

SC-300

Tag 3

# Microsoft Identity and Access Administrator

Guten Morgen !



LP 3

# Implement access management for apps



# Agenda

---

- LP 1 Implement an Identity Management Solution
- LP 2 Implement an Authentication and Access Management Solution
- LP 3 Implement Access Management for Apps
- LP 4 Plan and Implement an Identity Governance Strategy

~~Day~~

Labs

- Skillable (LODS)
- Go Deploy

# Outline

ARM API  
Azure

Damals



UPN

Password

Calendar

App

UPN  
Password

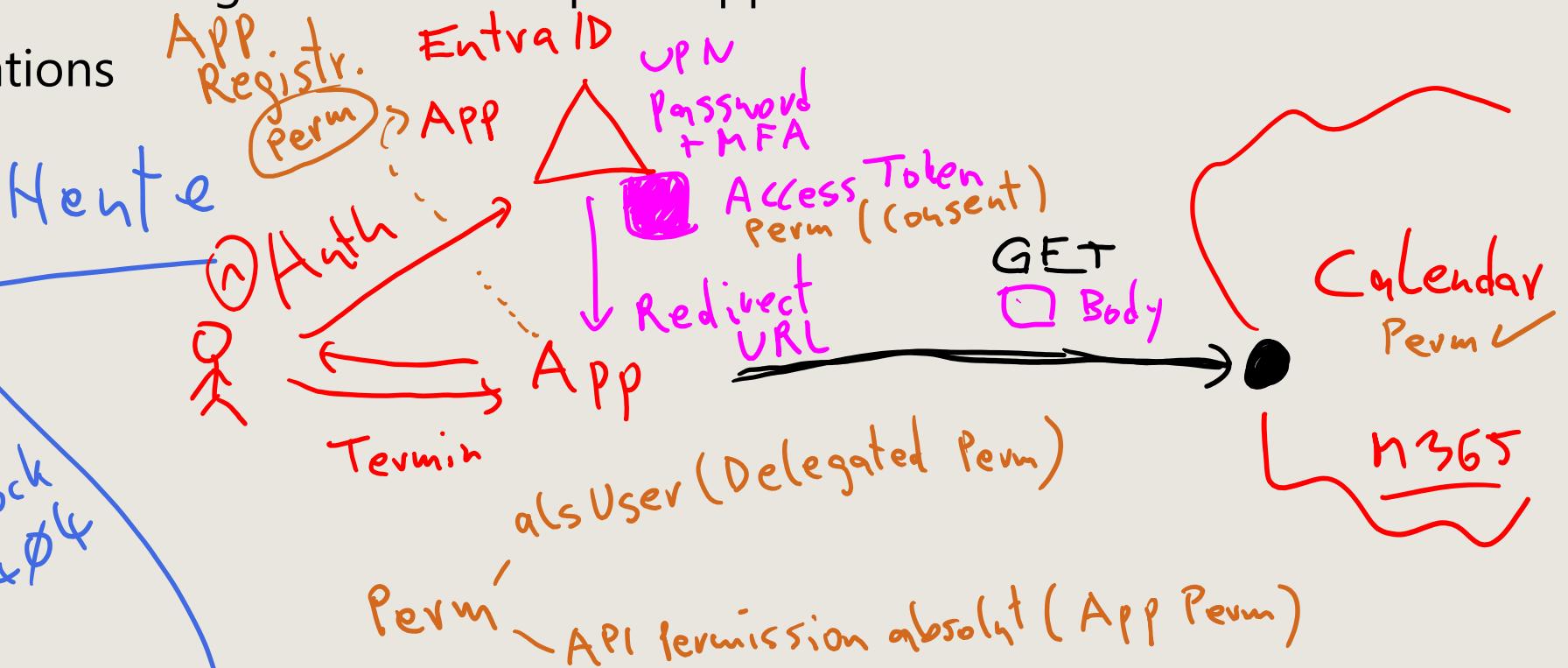
HTTPS  
GET  
POST  
REST API

Microsoft Graph

SaaS

- What is an app?
- Plan and design the integration of enterprise apps for single sign-on (SSO)
- Implement, and monitor the integration of enterprise apps
- Implement app registrations

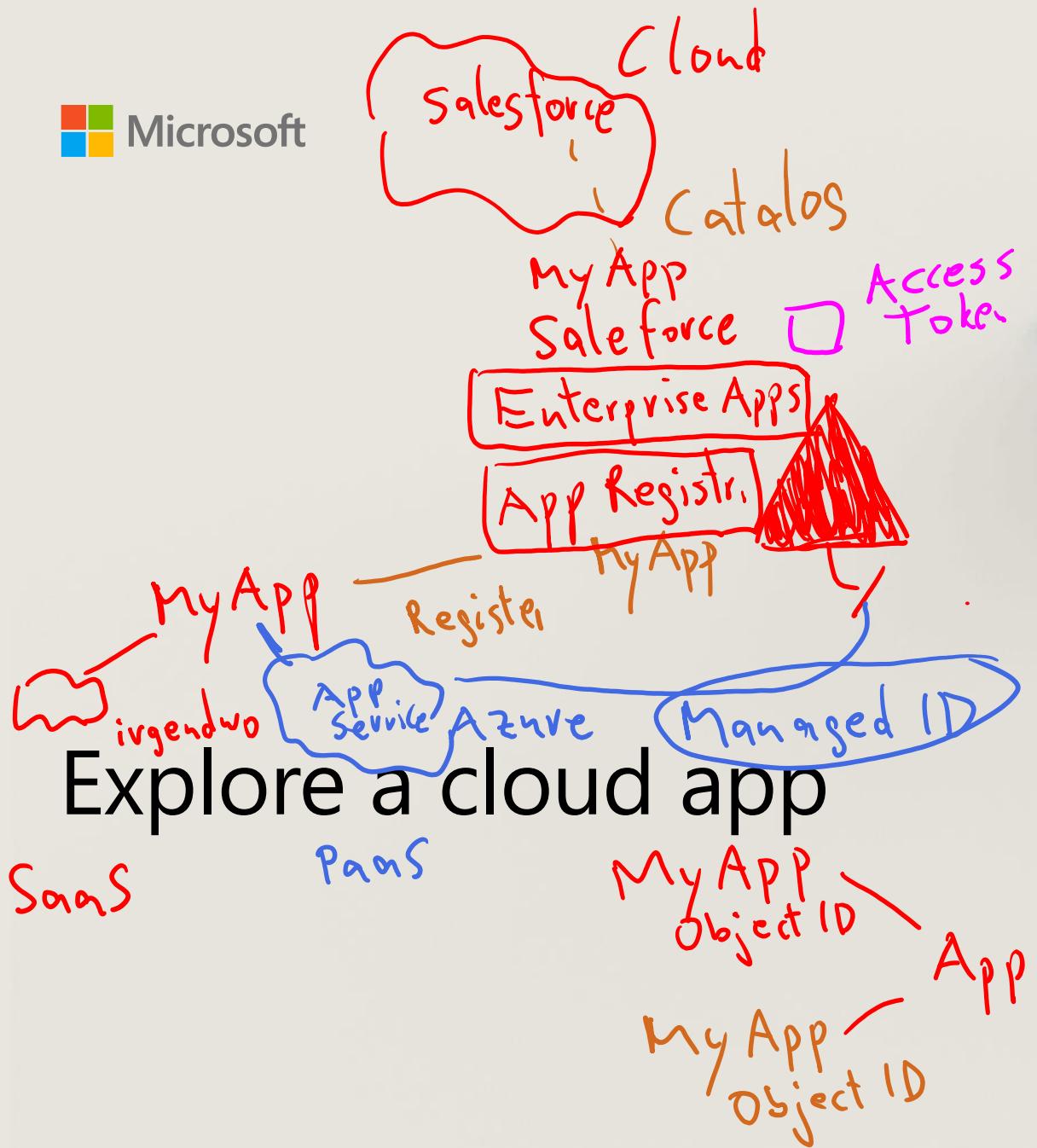
John Savill  
WWW  
1985  
Tim Berners-Lee  
CERN  
U. Stock  
404



# Learning objectives

After completing this module, you will be able to:

- 1** Configure and implement identity solutions for applications in Azure.
- 2** Compare and contrast managed identities and service principals.
- 3** Register and manage both apps and enterprise apps.



# Table of contents

After completing this section, you will be able to:

- 1** Explain the benefits of registering apps in Microsoft Entra ID.
- 2** Compare and contrast single and multitenant apps.
- 3** Describe what happens and the primary settings when an app is registered.
- 4** Describe the relationship between application objects and service principals.



# Benefits of registering an app



Restrict which users and how they log into an application.



Configure the scope permissions and API permissions available to the app.



Configure and store secrets within the Microsoft identity platform.

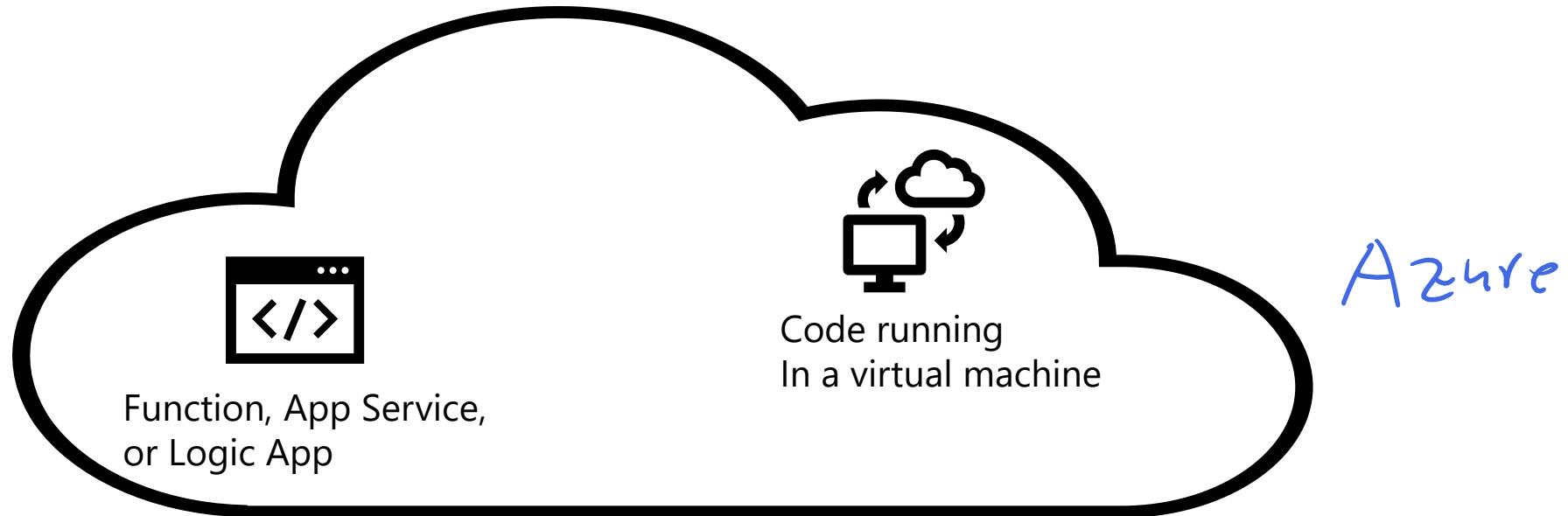


Enable custom branding of the application login.

