Configuring Microsoft Entra ID Sign-In for the Cigent Console

Document Type	Integration Guide
Audience	Cigent administrators and Microsoft Entra ID administrators
Purpose	Configure Microsoft Entra ID authentication for Cigent Console sign-in and role-based access

Revision: 2

Overview

This guide describes how to configure Microsoft Entra ID (formerly Azure Active Directory) authentication for the Cigent Console. When configured, users can sign in to the console using their organizational Microsoft credentials.

Entra ID integration enables administrators to:

- Authenticate users using the organization's Microsoft identity provider.
- Control console access through Entra ID security groups.
- Assign Cigent Console roles based on group membership.

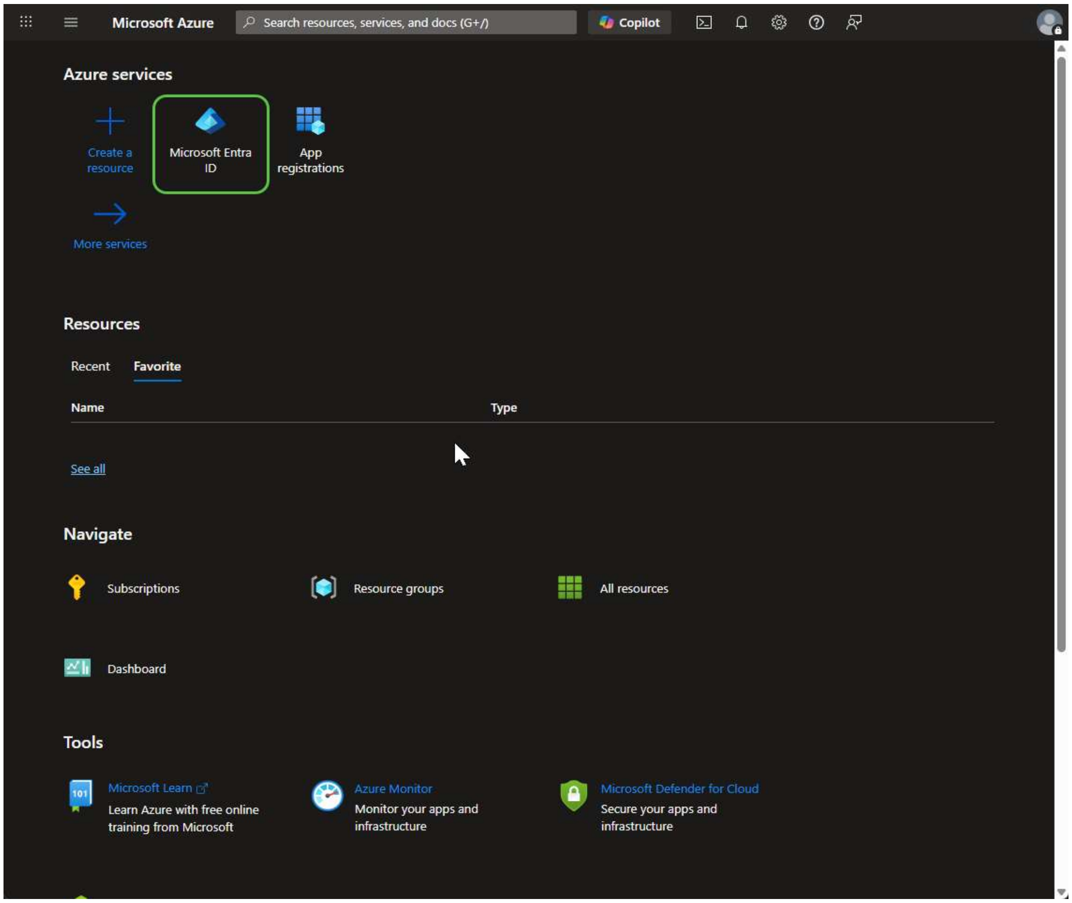
Prerequisites

Azure access	Access to the Microsoft Azure Portal and Microsoft Entra ID.
Administrative permissions	Permission to view tenant information and manage groups.
Console access	Administrative access to the Cigent Console.
Required values	Tenant ID and one or more Entra ID Group Object IDs.

Step 1 - Access Microsoft Entra ID

1. Log in to the Microsoft Azure Portal.
2. Navigate to Microsoft Entra ID.

> **Note:** This area of the Azure Portal contains the tenant, users, and groups required for the integration.



