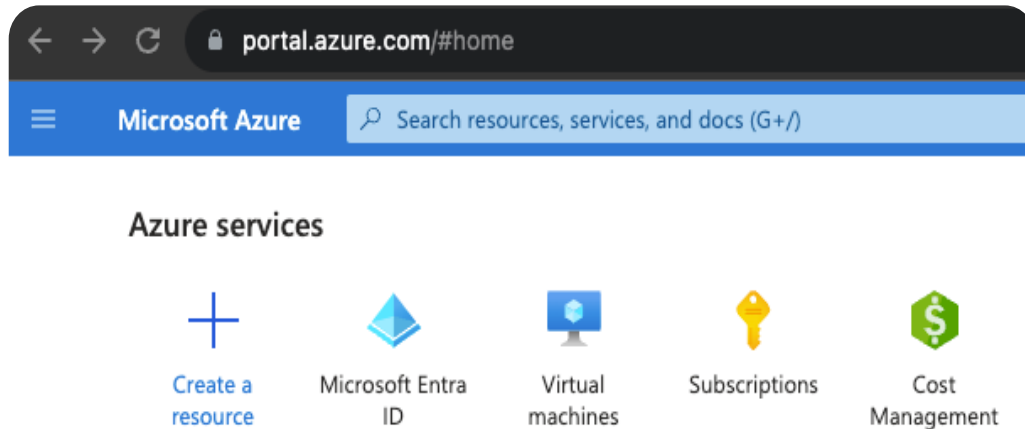
Configure Authentication Policy

1. Navigate to the Cloudbrink Admin portal admin.cloudbrink.com
2. Navigate to **Configure > Authentication > Create New Auth Policy** 