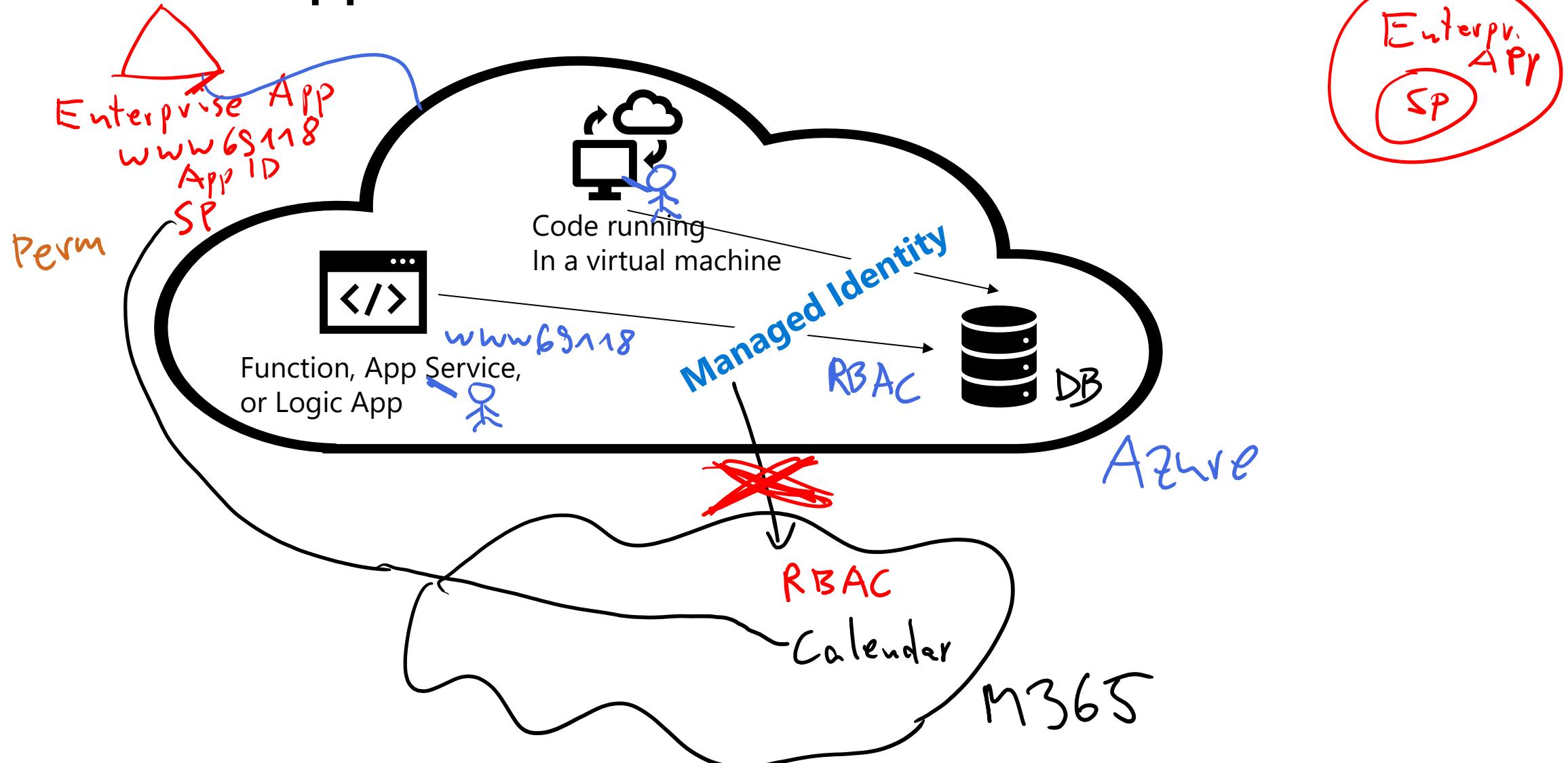
Contoso

# What is an app?

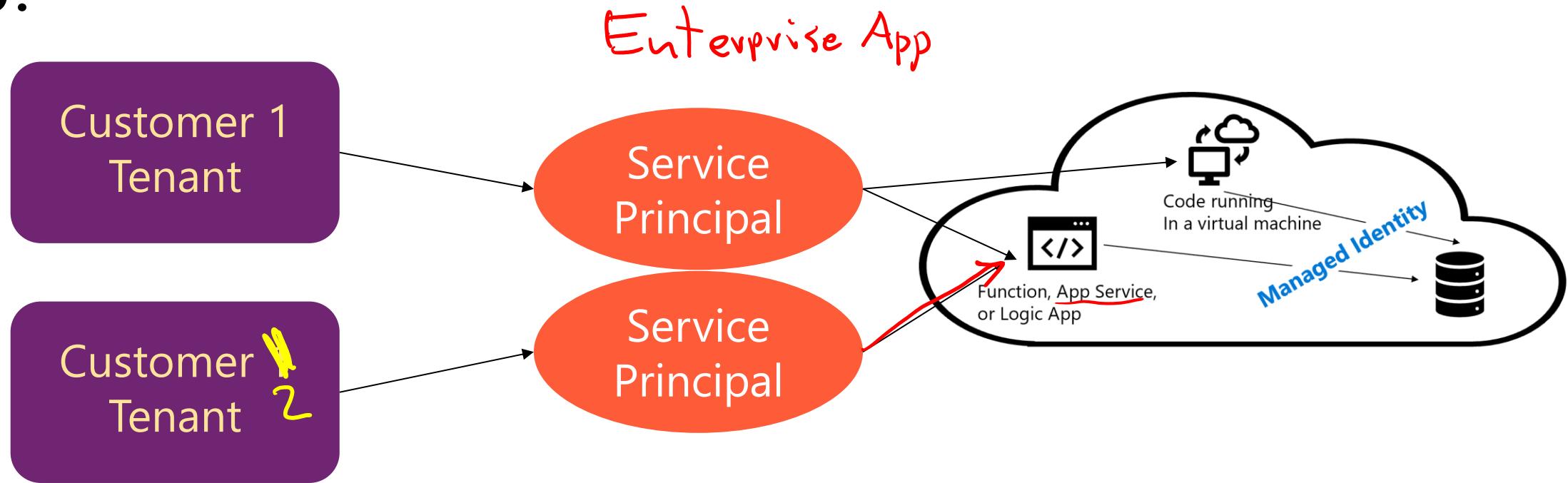
Code  
Entra SDKs



# What if an app needs access to Azure resources?



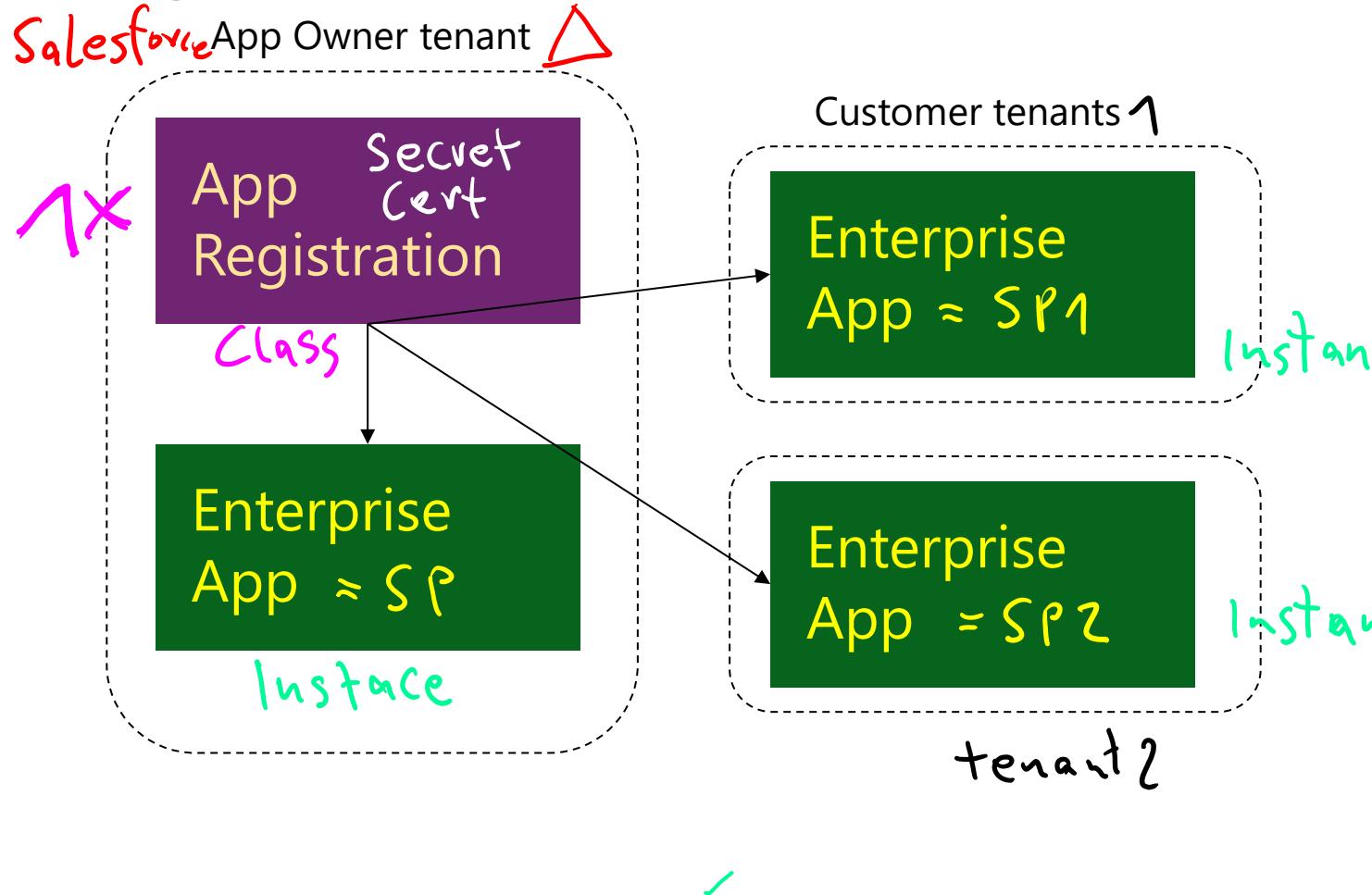
# What if people from other tenants need access to your app?



- Service principals are used:
  - Each tenant registers the app (creates a service principal)
  - Requires a key or certificate for authentication

Git

# Register an App in Microsoft Entra ID



## Global

- Unique application ID
- Redirect URI
- Branding
- API permissions
- Role definitions

## Tenant-specific service principal

- Reference to application
- + unique object ID
  - User / group assignments
  - Role assignments
  - Visibility in portals

# Single tenant versus multitenant apps

Audience	Single or Multi-tenant	Who can sign in
Accounts in this directory only	Single tenant 	All user and guest accounts in your directory.
Accounts in any Microsoft Entra directory	Multi-tenant 	All users and guests with a work or school account from Microsoft can use your application or API.
Accounts in any Microsoft Entra directory and personal Microsoft accounts (such as Skype, Xbox, Outlook.com)	Multitenant and Microsoft Accounts 	All users with a work or school, or personal Microsoft account can use your application or API. Includes schools, businesses using Microsoft 365, and services like Xbox and Skype.

# Create an app registration

## Values needed for app registration

- App name
  - What the user sees
- Account types that can log into the app
  - Single or multitenant
- URI
  - Where application is running after authentication

The screenshot shows the Microsoft Entra admin center interface. The left sidebar navigation includes Home, Favorites, Identity (Overview, Users, Groups, Devices), Applications (Enterprise applications, App registrations, Protection, Identity governance, External Identities, Show more), Protection, Identity governance, Verifiable credentials, Learn & support. The main content area is titled 'Register an application'. It contains fields for 'Name' (with placeholder 'The user-facing display name for this application (this can be changed later)') and 'Supported account types' (radio buttons for 'Accounts in this organizational directory only (qg14 only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'). There is also a 'Help me choose...' link. A 'Redirect URI (optional)' section with a dropdown for 'Select a platform' (e.g. https://example.com/auth) and a note about returning the authentication response. At the bottom, there is a note about agreeing to Microsoft Platform Policies and a large red-bordered 'Register' button.

# Application object versus service Principal

## Application Object

- How the service can issue tokens to access the application
- The resources that the application might need to access
- The actions that the application can take
- Contains the application ID

## Enterprise App Object Service Principal

- A reference back to an application object through the application ID property
- Records of local user and group application role assignments
- Records of local user and admin permissions granted to the application
- Records of local policies including Conditional Access policy
- Records of alternate local settings for an application

# Plan and design the integration of enterprise apps for SSO

# Objectives

- 1** Discover apps by using MDCA or ADFS app report
- 2** Configure app connectors in MDCA
- 3** Design and implement access management for apps
- 4** Design and implement app management roles
- 5** Configure preintegrated (gallery) SaaS apps
- 6** Implement and manage policies for OAuth apps (in MDCA)

Discover apps by using  
MDCA or ADFS app report

# What is CASB and Microsoft Defender for Cloud Apps (MDCA)?

## CASB—Cloud Access Security Broker

A security tool placed between a cloud service (like an app) and the user to interject enterprise security policies before the cloud-based resource is accessed.

## MDCA—Microsoft Defender for Cloud Apps (formerly Cloud App Security)

Microsoft implementation of a CASB service to protect data, services, and applications with enterprise policies. It provides supplemental reporting and analytics services.

