



# Setup Access to SecureX Sign-On

via Microsoft Azure

Martin G. Nystrom

# 1. User Sign In via “Sign in with Microsoft”

<https://sign-on.security.cisco.com>

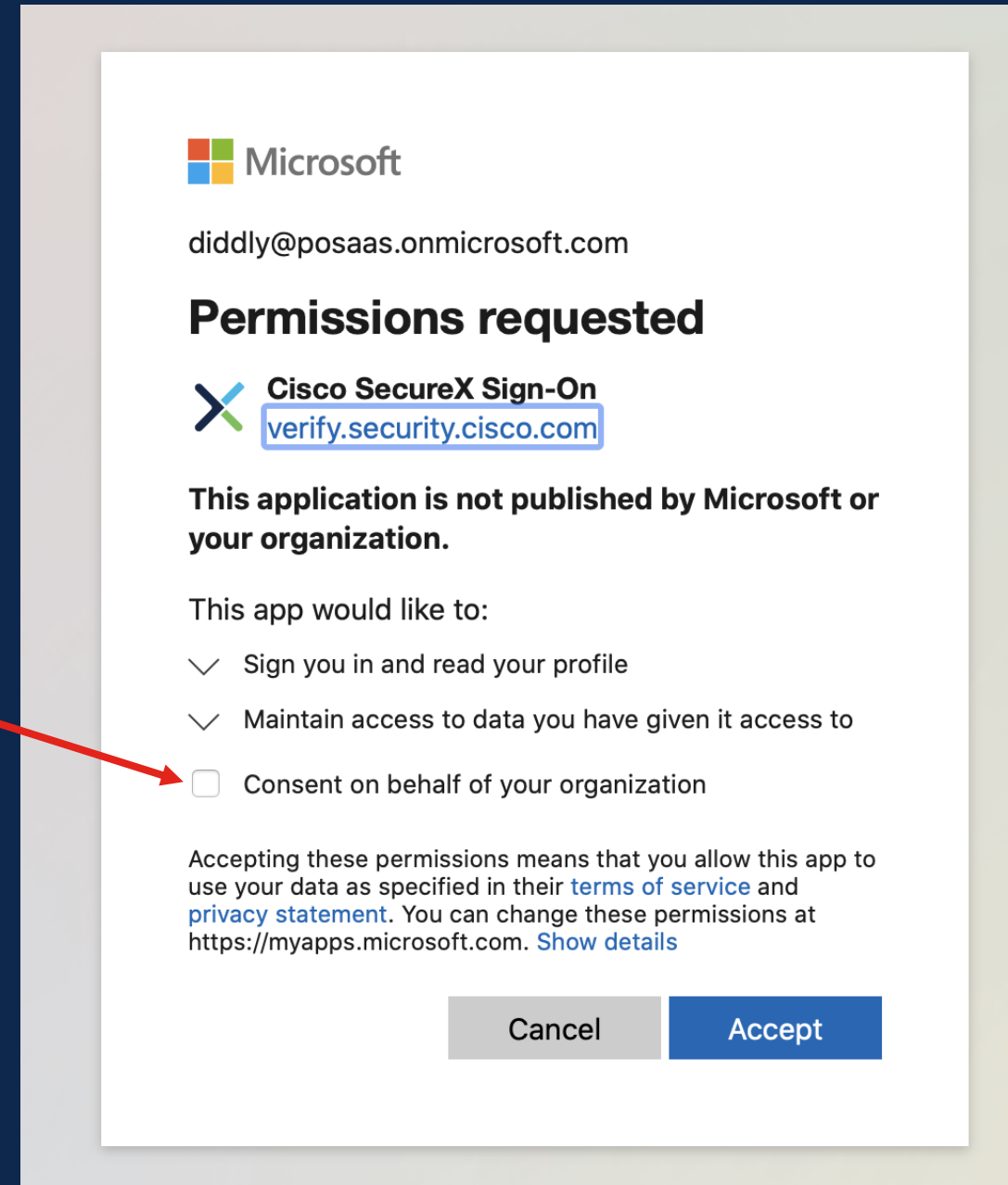


The screenshot displays the Cisco Secure Sign-On interface. At the top center is the Cisco logo. Below it is a circular profile picture of a person. The main heading is "Secure Sign-On". On the left, there is a "Username" field containing "diddly@cisco.com" and a "Remember me" checkbox which is checked. Below these is a "Next" button and a link for "Need help signing in?". In the center, there