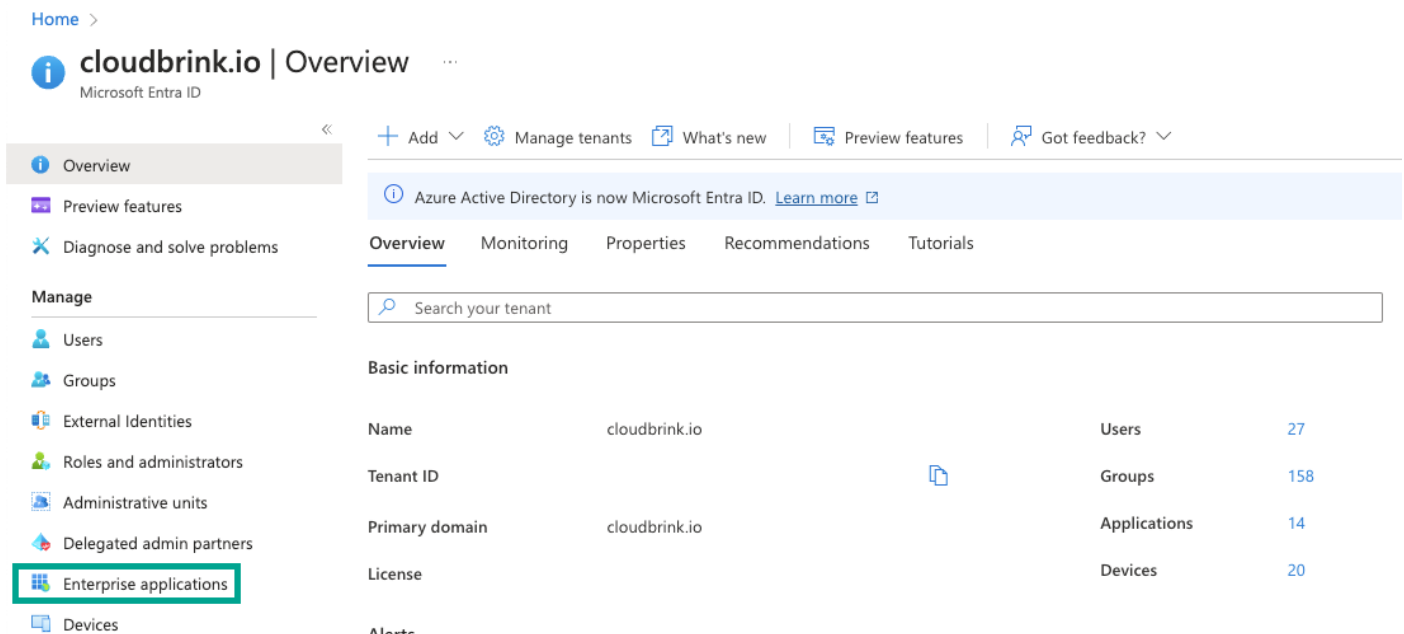


The screenshot shows the Cloudbrink Admin portal interface. The top navigation bar includes links for Device User Groups, Admin Users/Groups, Resources, Policies (active), and System. The left sidebar shows a settings icon and a search icon. The main content area is titled 'Authentication' and contains a 'New Authentication' form. The form has three radio button options: 'SAML SSO (Okta, Azure AD, OneLogin, Ping Id, etc)' (selected), 'Cloudbrink Passwordless Auth (All Domain Users) (OTP authorized access for all users in the domain)', and 'Cloudbrink Passwordless Auth (Select Users) (OTP authorized access for only whitelisted users)'. Below the options, the form fields are: 'AUTH POLICY NAME' (EntralD), 'EMAIL DOMAINS' (Must Be In domain.com Format And Press Enter +), 'META DATA URL' (Enter Meta Data Url), 'LOGIN URL' (Enter Login Url), 'ACS URL' (https://wren.cloudbrink.com/clb/svc/auth/dimz/crow/EntralD), and 'REALM' (Enter Realm).

3. Under SAML SSO, Input a unique **Auth Policy Name**, and **Email Domain**
4. Copy the **ACS URL** to a notepad
5. Navigate to the Entra ID portal.



6. Navigate to **Enterprise Applications** on the left hand panel



7. Click **+ New application** to create a new Enterprise Application for Cloudbrink
8. Click **+ Create your own application** and fill out the name of the app, as well as ensuring that "Integrate any other application you don't find in the gallery (Non-gallery)" is selected. Hit save.

What's the name of your app?

Cloudbrink ✓

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

9. On the next screen, select **1. Assign users and groups**


Properties


CL Name ⓘ
Cloudbrink ⓘ


Application ID ⓘ
746c6a64-4c08-4f2f-a51... ⓘ


Object ID ⓘ
41d6b3b4-4e2e-475e-9... ⓘ

Getting Started

**1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)

**2. Set up single sign on**
Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)

**3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)

**4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)

10. Select **+ Add user/group** and select the group(s) you'd like to have access via Cloudbrink.

Note: While here, you should copy the group "Object ID" value(s) and put them in your notepad from earlier. These will be used to map groups to access levels in the Cloudbrink admin portal later.



Membership type	Assigned ⓘ
Source	Cloud ⓘ
Type	Security ⓘ
Object Id	9921a048-9f4f-4f07-85ba-544e3a27bfe6 ⓘ
Created at	5/31/2023, 8:34:08 PM ⓘ

11. After you've added the groups required, from you Enterprise App menu, Select "Single sign-on" and then "SAML" from the left hand panel under manage.

«

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on


Provisioning


Application proxy


Self-service

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Select a single sign-on method [Help me decide](#)

**Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

**Password-based**
Password storage and replay using a web browser extension or mobile app.

12. Copy the "Login URL" lower on the page under number 4 to your notepad.

4

Set up Cloudbrink-Test

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com/4b060e07-99f3-...
Microsoft Entra Identifier	https://sts.windows.net/4b060e07-99f3-493a-872...
Logout URL	https://login.microsoftonline.com/4b060e07-99f3-...

13. Click "Edit" on the Basic SAML Configuration

1

Basic SAML Configuration

[Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

14. Under the right hand window, fill in the following fields:

- Identifier (Entity ID):** <https://wren.cloudbrink.com/<example>/svc/auth/<example>>
 - This is copied from step 4 above
- Reply URL:** <https://wren.cloudbrink.com/<example>/svc/auth/<example>>
 - Same as above
- Sign on URL:** <https://login.microsoftonline.com/<example>/>
 - Copied from step 12.

15. Once all above fields are filled appropriately, hit save on the top left.

Basic SAML Configuration

[Save](#)

[Got feedback?](#)

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
https://wren.cloudbrink.com/...			

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
https://wren.cloudbrink.com/...			

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
https://login.microsoftonline.com/.../saml2			

16. Click edit on the **Attributes & Claims** section

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

17. Click on **Add new claim** and fill out the following fields (non-specified fields can be left as default), and then click **Save**:

- Name:** Email
- Source attribute:** user.mail

Manage claim ...

Save

Discard changes

Got feedback?