# Microsoft Defender for Cloud Apps capabilities

- Shadow IT discovery—find and manage cloud apps
- Information protection—protect information as it travels
- Threat protection—look for unusual behavior
- Compliance assessment—assess against regulatory requirements

# Microsoft Defender for Cloud Apps

## Cloud Access Security Broker (CASB)

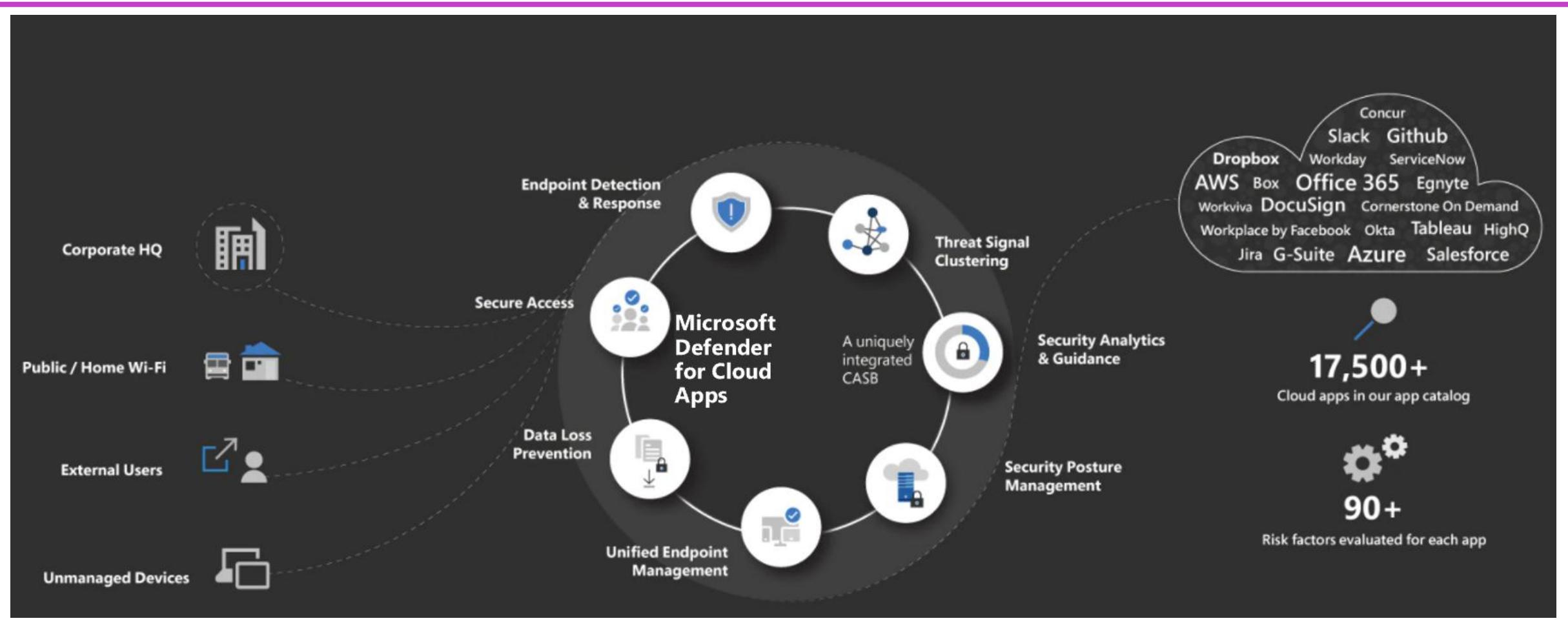
Several different deployment modes:

- Log collection
- API connectors
- Reverse proxy

Providing admins with:

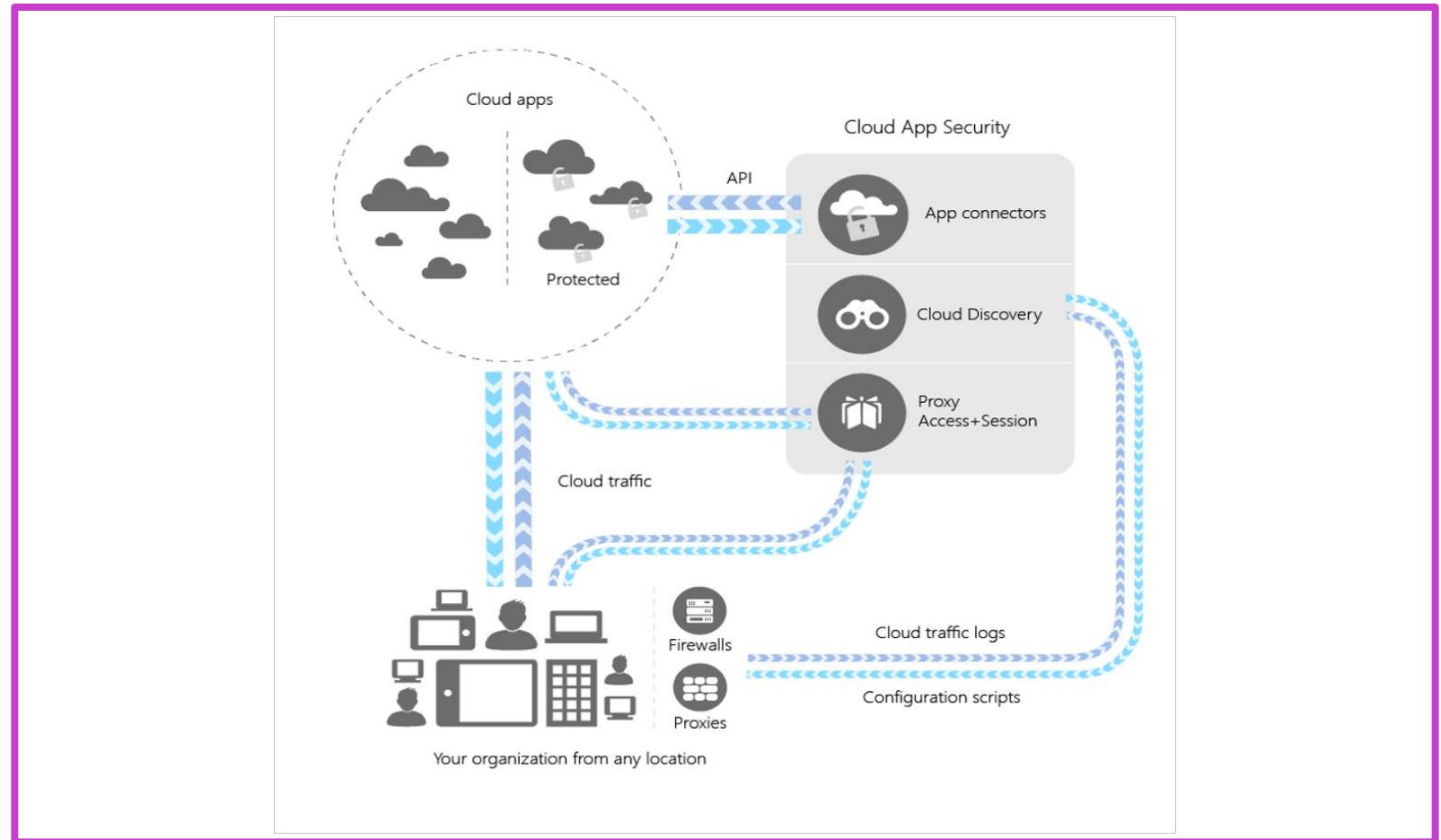
- Rich visibility
- Data control
- Sophisticated analytics
- Identification of cyberthreats

# Microsoft Defender for Cloud Apps—process flow



# Microsoft Defender for Cloud Apps architecture

- **Cloud Discovery**  
Find apps
- **Sanctioning**  
Allow/deny apps
- **Connectors**  
Extend protection into  
the app  
with APIs
- **Conditional Access –**  
Set access requirements
- **Policy control –** Define  
user behavior with apps



# Set up Cloud Discovery with Microsoft Defender for Cloud Apps

Cloud Discovery

Cloud Discovery enables you to:

- Gain continuous visibility over Shadow IT
- Analyze cloud app usage
- Dive into a specific app, user or IP address
- Get notifications about new discovered apps

Create a new report    Configure automatic upload    View sample report

The screenshot shows the Microsoft Defender for Cloud Apps interface. On the left, there's a navigation sidebar with options like Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery (which is selected), Cloud app catalog, OAuth apps, Activity log, Governance log, Policies, and Reports. The main area is titled "Cloud Discovery" and features an illustration of a person holding a smartphone with a cloud icon on the screen, standing next to a large blue puzzle piece. Below the illustration, it says "Cloud Discovery enables you to:" followed by a list of four points. At the bottom, there are three buttons: "Create a new report", "Configure automatic upload", and "View sample report". To the right of these buttons is a screenshot of the "Cloud App Security" dashboard. The dashboard has a header with "Cloud App Security", "Discover", "Control", and "Alerts". It shows a summary section with metrics: 128 Apps, 5875 Users, 3861 IPs, and 9.5 TB Traffic. Below this are sections for "App categories" (showing a bar chart for Collaboration, Cloud storage, Webmail, Social network, and Online working) and "Risk levels" (showing a donut chart with 890 users at high risk). There are also buttons for "Cloud Discovery open alerts", "Create policy", "New app alerts", and "Get suspicious usage alerts".

# MDCA—discovering apps with Cloud Discovery

## Cloud Discovery

With the new application inventory, you can discover and manage all SaaS and related OAuth apps from a single location. [View application inventory](#)

Updated on May 5, 2025, 12:57 PM

Dashboard    Discovered apps    Discovered resources    IP addresses    Users    Devices

**Microsoft Sentinel**  
Discover and respond to threats with your SIEM.

Devices: 25 | Traffic: 24.5 GB (↑ 8.0 GB, ↓ 16.5 GB)

App categories: 1-5 of 34 | Traffic: 24.5 GB (↑ 8.0 GB, ↓ 16.5 GB)

Category	Traffic
Security	8.1 GB
Content management	5.8 GB
Collaboration	5.7 GB
Online meetings	1.5 GB
IT services	1.4 GB

Risk levels: All categories | Traffic

Configure score metric

Top entities: User | Total

User	Total
dbe303@woodgrove.ms	2.8 GB
veko65@woodgrove.ms	2.8 GB
joeyc@woodgrove.ms	2.6 GB
SRFC-LPTP2-BLCK/R	2.5 GB
alkh68@woodgrove.ms	2.2 GB

View all users

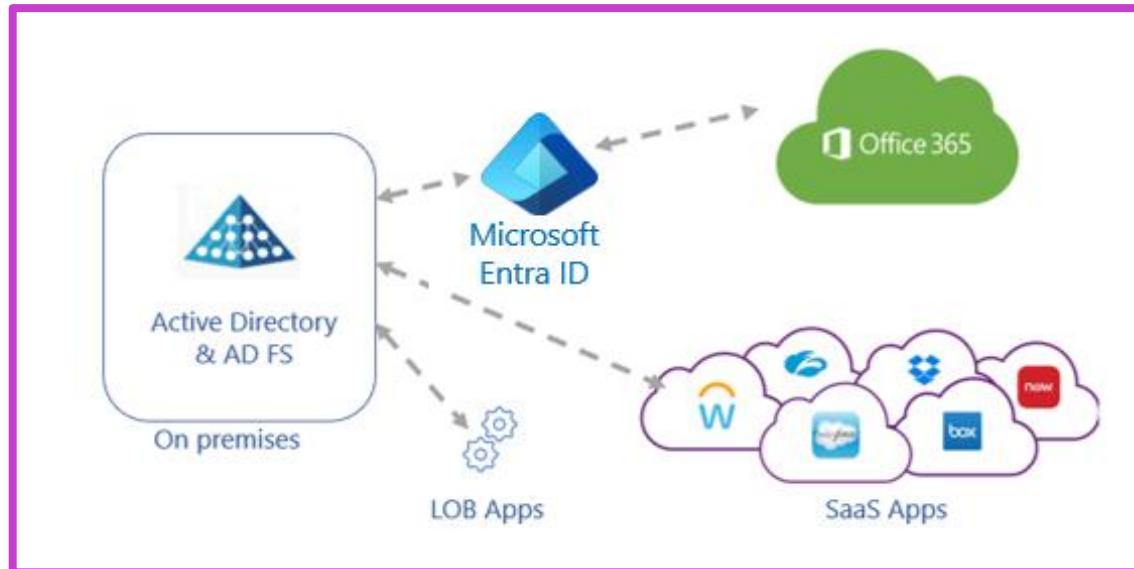
Discovered apps: 1-15 of 99 | All categories | Traffic

App	Traffic
Microsoft SharePoint Online	5.6 GB
Microsoft Teams	1.5 GB
Microsoft OneDrive for Business	595 MB
Microsoft Exchange Online	121 MB

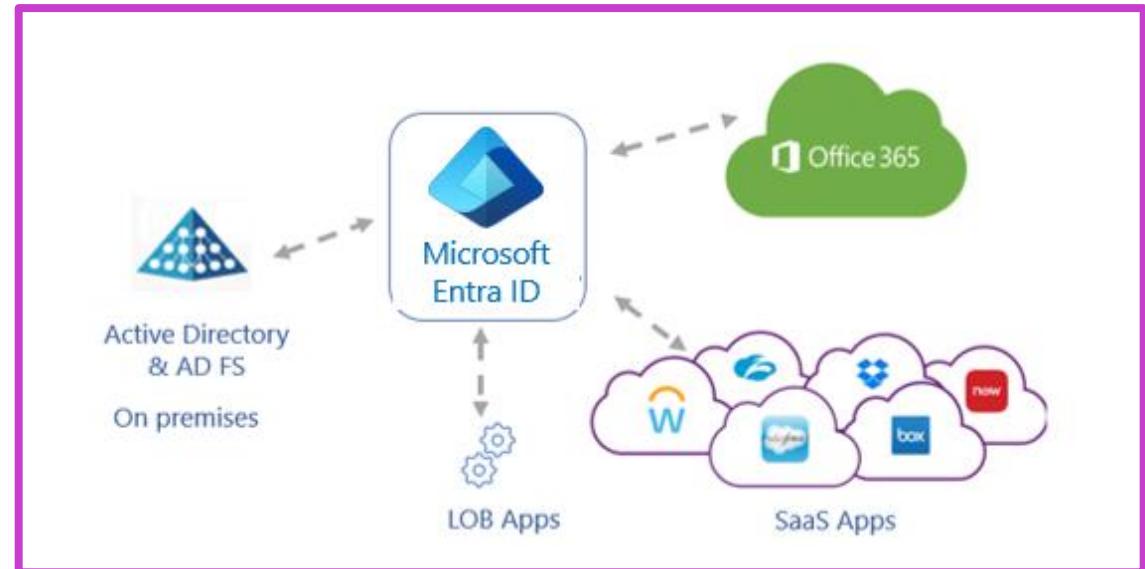
Apps headquarters location: All categories

© Copyright Microsoft Corporation. All rights reserved.