is an "OR" separator. On the right, there are two sign-in buttons: "Sign in with Cisco.com" and "Sign in with Microsoft". The "Sign in with Microsoft" button is highlighted with a red rectangular border. At the bottom center, there is a link for "Don't have an account? Sign up".

## 2. User receives "Permissions requested"

- Admin can approve themselves and for their org\*
- "Hey admin come sign in and approve this"

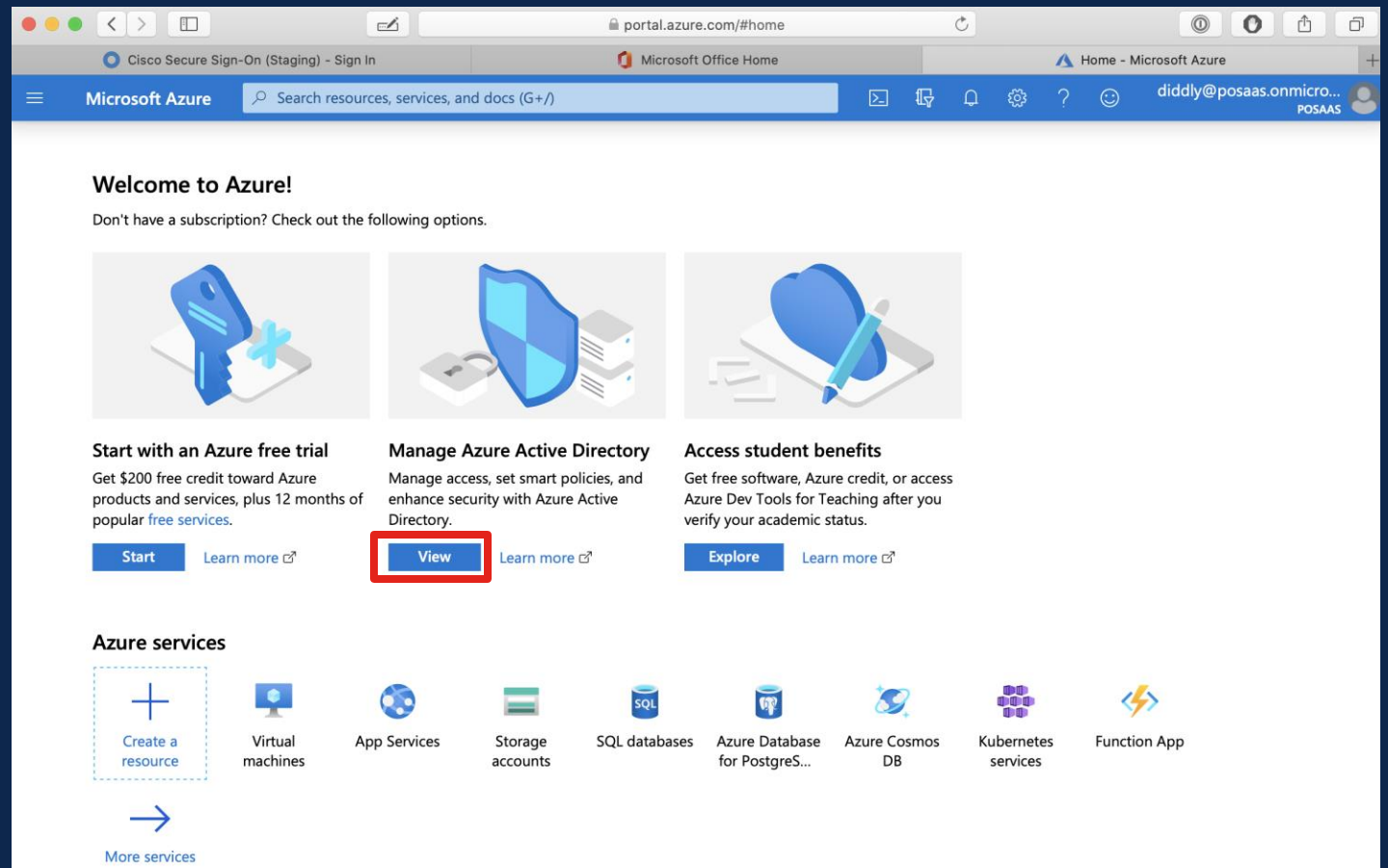
*\* many admins use distinct accounts for their user vs admin role. They must sign in and click this with their admin role/account*