Learn Azure with free online training from Microsoft

Monitor your apps and infrastructure

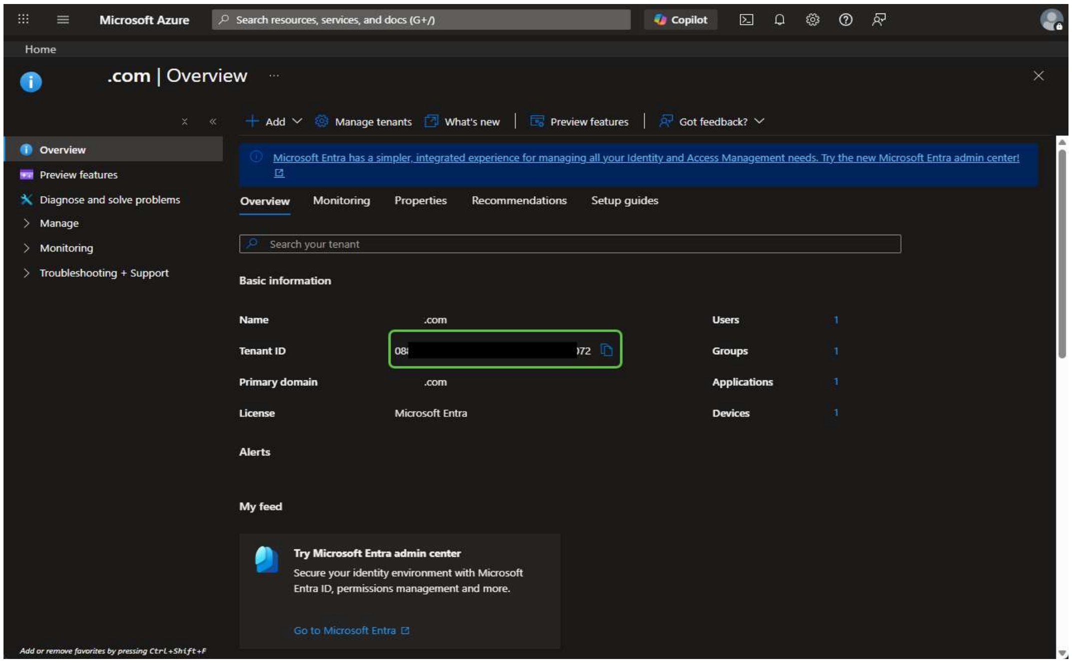
Secure your apps and infrastructure

Figure 1. Microsoft Entra ID location in Azure Portal

Step 2 - Locate the Tenant ID

1. Open the Overview page for Microsoft Entra ID.
2. Locate the Tenant ID field.
3. Copy and save the Tenant ID for use in the Cigent Console.

> **Note:** The Tenant ID uniquely identifies the organization's Entra ID directory and is required by the Cigent Console integration.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Basic information

Name	.com	Users	1
Tenant ID	[redacted]	Groups	1
Primary domain	.com	Applications	1
License	Microsoft Entra	Devices	1

Alerts

My feed

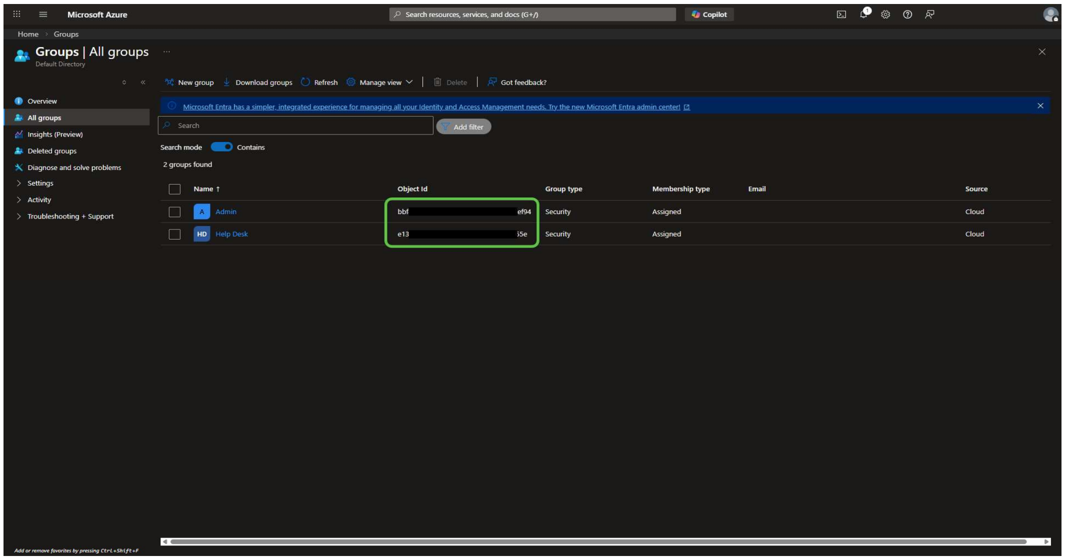
Try Microsoft Entra admin center
Secure your identity environment with Microsoft Entra ID, permissions management and more.
Go to Microsoft Entra

Figure 2. Tenant ID in Microsoft Entra ID Overview

Step 3 - Create or Identify Entra ID Groups

1. Navigate to Groups in Microsoft Entra ID.
2. Create new groups or select existing groups for Cigent Console access.
3. Add the appropriate users to each group.
4. Record the Object ID for each group that will be mapped in the Cigent Console.