# Active Directory Federation Services



AD FS extends single sign-on (SSO) functionality between trusted business partners without requiring users to sign in separately to each application.



To increase application security, your goal is to have a single set of access controls and policies across your on-premises and cloud environments.

# Discover apps that can be migrated

There are two types of applications to migrate

- SaaS applications—procured by the organization
- Line-of-business applications—developed by the organization

The screenshot shows a Microsoft Entra interface titled "Usage & insights | AD FS application migration". On the left, there's a sidebar with options: "Microsoft Entra application activity (Preview)", "AD FS application migration" (which is selected and highlighted in grey), "Service principal sign-in activity (Preview)", and "Application credential activity (Preview)". The main area has a "Date range" dropdown set to "30 days". Below that is a table titled "Application Identifier" with columns for the identifier and "Unique User Count". The data is as follows:

Application Identifier	Unique User Count
CL clearforce_sp_ms	17
CV cvent	6
FI financialknowledge.net	26
GE getabstract	79
OA http://identity.office.net	31
AR http://mssource.sourcing.ariba.com	32
WS http://nebulaservices/tenantsite	31
EB http://shibboleth.ebscohost.com	1

# Configure connectors to apps in MDCA

# What is an app connector in Defender for Cloud Apps?

Capability	Apps with MDCA connectors
Connect to API provided by the app creator	
Enables greater visibility into the apps	
All communication over secure HTTPS	
<b>Common connector API limitations:</b> <ul data-bbox="166 846 627 1139" style="list-style-type: none"><li>• Throttling</li><li>• API limits</li><li>• Dynamic time-shifting</li><li>• API windows</li></ul>	<b>Connectors:</b> <ul data-bbox="1472 529 1881 1225" style="list-style-type: none"><li>• Atlassian</li><li>• Azure</li><li>• AWS</li><li>• Box</li><li>• DocuSign</li><li>• Dropbox</li><li>• GitHub</li><li>• Google Workspace</li><li>• Many others</li></ul>
Services vary by app	

# How app connectors work in MDCA

Defender for Cloud Apps is deployed with system admin privileges to allow full access to all objects in your environment.

The app connector flow is as follows:

- Defender for Cloud Apps scans and saves authentication permissions.
- Defender for Cloud Apps requests the user list. The first time the request is done, it may take some time until the scan completes. After the user scan is over, Defender for Cloud Apps moves on to activities and files. As soon as the scan starts, some activities will be available in Defender for Cloud Apps.
- After completion of the user request, Defender for Cloud Apps periodically scans users, groups, activities, and files. All activities will be available after the first full scan.

# Common services offered by app connector

Connections may take some time depending on the size of the tenant, the number of users, and the size and number of files that need to be scanned. Depending on the app to which you're connecting, API connection enables the following items:

- Account information—visibility into users, accounts, profile information, status (suspended, active, disabled) groups, and privileges.
- Audit trail—visibility into user activities, admin activities, sign-in activities.
- Account governance—ability to suspend users, revoke passwords, and so on.
- App permissions—visibility into issued tokens and their permissions.
- App permission governance—ability to remove tokens.
- Data scan—scanning of unstructured data using two processes—periodically (every 12 hours) and in real-time scan (triggered each time a change is detected).
- Data governance—ability to quarantine files, including files in trash, and overwrite files.

# Implement and manage policies for OAuth apps

# Create a new OAuth app policy

1. Launch Microsoft Defender for Cloud Apps at <https://security.microsoft.com>.
2. Under Cloud Apps, select OAuth apps.
3. Filter the apps according to your needs.
  - For example, you can view all apps that request Permission to Modify calendars in your mailbox.
4. Select the New policy from search button.

The screenshot shows the Microsoft Defender for Cloud Apps interface. On the left, there's a sidebar with various options like Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps (which is highlighted with a red box), Files, Activity log, Governance log, Policies, and Reports. The main area is titled "Manage OAuth apps" and contains a table of OAuth applications. The table has columns for Name, Authorized by, Permission level, and Last authorized. There are buttons for Bulk selection, New policy from search, and Export. The table data is as follows:

Name	Authorized by	Permission level	Last authorized
CDX MS Cloud App Security Demo	1 user	High	May 7, 2022, 2:17 AM
dxprovisioning-yammer-apiauth	shield icon	Medium	May 6, 2022, 9:24 AM
dxprovisioning-worker-app	shield icon	High	May 6, 2022, 9:36 PM
dxprovisioning-graphapi-client	shield icon	High	May 6, 2022, 8:12 AM
dxprovisioning-worker-mfa	shield icon	Medium	May 6, 2022, 8:12 AM
MOD Demo Platform UnifiedApiConsumer	shield icon	High	May 6, 2022, 8:12 AM

# Design and implement access management for apps

# Microsoft Entra ID—enterprise applications

Microsoft Entra ID → enterprise applications

Gallery of thousands of preintegrated applications

- Many of the applications your organization uses are already in the gallery
- Add your own business apps

After an application is added to your Microsoft Entra tenant, you can:

- Configure properties for the app
- Manage user access to the app with a Conditional Access policy
- Configure single sign-on

# Exercise: Implement access management for apps

Add an app to your Microsoft Entra tenant:

Add an Enterprise app and assign your administrator account



[Launch this Exercise in GitHub](#)

**Enterprise applications | All applications**  
Microsoft Entra ID for workforce

[+ New application](#) Refresh Download (Export) Preview info

Search by application name or object ID Application type == **Enterprise**

12 applications found

Name	Object ID	Application ID
AA	AADClaimsXRay	

# Design and implement app management roles

# Delegate application register and management



By restricting who can register applications and manage them

---



By assigning one or more owners to an application

---



By assigning a built-in administrative role that grants access to manage configuration in Microsoft Entra ID for all applications

---



By creating a custom role defining specific permissions, and assigning it

# Built in admin application roles

## Application administrator

Includes the ability to manage all aspects of enterprise applications; including registrations and application proxy settings.

## Cloud application administrator

Includes the ability to manage most aspects of enterprise applications, but **excludes the ability to manage application proxy settings**.

# Exercise: Create a new custom role to grant access to manage app registrations

A custom role can be assigned at organization-wide scope or at the scope of a single Microsoft Entra ID object.

Create a new custom role that can be used to grant access to manage app registrations.



[Launch this Exercise in GitHub](#)

**Roles and administrators | All roles**  
Microsoft Entra ID for workforce

+ New custom role    Delete custom role    Download assignments    I

**i** Get just-in-time access to a role when you need it using PIM. Learn more about PIM

**i** **Your Role:** Global Administrator and 2 other roles

**Administrative roles**  
Administrative roles are used for granting access for privileged actions in Microsoft Entra ID, such as granting access to manage other parts of Microsoft Entra ID not related to application registrations.

[Learn more about Microsoft Entra ID role-based access control](#)

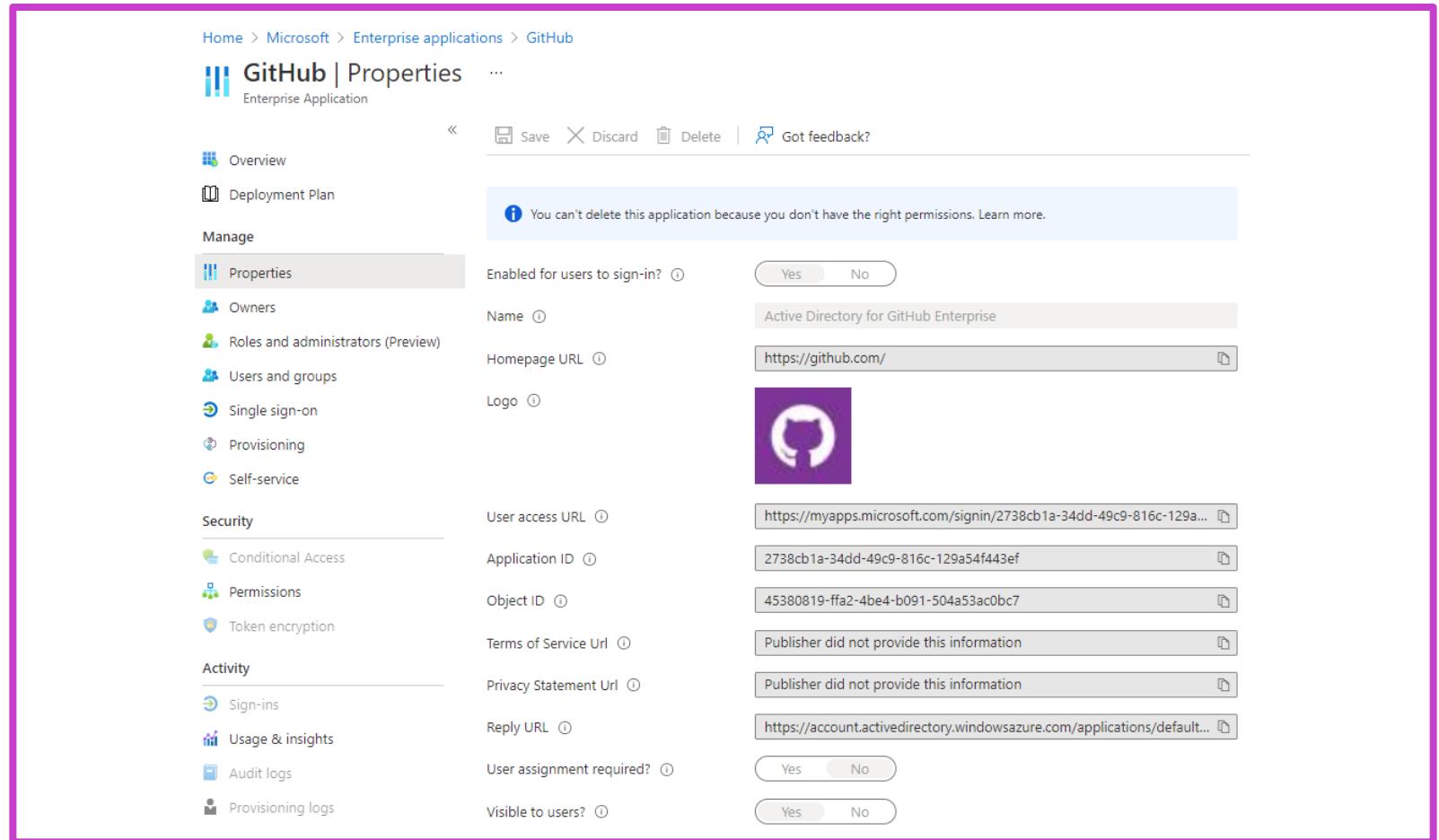
Search by name or description    Add filters

Role	Description
<input type="checkbox"/> Application Administrator	Can create and...
<input type="checkbox"/> Application Developer	Can create app...

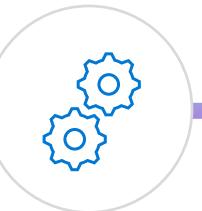
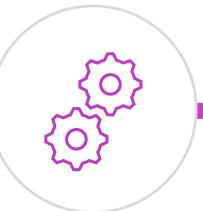
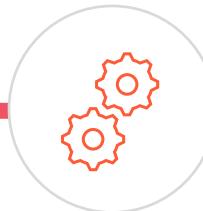
# Configure preintegrated (gallery) SaaS apps

# Enterprise application properties

- Give the application a name
- Pick the URL that opens for users
- Name/Homepage URL
- ApplicationID/ObjectID
- Terms of Service/Privacy Statement



# Configure app properties



Enabled for users  
to sign in?