The screenshot shows a Microsoft permissions request dialog. At the top is the Microsoft logo and the email address diddly@posaaS.onmicrosoft.com. The title is "Permissions requested". Below that is the Cisco SecureX Sign-On logo and the URL verify.security.cisco.com. A warning message states: "This application is not published by Microsoft or your organization." The dialog lists permissions: "Sign you in and read your profile" and "Maintain access to data you have given it access to", both with checkmarks. There is an unchecked checkbox for "Consent on behalf of your organization", which is highlighted by a red arrow from the text on the left. At the bottom, there are "Cancel" and "Accept" buttons. A disclaimer at the bottom states: "Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details".

# Alternatively, admin can approve via portal

1. Admin sign into portal.azure.com
2. Manage Azure Active Directory



The screenshot shows the Microsoft Azure portal home page. The browser address bar displays `portal.azure.com/#home`. The page features a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, there is a "Welcome to Azure!" section with a message: "Don't have a subscription? Check out the following options." This section contains three cards:

- Start with an Azure free trial**: "Get \$200 free credit toward Azure products and services, plus 12 months of popular free services." Includes "Start" and "Learn more" buttons.
- Manage Azure Active Directory**: "Manage access, set smart policies, and enhance security with Azure Active Directory." The "View" button is highlighted with a red box. Includes "View" and "Learn more" buttons.
- Access student benefits**: "Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status." Includes "Explore" and "Learn more" buttons.

Below these cards is the "Azure services" section, which includes a "Create a resource" button and a row of service icons: Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, and Function App. A "More services" link is located at the bottom of this section.

# 3. Click Enterprise Applications

The screenshot shows the Microsoft Azure portal interface. The browser address bar displays the URL: `portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade`. The page title is "posaaas | Overview - Microsoft Azure". The user's email address, `diddly@posaaas.onmicro...`, is visible in the top right corner. The main navigation pane on the left lists various management options, with "Enterprise applications" highlighted by a red rectangular box. The main content area shows the "posaaas | Overview" page for the Azure Active Directory tenant. It includes a search bar, a "Switch directory" button, and a "Delete directory" button. A notification banner at the top states: "Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)". The "Overview" section displays the tenant name "posaaas", the domain "posaaas.onmicrosoft.com", and the user's role as "Global administrator and 7 other roles". The Tenant ID is "23b779f1-96d3-4127-943b-433803dc63ad". Below this, there is a "Find" section with a dropdown menu set to "Users" and a search input field. The "Azure AD Connect" section shows the status as "Not enabled" and the last sync as "Sync has never run".