> **Note:** Group names may be chosen freely. The Object ID, not the display name, is the value required for configuration.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

2 groups found

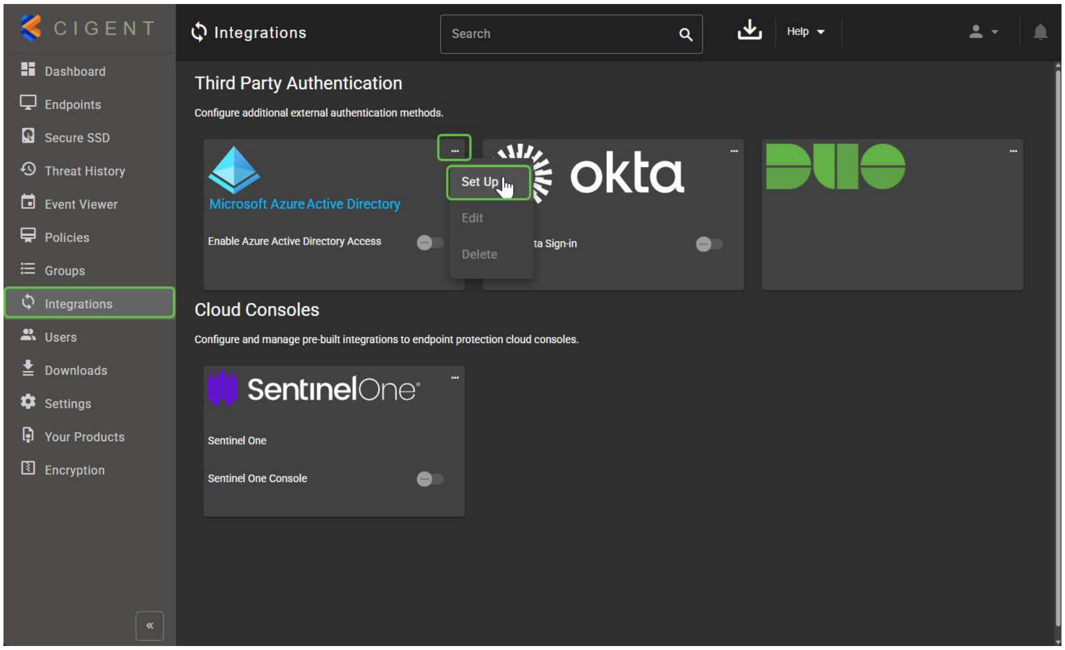
Name ↑	Object Id	Group type	Membership type	Email	Source
A Admin	bbf[redacted]ef94	Security	Assigned		Cloud
HD Help Desk	e13[redacted]5e	Security	Assigned		Cloud

Figure 3. Example Entra ID group configuration and Object ID

Step 4 - Configure Entra ID Integration in the Cigent Console

1. Log in to the Cigent Console as an administrator.
2. Open the Integrations page from the navigation menu.
3. Locate Microsoft Entra ID integration.
4. Select Setup from the options menu (ellipsis).

> **Note:** This step opens the console-side configuration for the identity provider connection.



Third Party Authentication

Configure additional external authentication methods.

Enable Azure Active Directory Access

Cloud Consoles

Configure and manage pre-built integrations to endpoint protection cloud consoles.