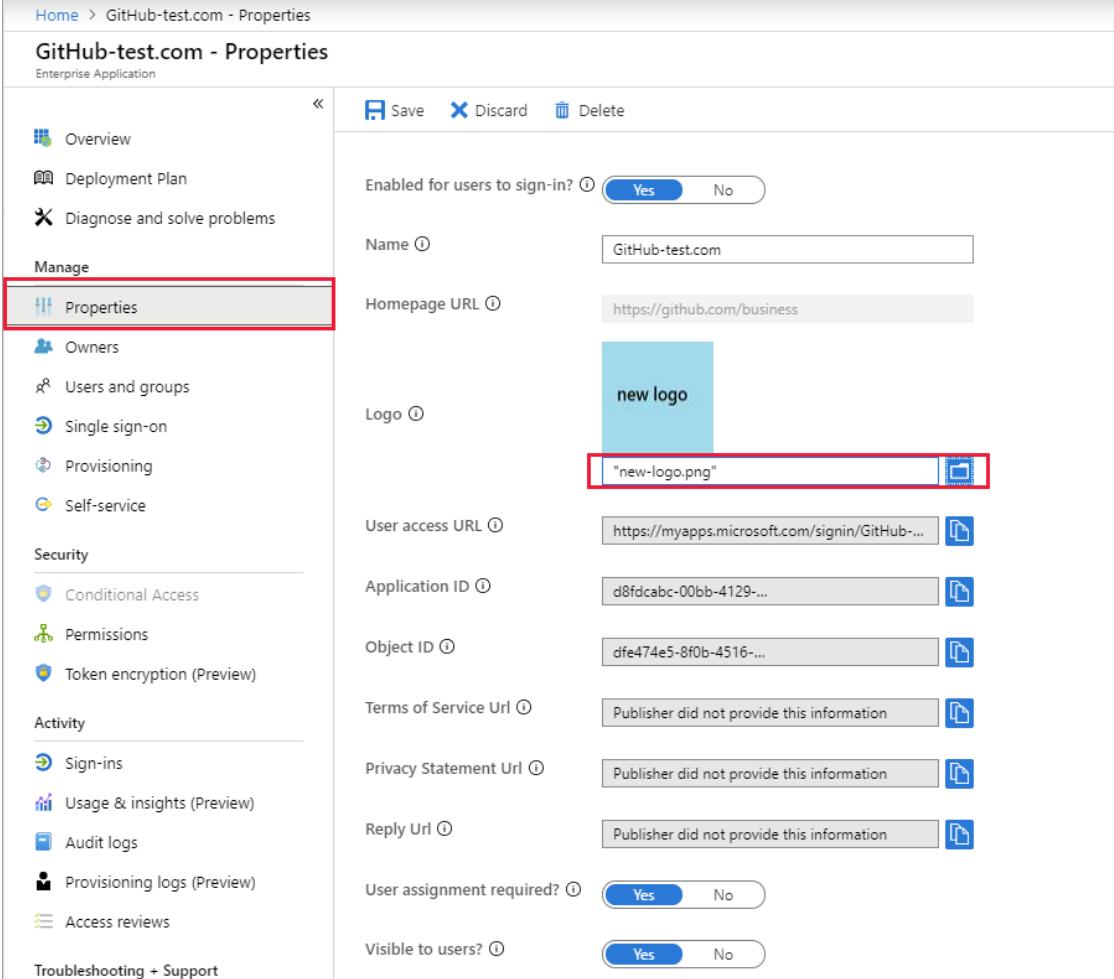
User assignment required?

Visible to users?

*MyApps.microsoft.com*

Enabled for users to sign in?	User assignment required?	Visible to users?	Behavior for users who have either been assigned to the app or not.
Yes	Yes	Yes	<ul style="list-style-type: none"><li>Assigned users can see the app and sign in.</li><li>Unassigned users cannot see the app and cannot sign in.</li></ul>
Yes	Yes	No	<ul style="list-style-type: none"><li>Assigned users cannot see the app but they can sign in.</li><li>Unassigned users cannot see the app and cannot sign in.</li></ul>
Yes	No	Yes	<ul style="list-style-type: none"><li>Assigned users can see the app and sign in.</li><li>Unassigned users cannot see the app but can sign in.</li></ul>

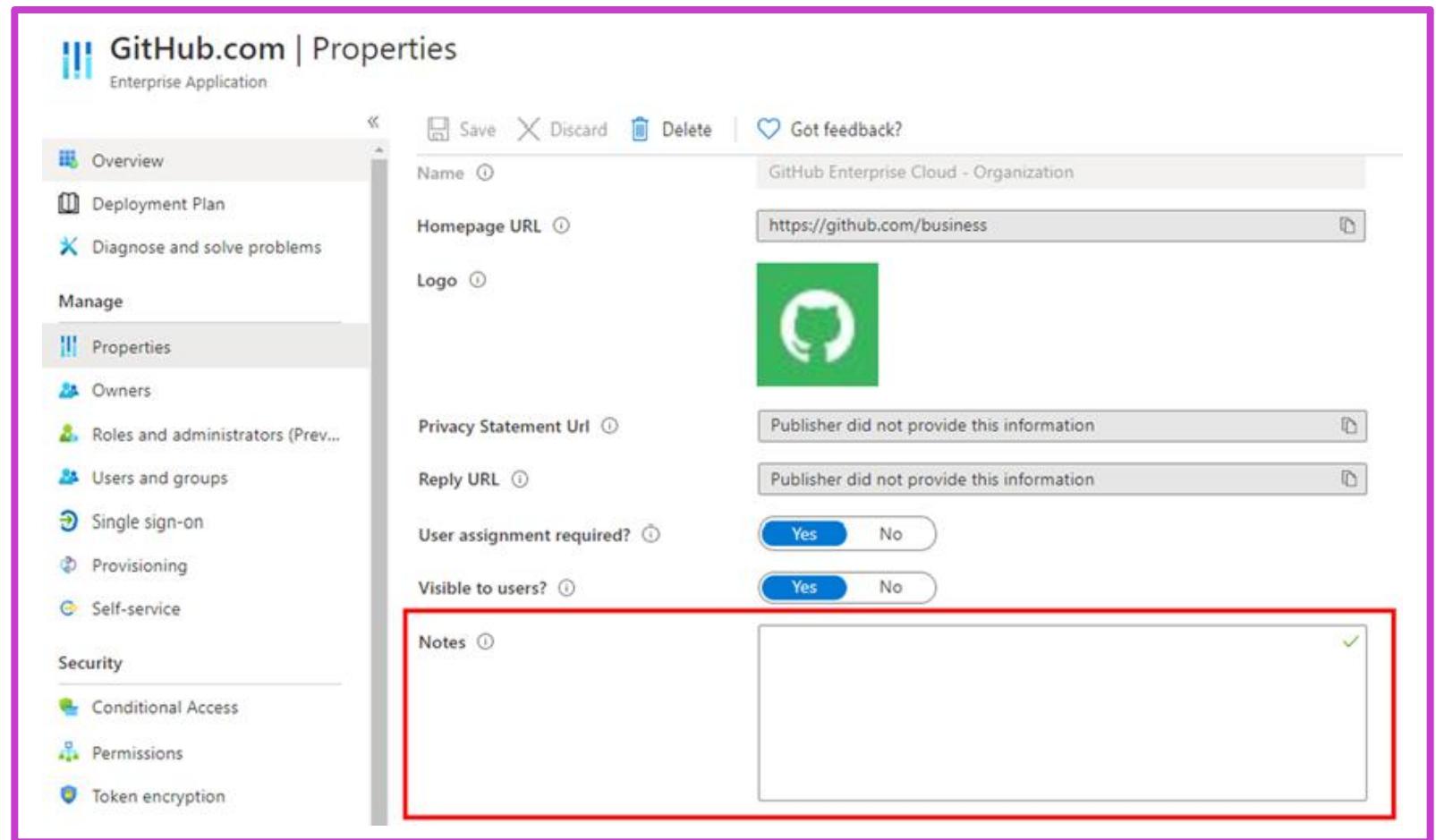
# Custom logo



The screenshot shows the 'Properties' page for an enterprise application named 'GitHub-test.com'. The left sidebar lists various management sections: Overview, Deployment Plan, Diagnose and solve problems, Manage (with Properties selected), Owners, Users and groups, Single sign-on, Provisioning, Self-service, Security, Conditional Access, Permissions, Token encryption (Preview), Activity, Sign-ins, Usage & insights (Preview), Audit logs, Provisioning logs (Preview), Access reviews, and Troubleshooting + Support. The main right pane displays settings for the application, including 'Enabled for users to sign-in?' (Yes), 'Name' (GitHub-test.com), 'Homepage URL' (https://github.com/business), 'Logo' (placeholder image labeled 'new logo'), 'User access URL' (https://myapps.microsoft.com/signin/GitHub...), 'Application ID' (d8fdcabc-00bb-4129...), 'Object ID' (dfe474e5-8f0b-4516...), 'Terms of Service Url' (Publisher did not provide this information), 'Privacy Statement Url' (Publisher did not provide this information), 'Reply Url' (Publisher did not provide this information), 'User assignment required?' (Yes), and 'Visible to users?' (Yes). The 'Logo' field and its corresponding file path 'new-logo.png' are both highlighted with red boxes.

# Add notes

Add any information that is relevant for the management of the application



# Summary



## In this section, you learned how to:

- Discover apps by using MDCA or ADFS app report.
- Design and implement access management for apps.
- Design and implement app management roles.
- Configure preintegrated (gallery) SaaS apps.

# Implement and monitor the integration of enterprise apps for SSO

# Learning objectives

- 1 Implement token customizations
- 2 Implement and configure consent settings
- 3 Integrate on-premises apps by using Microsoft Entra application proxy
- 4 Integrate custom SaaS apps for SSO
- 5 Implement application user provisioning
- 6 Monitor and audit access/sign-on to Microsoft Entra ID integrated enterprise applications
- 7 Create and manage application collections (in My Apps)

# Implement token customizations

# Token configuration – claims – SAML-based SSO

The screenshot shows the Azure portal interface for managing app registrations. On the left, the navigation menu includes 'Home', 'App registrations', 'GitHub.com | Token configuration' (selected), 'Overview', 'Quickstart', 'Manage' (selected), 'Branding', 'Authentication', 'Certificates & secrets', 'Token configuration' (selected), 'API permissions', 'Expose an API', 'Owners', 'Roles and administrators (Pr...', 'Manifest', 'Support + Troubleshooting', and 'Troubleshooting'. The main content area displays the 'Optional claims' section under 'Token configuration'. It shows a table with columns 'Claim ↑', 'Description', and a '+' button to add new claims. A modal window titled 'Add optional claim' is open, showing a list of available claims categorized by token type: 'ID' (selected), 'Access', and 'SAML'. The 'ID' category contains the following claims:

Claim	Description
acct	User's account status in tenant
auth_time	Time when the user last authenticated; See OpenID Con...
ctry	User's country
email	The addressable email for this user, if the user has one
enfpolids	Enforced policy IDs; a list of the policy IDs that were eva...
family_name	Provides the last name, surname, or family name of the ...
fwd	IP address
given_name	Provides the first or "given" name of the user, as set on ...
home_oid	For guest users, the object ID of the user in the user's h...

At the bottom of the modal are 'Add' and 'Cancel' buttons.

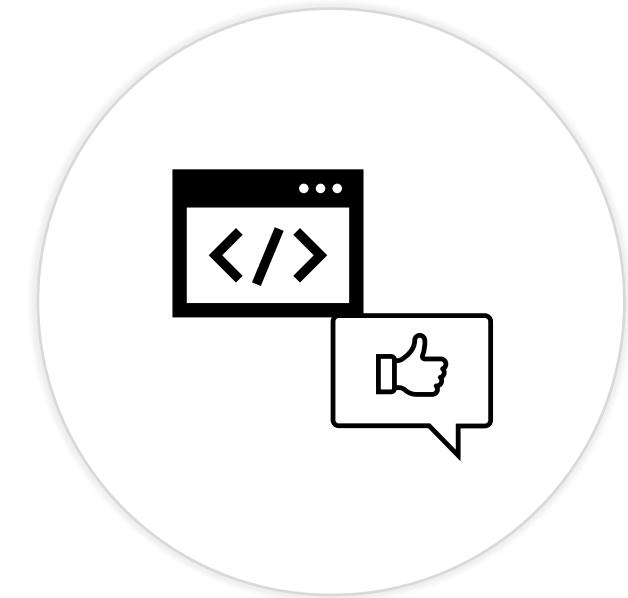
# Implement and configure consent settings

# Why is consent important?

A user or admin must grant permissions to an app before it can access company data.

Users can allow apps access to specific information, like a mailbox, but not access to organization servers.

Users may not think through ramifications of granting access; they just want to use an app to do a task



# What are Consent Settings?

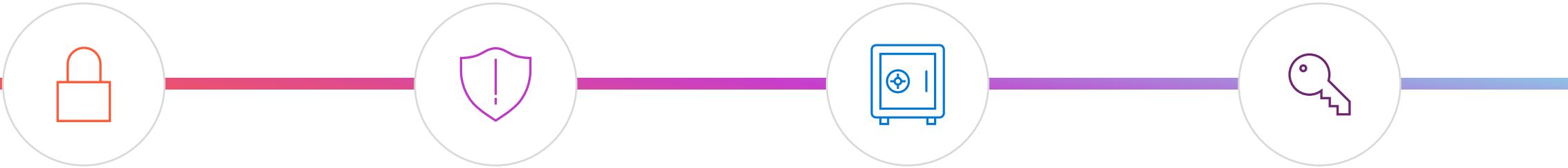
## User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- Do not allow user consent  
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)  
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps  
All users can consent for any app to access the organization's data.

- Before an application can access the organization's data, a user must grant the application permissions to do so
- All users can consent to applications for permissions that do not require administrator consent
- By allowing users to grant apps access to data, users can acquire useful applications and be productive

# User consent settings



## Disable user consent

Users cannot grant permissions to applications. Requires an admin to grant.