Name *

Email

Namespace

Enter a namespace URI

Choose name format

Source *

☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute *

user.mail

Claim conditions

Advanced SAML claims options

18. Click **Add a Group claim** and in the pane that appears to the right, enter in the following fields and click **Save**:

- Which groups associated:** Security groups
- Source attribute:** Group ID
- Advanced options:**
 - Customize the name of the group claim:** Checkbox selected Groups
 - Name (required):** Groups

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- ☐ None
☐ All groups
☒ Security groups
☐ Directory roles
☐ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups ⓘ

Advanced options

☐ Filter groups

Attribute to match

Match with

String

☒ Customize the name of the group claim

Name (required)

Groups

Save

- Back within the Single sign-on section of the application, under the 3 SAML Signing Certificate section, copy the **App Federation Metadata URL** to your notepad.
- Click the three little dots on the top right corner under the **SAML Certificates** window and click **Edit**.

SAML Certificates

Token signing certificate

Status: Active
 Thumbprint: 5CBD964DA9FA397D9216D50C710DBE4AF1E1C9DF
 Expiration: 12/7/2026, 9:16:47 AM
 Notification Email: john@cloudbrink.io

App Federation Metadata Url: <https://login.microsoftonline.com/4b060e07-99f3-...>

Certificate (base64): Download
 Certificate (Raw): Download
 Federation Metadata XML: Download

Verification certificates (optional)

Required: No
 Active: 0
 Expired: 0

...

Edit

21. In the pane that appears to the right:
 - a. Click **Import Certificate**, and select the .PFX certificate file separately provided by Cloudbrink
 - b. While importing the file, enter in the **password** also separated by Cloudbrink
 - c. Ensure the certificate is set as **Active**
 - d. Change the **Signing Option** to **Sign SAML response and assertion**
 - e. Optionally, input a **Notification Email Address** to be notified of cert expiry reminders

SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save + New Certificate **Import Certificate** Got feedback?

Status	Expiration Date	Thumbprint
Active	12/7/2026, 9:16:47 AM	5CBD964DA9FA397D9216D50C710DBE4AF1E1C9DF

Signing Option: Sign SAML response and assertion

Signing Algorithm: SHA-256

Notification Email Addresses

notifyme@emaildomain.com

22. Navigate back to the **Cloudbrink Admin Portal** and to your **Authentication Policy**
23. Paste in the **Metadata URL**, and **Login URL** as copied to your notepad in steps 12 and 19. Then click the checkmark in the top right corner to save

New Authentication

☒ SAML SSO
(Okta, Azure AD, OneLogin, Ping Id, etc)
 ☐ Cloudbrink Passwordless Auth (All Domain Users)
(OTP authorized access for all users in the domain)
 ☐ Cloudbrink Passwordless Auth (Select Users)
(OTP authorized access for only whitelisted users)

AUTH POLICY NAME: EntraID

EMAIL DOMAINS: Must Be In domain.com Format And Press E

cloudbrink

META DATA URL: https://login.microsoftonline.com/4b060e07-99f3-493a-8724-b546522e09bc/federationmetadata/2007-06/federationmeta

LOGIN URL: https://login.microsoftonline.com/4b060e07-99f3-493a-8724-b546522e09bc/saml2

ACS URL: https://wren.cloudbrink.com/clb/svc/auth/dimz/crow/EntraID

REALM: Enter Realm

24. Navigate to **Device User Groups**
25. For every group you desire to use with Cloudbrink for login, create a corresponding device user group the the Device User Group value being the EntraID Group Object ID

Device User Groups

Admin Users/GroupsResourcesPoliciesSystem

Device User Groups

Device User Groups 3

DEVICE USER GROUP	DESCRIPTION
Engineering-Division	Device User Group for users belonging to the Engineering Division
Marketing-Division	Device User Group for users belonging to the Marketing Division
Sales-Division	Device User Group for users belonging to the Sales Division

New Device User Group

DEVICE USER GROUP

1544721a-9184-4c2f-b7ec-4072c14c0782

DESCRIPTION

ObjectID for the EntraID Group "Engineering"

26. Create a new **Device User Group Policy**, and select the desired Resource Template. Optionally, select your desired DSPA Policy, Device Session Policy, and Mobile Access Policy

Engineering-Resource-Template

DEVICE USER GROUP	1544721a-9184-4c2f-b7ec-4072c14c0782
RESOURCE TEMPLATE	Engineering-Resource-Template
DSPA POLICY	Ubuntu-Secure-Device
DEVICE SESSION POLICY	8-HR-Policy
MOBILE ACCESS POLICY	

27. Users logging in to the Brink App with the configured group will then have the desired policies applied

Support

We would love to hear from you! For any questions, concerns, or feedback regarding this feature, please reach out at support@cloudbrink.com