Sentinel One

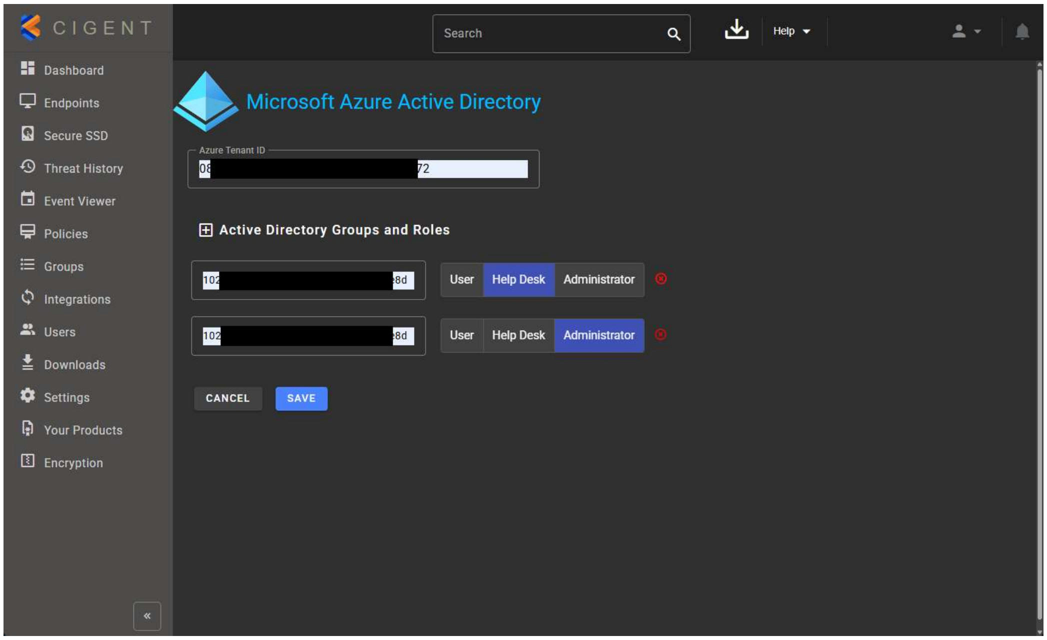
Sentinel One Console

Figure 4. Microsoft Entra ID integration setup in Cigent Console

Step 5 - Enter Tenant and Group Information

1. Enter the Tenant ID obtained from Microsoft Entra ID.
2. Enter one or more Group Object IDs.
3. Assign the appropriate Cigent Console role to each group mapping.

> **Note:** Each group may be assigned a different role, enabling role-based access management through Entra ID group membership.



Microsoft Azure Active Directory

Azure Tenant ID: 0[redacted]72

Active Directory Groups and Roles

10[redacted]8d — User [✓ Help Desk] Administrator

10[redacted]8d — User Help Desk [✓ Administrator]

CANCEL SAVE

Figure 5. Tenant ID, group mapping, and role assignment

Step 6 - Test the Integration

1. Navigate to the Cigent Console login page.
2. Select Sign in with Microsoft.
3. Authenticate using organizational Microsoft credentials.
4. Confirm that the user is redirected back to the Cigent Console with the expected access level.

> **Note:** If the user is already authenticated with Microsoft, sign-in may complete automatically without prompting for credentials again.

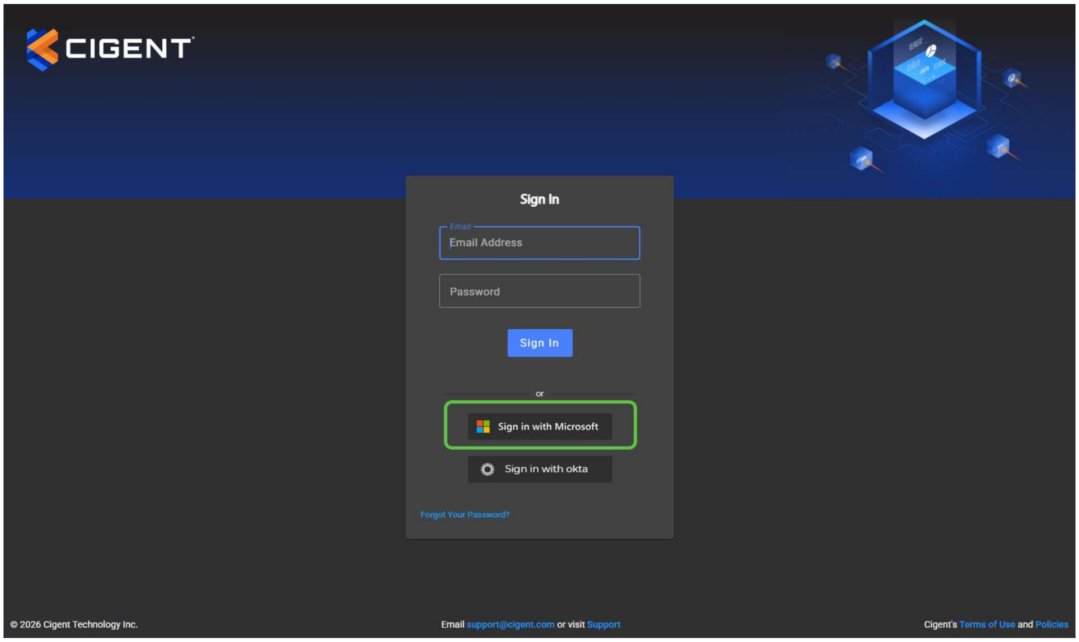


Figure 6. Microsoft sign-in flow from the Cigent Console login page

Result

After configuration is complete, users who are members of the mapped Entra ID groups can sign in to the Cigent Console using their Microsoft organizational accounts. Access can be managed through group membership in Entra ID rather than by maintaining individual console accounts.