## Users can consent to apps from verified publishers

Users can only consent to apps that were published by a verified publisher.

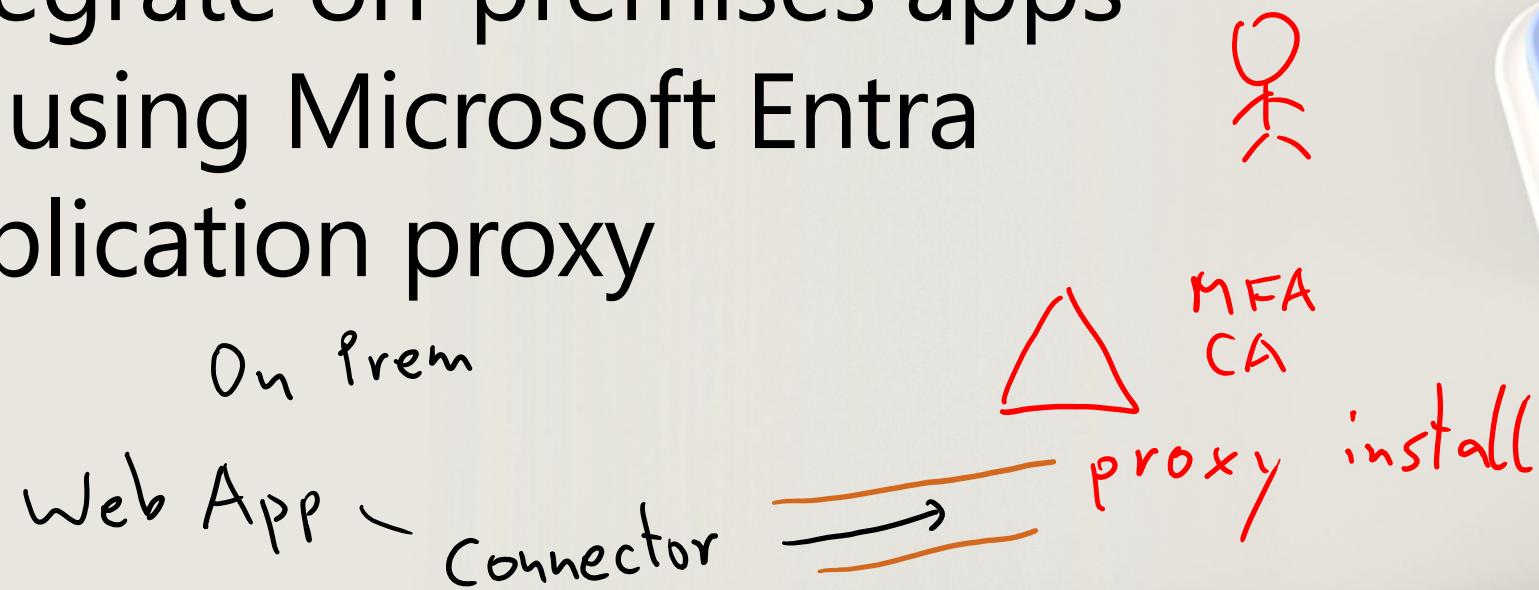
## Users can consent to all apps

Users can consent to any permission.

## Custom app consent policy

Users can consent to custom app consent policies.

# Integrate on-premises apps by using Microsoft Entra application proxy



# What is Application Proxy?

A feature to allow users to access on-premises application.

Proxy service runs in the cloud and has an App Proxy connector running on-premises.

Securely passes sign-on tokens from Microsoft Entra ID to the application.



# Value of Application Proxy

**Protocol translation to/from modern authentication**

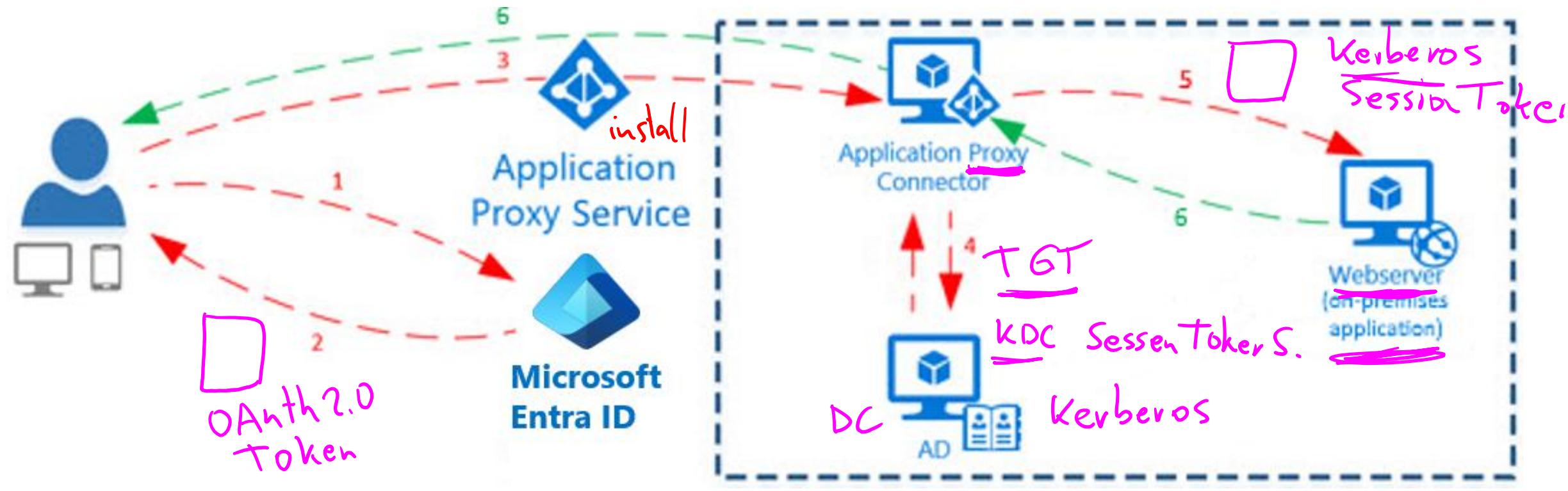
Example: Convert Kerberos token to a modern auth token

**Use seamless single sign-on to remove user action to log in multiple times**

**Allows apps to stay on-premises (for whatever reason), but still be securely available to the user**



# Application Proxy



Application Proxy is a feature of Microsoft Entra ID that enables users to access on-premises web applications from a remote client.

Constrained deleg.

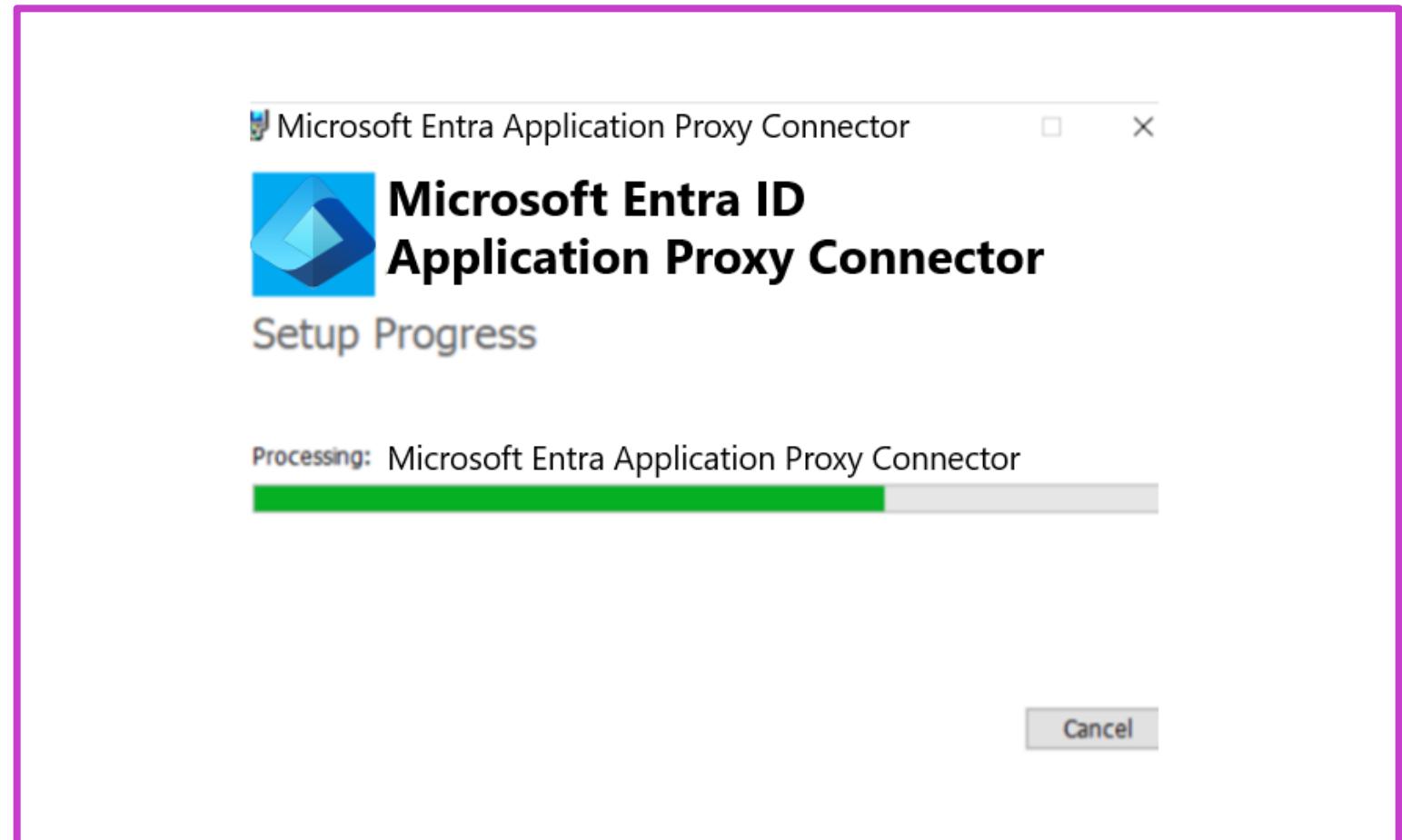
# Exercise: Add an on-premises application for remote access through Application Proxy in Microsoft Entra ID

## Interactive guide

Enable integrated windows authentication to on-premises applications with Microsoft Entra application proxy.



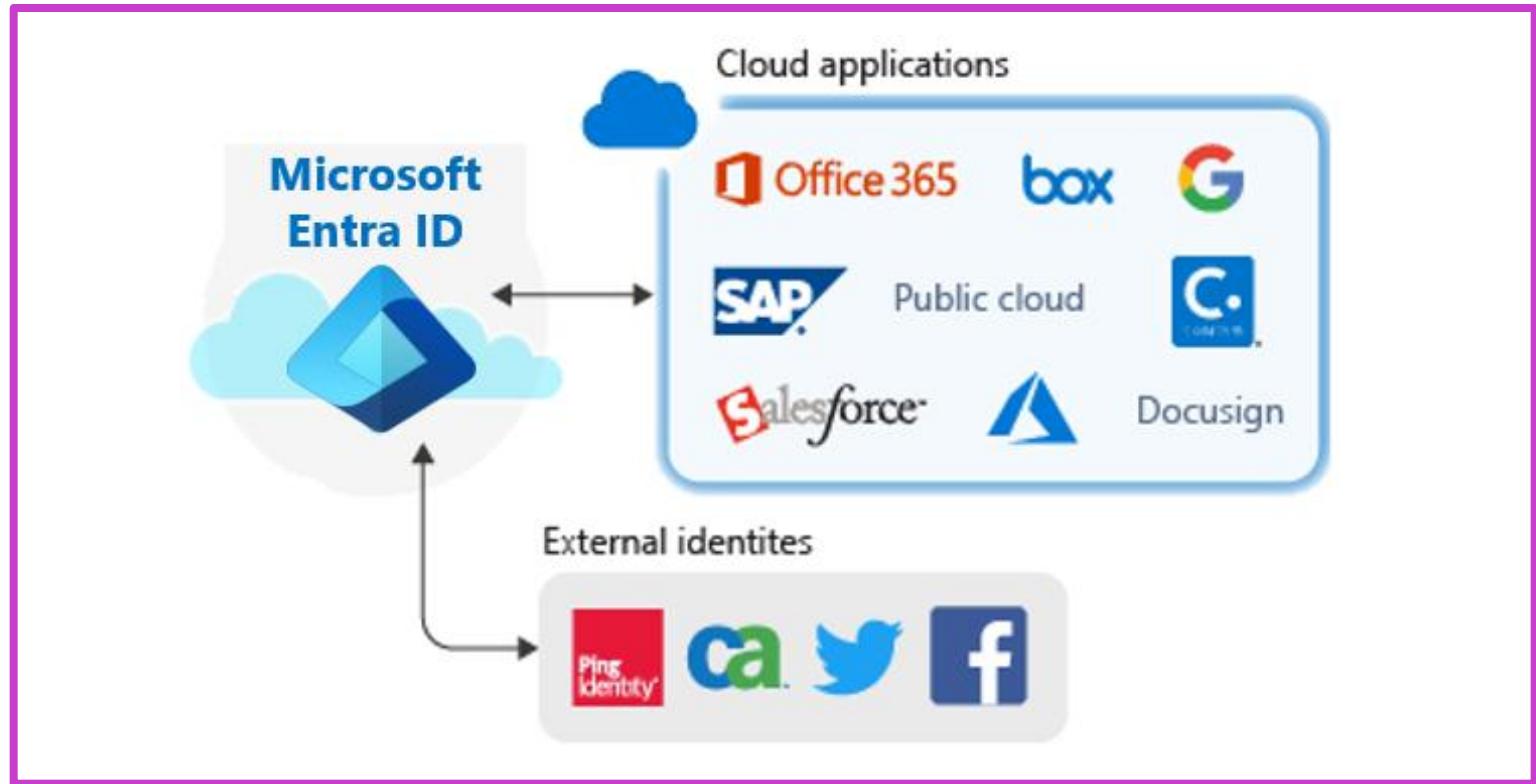
[Visit this  
interactive guide  
in Microsoft Learn](#)



# Integrate custom SaaS apps for SSO

# SSO for SaaS apps

- You can use Microsoft Entra ID as your identity system for just about any app. Many apps are already preconfigured and can be set up with minimal effort. These pre-configured apps are published in the Microsoft Entra App Gallery.
- You can manually configure most apps for single sign-on if they aren't already in the gallery. Microsoft Entra ID provides several SSO options: SAML-based SSO and OIDC-based SSO.