# 4. Click “SecureX Sign-On...”













Home > Enterprise applications | All applications posaaS - Azure Active Directory ×

« [+ New application](#) | [Columns](#) | [Got feedback?](#)

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application Type: Enterprise Applications | Applications status: Any | Application visibility: Any [Apply](#) [Reset](#)

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
 <a href="#">Cisco SecureX Sign-On</a>	<a href="https://sign-on.cisco.com/oauth2/v1/authorize/callback">https://sign-on.cisco.com/oauth2/v1/authorize/callback</a>	42e30b97-a9d0-4e56-a374-d75514bbe...	1c6a068c-97e0-4b30-a5ae-ef613bb972...
 <a href="#">Common Data Service</a>	<a href="http://www.microsoft.com/dynamics/crm">http://www.microsoft.com/dynamics/crm</a>	ce51074a-bc50-4253-b112-6838c88c32...	00000007-0000-0000-c000-0000000000...
 <a href="#">ISE</a>		5c432154-4ba8-419b-8afd-aa03d4423c...	4fed75ce-d888-4936-8a28-8ea4668d8...
 <a href="#">Microsoft Sample Data Packs</a>	<a href="https://developer.microsoft.com/en-us/office">https://developer.microsoft.com/en-us/office</a>	82e23652-c8e9-4f8b-933c-1a74120a8d3f	a1cffbc6-1cb3-44e4-a1d2-cee9cce700f1
 <a href="#">Microsoft Teams</a>		675ab404-f3b8-44a9-be95-ae393a322...	cc15fd57-2c6c-4117-a88c-83b1d56b4b...
 <a href="#">Office 365 Exchange Online</a>	<a href="http://office.microsoft.com/outlook/">http://office.microsoft.com/outlook/</a>	37950df7-61e0-43cc-8c38-dd2a7f6c1894	00000002-0000-0ff1-ce00-0000000000...
 <a href="#">Office 365 Management APIs</a>		5a686df5-c9de-4de2-980a-9fe51edaa4...	c5393580-f805-4401-95e8-94b7a6ef2fc2
 <a href="#">Office 365 SharePoint Online</a>	<a href="http://office.microsoft.com/sharepoint/">http://office.microsoft.com/sharepoint/</a>	fecfc437-1936-4202-b3bc-9d25ad9934...	00000003-0000-0ff1-ce00-0000000000...
 <a href="#">Office 365 Yammer</a>	<a href="https://products.office.com/yammer/">https://products.office.com/yammer/</a>	c6bf0748-b5ae-432a-a3c9-58b7886ed3...	00000005-0000-0ff1-ce00-0000000000...
 <a href="#">Outlook Groups</a>		991787a9-71fd-49fc-bb3b-6f206daf82d3	925eb0d0-da50-4604-a19f-bd8de9147...
 <a href="#">Power BI Service</a>		83546a6f-7765-4108-942b-f223cb5bc8...	00000009-0000-0000-c000-0000000000...
 <a href="#">Skype for Business Online</a>		b6df5330-f0aa-4a01-9769-a08a3cc4152d	00000004-0000-0ff1-ce00-0000000000...

© 2019 Cisco | Troubleshooting + Support

# 5. Assign Group or Users

Home > Enterprise applications | All applications >

## Cisco SecureX Sign-On | Overview

Enterprise Application

- Overview
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Users and groups
  - Provisioning
  - Self-service
- Security
  - Conditional Access
  - Permissions
  - Token encryption
- Activity
  - Sign-ins
  - Usage & insights (Preview)
  - Audit logs
  - Provisioning logs (Preview)
  - Access reviews
- Troubleshooting + Support
  - Virtual assistant (Preview)
  - New support request

### Properties

**Name** ⓘ  
Cisco SecureX Sign-On

**Application ID** ⓘ  
1c6a068c-97e0-4b30-a5ae-e...

**Object ID** ⓘ  
42e30b97-a9d0-4e56-a374-...

### Getting Started

- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Provision User Accounts**  
You'll need to create user accounts in the application  
[Learn more](#)
- 3. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)
- 4. Self service**  
Enable users to request access to the application using their Azure AD credentials  
[Get started](#)

### What's New

- Sign in charts have moved!**  
The new Insights view shows sign in info along with other useful application data. [View insights](#)
- Delete Application has moved to Properties**  
You can now delete your application from the Properties page. [View properties](#)
- Getting started has moved to Overview**  
The Getting Started page has been replaced by the steps above

# Reference Materials

[Configure user consent](#)

[Manage consent requests](#)

[Grant admin consent](#)