## SaaS App Integration Tutorials

<https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/tutorial-list>

# Exercise: Troubleshoot SAML single sign-on for custom SaaS apps

## Interactive guide

Integrate an application in Microsoft Entra ID providing the single sign-on experience

[Visit this interactive guide](#)



Dashboard > Enterprise applications | All applications >

### ClaimsXRay | Overview

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage

Properties Owners Users and groups Single sign-on

**Properties**

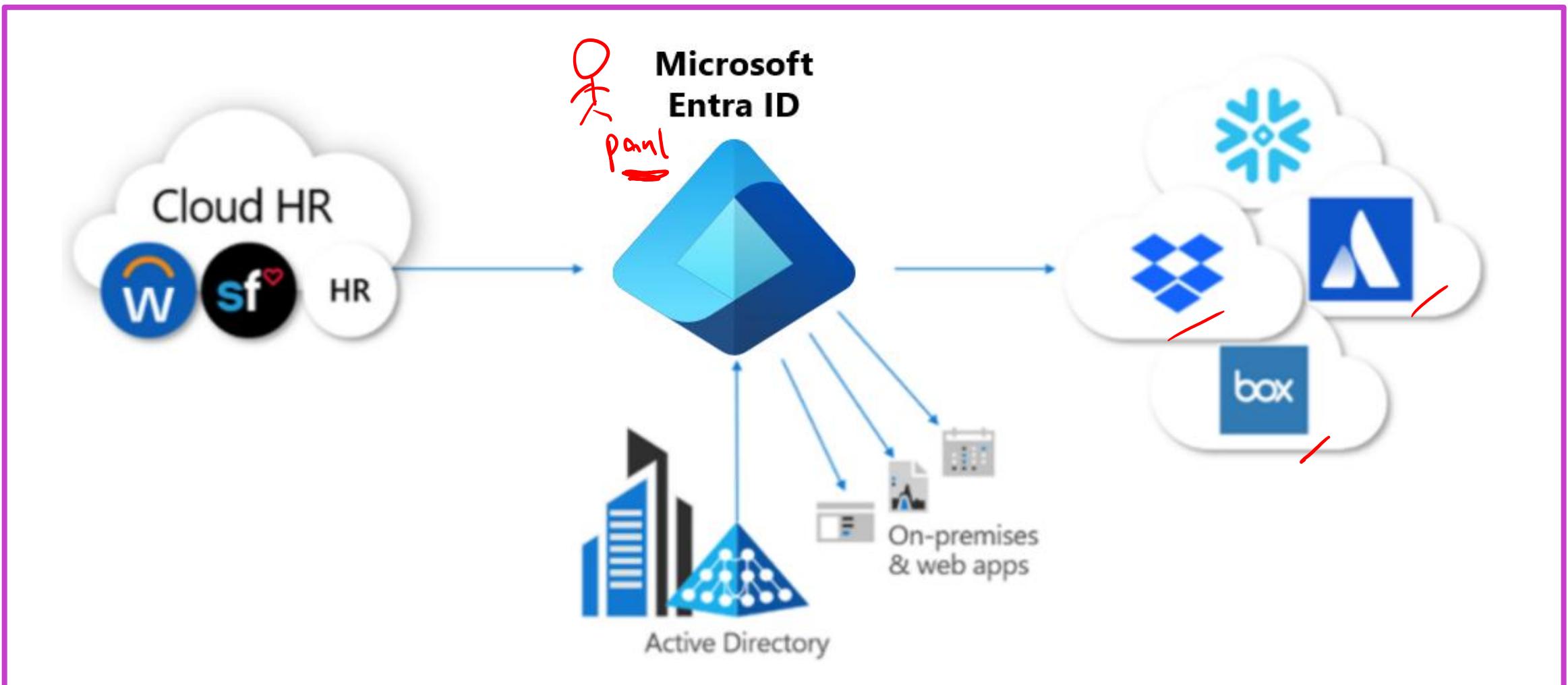
Name  Application ID  Object ID

**Getting Started**

The screenshot shows the 'ClaimsXRay' application overview in Microsoft Entra ID. On the left, there's a sidebar with links for 'Overview', 'Deployment Plan', and 'Diagnose and solve problems'. Below that is a 'Manage' section with 'Properties', 'Owners', 'Users and groups', and 'Single sign-on'. The 'Single sign-on' link is highlighted with a red box and has a red arrow pointing to it from the 'Manage' section. The main content area on the right displays the application's properties, including its name ('ClaimsXRay'), application ID ('69a1e7ec-1...'), and object ID ('ff9803a4-...'). There's also a 'Getting Started' section.

# Implement application user provisioning

# Application user provisioning



# Manual vs. automatic provisioning

The screenshot shows the Microsoft Entra admin center interface. At the top, there are two navigation items: 'Federated SSO' and 'Provisioning'. The 'Provisioning' item is highlighted with a red box. Below this, under the heading 'Featured applications', there are three application cards: 'Box', 'Concur', and 'Cornerstone OnDemand'. Each card displays the application logo, its name, and a small icon representing the provisioning status. The 'Box' and 'Concur' icons have a red box around them, while the 'Cornerstone OnDemand' icon does not.

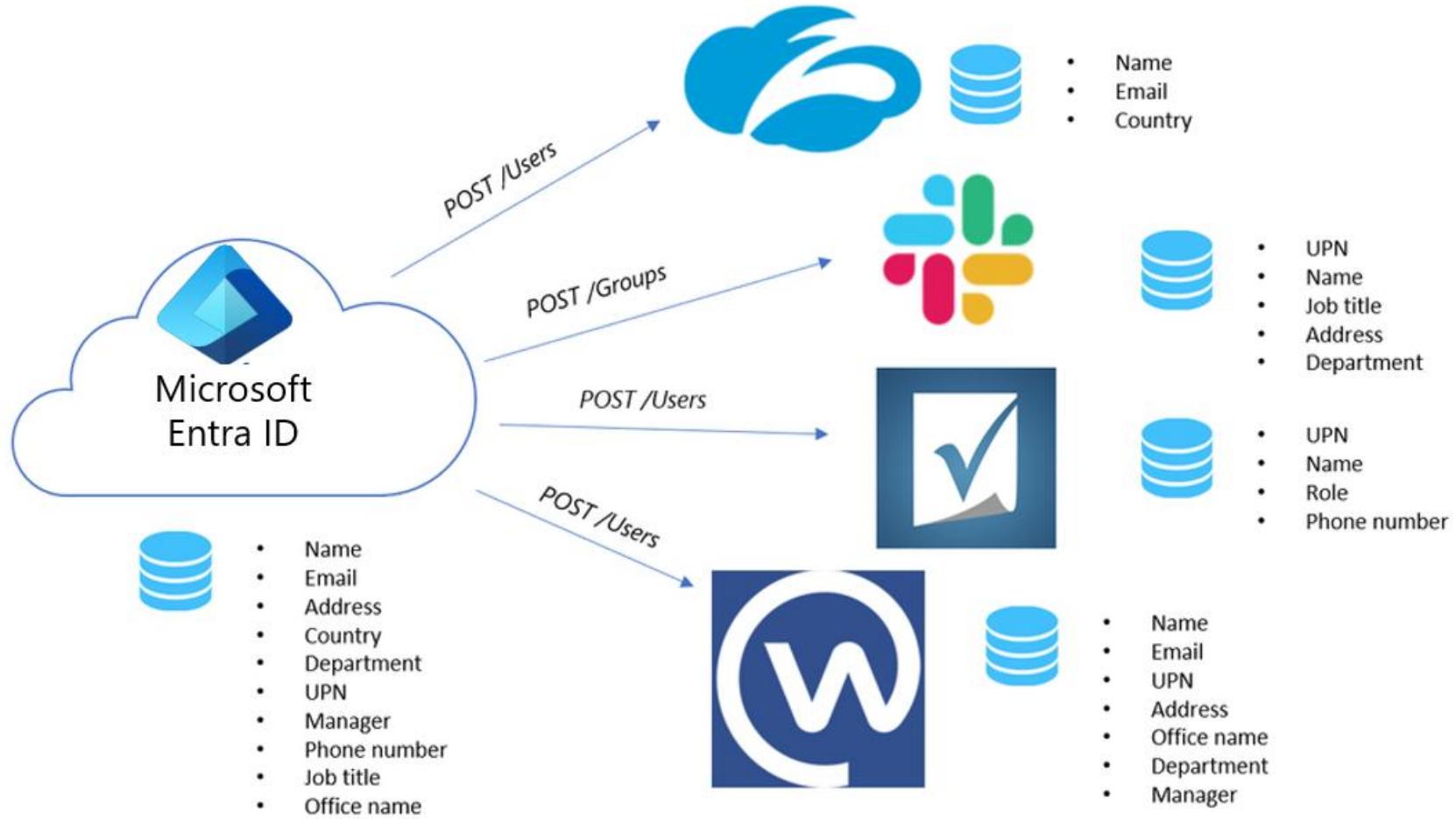
## Manual provisioning

As yet, there is no automatic Microsoft Entra provisioning connector for the app yet. User accounts must be created manually.

## Automatic provisioning

A Microsoft Entra provisioning connector has been developed for this application.

# SCIM provisioning overview



Monitor and audit  
access/sign-on to Microsoft  
Entra integrated enterprise  
applications

# Usage and insight reports

- What are the most used applications in the organization?
- What applications have the most failed sign-ins?
- What are the top sign-in errors for each application?

The screenshot shows the Microsoft Entra admin center interface. At the top, there's a navigation bar with 'Microsoft Entra admin center' and a 'Home > Usage & insights' breadcrumb. On the left, a sidebar lists various administrative categories like 'User experiences', 'Hybrid management', 'Monitoring & health', and 'Protection'. The 'Usage & insights' section is highlighted with a grey background. It contains a list of activity types: 'Microsoft Entra application activity (Preview)', 'AD FS application activity', 'Authentication methods activity', 'Service principal sign-in activity (Preview)', and 'Application credential activity (Preview)'. The 'Microsoft Entra application activity (Preview)' item has a small user icon next to it.

Microsoft Entra admin center

User experiences

Hybrid management

Monitoring & health

Sign-in logs

Audit logs

Provisioning logs

Health (Preview)

Log Analytics

Diagnostic settings

Workbooks

Usage & insights

Bulk operations

... Show less

Protection

Identity governance

Home >

Usage & insights

Microsoft Entra application activity (Preview)

AD FS application activity

Authentication methods activity

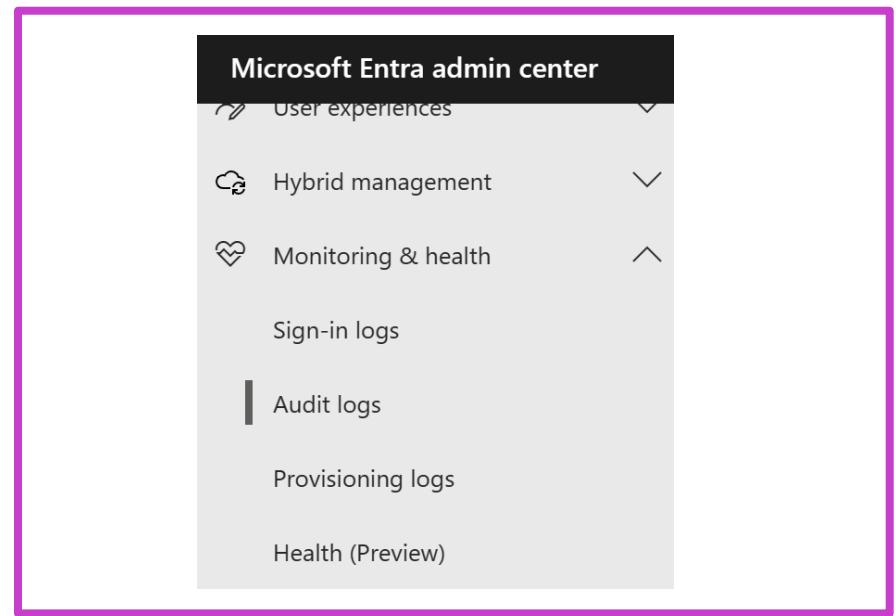
Service principal sign-in activity (Preview)

Application credential activity (Preview)

# Audit Logs (in Microsoft Entra ID)

## Record of system activities for compliance

- The date and time of the occurrence
- The service that logged the occurrence
- The category and name of the activity (what)
- The status of the activity (success or failure)
- The initiator/actor (who) of an activity

A screenshot of the Microsoft Entra Audit logs table. The table has columns for Date, Service, Category, Activity, Status, Status reason, Target(s), and Initiated by (actor). The data shows several log entries from July 9, 2021, at various times between 9:36:09 AM and 9:38:48 AM. Most entries are for Core Directory services and ApplicationManagement categories, involving actions like Update service principal, Update application, and Add service principal, all with Success status. Some entries mention Microsoft.Online.Directory... and Zoom as targets. AAD App Management is listed as the initiator for several entries.

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
7/9/2021, 9:38:48 AM	Core Directory	ApplicationManagement	Update service principal	Success		Zoom	
7/9/2021, 9:38:48 AM	Core Directory	ApplicationManagement	Update service principal	Failure	Microsoft.Online.Directory...	Zoom	AAD App Management
7/9/2021, 9:38:48 AM	Core Directory	ApplicationManagement	Update service principal	Success		Zoom	AAD App Management
7/9/2021, 9:36:10 AM	Core Directory	ApplicationManagement	Update application	Success		Zoom	AAD App Management
7/9/2021, 9:36:10 AM	Core Directory	ApplicationManagement	Update service principal	Success		Zoom	AAD App Management
7/9/2021, 9:36:09 AM	Core Directory	ApplicationManagement	Add service principal	Success		Zoom	AAD App Management
7/9/2021, 9:36:09 AM	Core Directory	ApplicationManagement	Add application	Success		Zoom	AAD App Management
7/9/2021, 9:28:02 AM	Core Directory	ApplicationManagement	Add service principal	Success			AAD App Management

# Enterprise applications audit logs

## Application-based audit reports

- What applications have been added or updated?
- What applications have been removed?
- Has a service principal for an application changed?
- Have the names of applications been changed?
- Who gave consent to an application?

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with the following items:

- Home
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
- Applications
  - Enterprise applications (highlighted with a red box)
  - App registrations
  - Roles & admins
  - Billing
  - Settings
  - Protection
  - Identity governance
  - External Identities
- Security
  - Conditional Access
  - Consent and permissions
- Activity
  - Sign-in logs
  - Usage & insights
- Audit logs (highlighted with a red box)
- Provisioning logs

The 'Enterprise applications' and 'Audit logs' items are specifically highlighted with red boxes.

# Create and manage application collections

# Create app collections

Create an admin application collection	Create a collection using the My Apps portal
<ol style="list-style-type: none"><li>1. Go to Microsoft Entra ID then select Enterprise Applications.</li><li>2. Under Manage, select App Launchers.</li><li>3. Select New collection.</li><li>4. In the New collection page, enter a Name and Description.</li><li>5. Select the Applications tab. Select + Add application to open the Add applications page.</li><li>6. Select all the applications you want to add.</li><li>7. When you're finished adding applications, select Add.</li><li>8. Select the Owners tab. Select + Add users and groups.</li><li>9. Select Review + Create. The properties for the new collection appear.</li></ol>	<ol style="list-style-type: none"><li>1. Open the My Apps portal.</li><li>2. Select the ellipsis (...) on the apps screen.</li><li>3. Choose Manage collections.</li><li>4. Select Create collection.</li><li>5. Select the + Add apps option to add all the apps you want in the collection.</li><li>6. After picking your apps, select the Add selected apps button.</li><li>7. Give the collection a name and choose Create collection.</li></ol>

# Summary



## In this section, you learned how to:

- Implement token customizations
- Implement and configure consent settings
- Integrate on-premises apps by using Microsoft Entra Application Proxy
- Integrate custom SaaS apps for SSO
- Implement application user provisioning
- Monitor and audit access/Sign-On to Microsoft Entra ID integrated enterprise applications

# Implement app registrations

# Learning objectives

- 1** Plan your line-of-business application registration strategy
  - 2** Implement application registrations
  - 3** Configure application permissions
  - 4** Implement application authorization
  - 5** Manage and monitor applications with app governance
- 

# Plan your line-of-business application registration strategy

# Why do applications integrate with Microsoft Entra ID?

Add applications to Microsoft Entra ID to leverage one or more of the services it provides, including:

- Application authentication and authorization
- User authentication and authorization
- Single sign-on (SSO) using federation or password
- User provisioning and synchronization
- OAuth authorization services
- Application publishing and proxy
- Directory schema extension attributes
- Role-based access control

# Application objects and service principals

## Application objects:

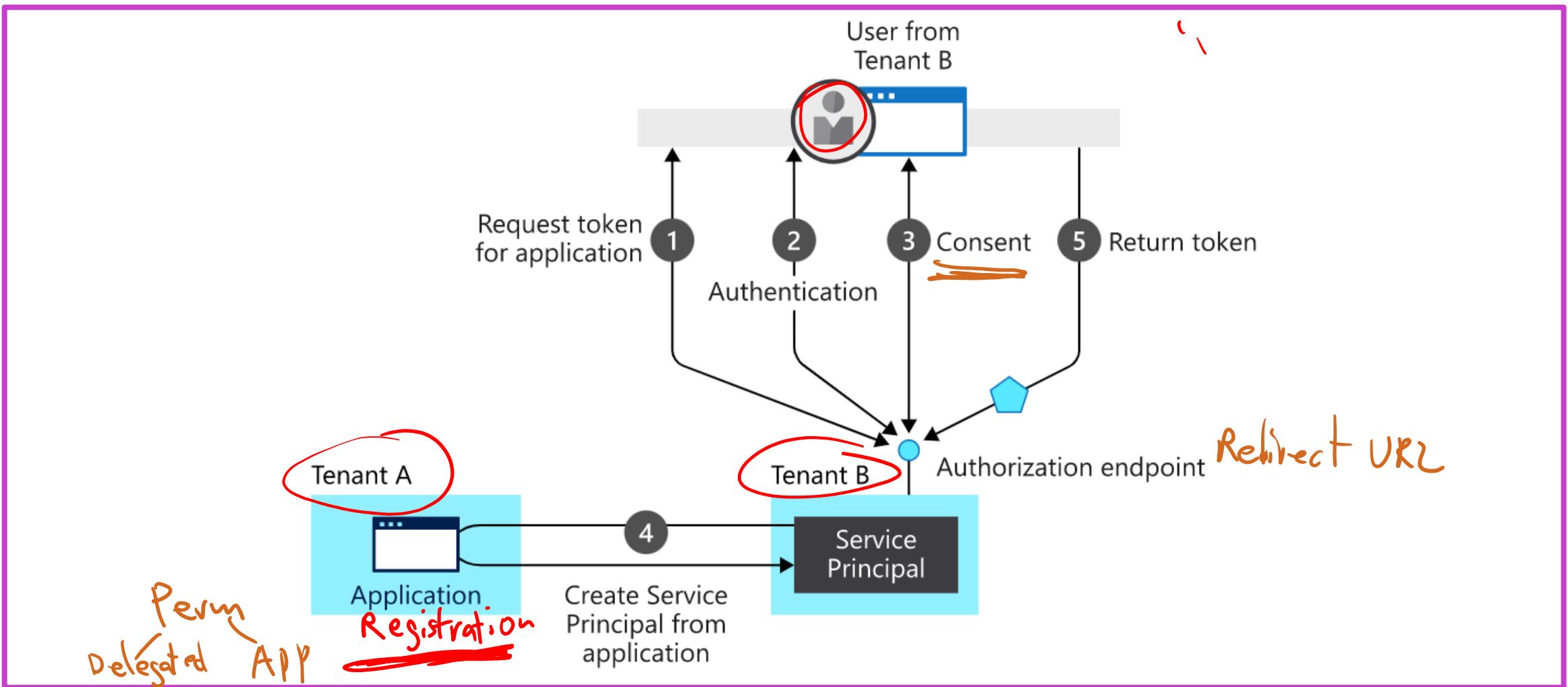
- Define and describe the application to Microsoft Entra ID, enabling it to know how to issue tokens based on its settings
- Will only exist in their tenant

## Service principals

- Govern an application connecting to Microsoft Entra ID
- Can be considered the instance of the application in your tenant

# New app registration

Mail.Read  
Mail.ReadWriteAll  
...

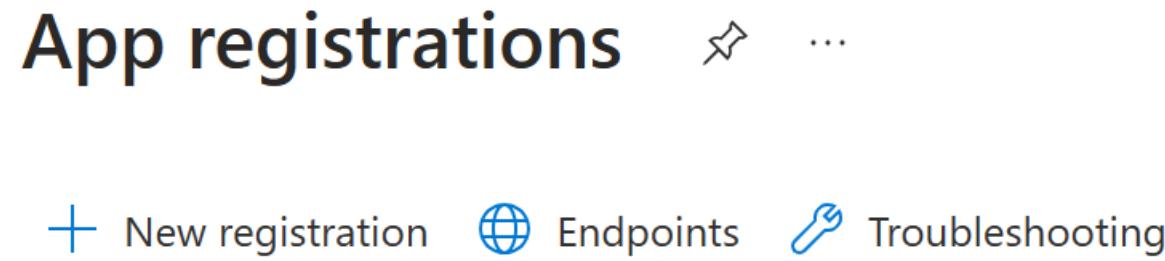


# Who has permission to add applications to my Microsoft Entra instance?

- By default, all users in your directory have rights to register application objects they are developing, and they have discretion over which applications they share or give access to their organizational data through consent.
- When the first user in your directory signs into an application and grants consent, that will create a service principal in your tenant; otherwise, the consent grant information will be stored on the existing service principal.

# Implement application registrations

# Demo: Register and application



# After your app is registered:

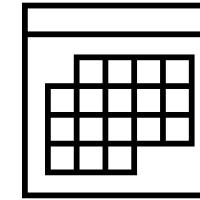
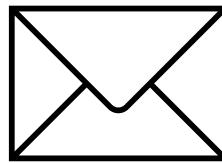
- 1 Add a redirect URI
- 2 Configure platform settings
- 3 Add credentials
- 4 Add a certificate and a client secret
- 5 Register the web API
- 6 Add a scope

# Configure application permissions

# Application permissions

Applications that integrate with Microsoft identity platform follow an authorization model that gives users and administrators control over how data can be accessed. Permissions for tasks like these can be controlled:

- Read a user's calendar
- Write to a user's calendar
- Send mail as a user



# Permissions and consent: permission types

## Delegated permissions

- Used by apps that have a signed-in user present
- Either the user or an administrator consents to the permissions that the app requests

## Application permissions

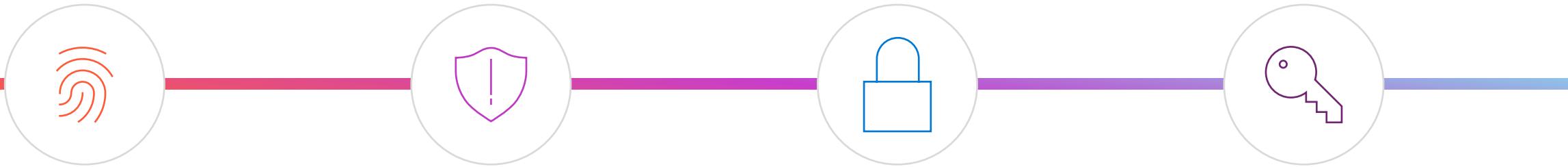
- Used by apps that run without a signed-in user present
- Only an administrator can consent to application permissions

# OpenID connect scopes

Access Token

Claim

Claim



## OpenID

By using this permission, an app can receive a unique identifier for the user in the form of the sub claim.

## Email

The email claim is included in a token only if an email address is associated with the user account

## Profile

It gives the app access to a large amount of information about the user.

## Offline access

The app can receive refresh tokens from the Microsoft identity platform token endpoint.

# Exercise: Grant tenant-wide admin consent to an application



## Grant admin consent in app registrations

For applications your organization has developed, or for those that are registered directly in your Microsoft Entra tenant, you can grant tenant-wide admin consent from app registrations in the Microsoft Entra admin center.

[Launch this Exercise in GitHub](#)

The screenshot shows a step in the Microsoft Entra admin center where admin consent is being granted for an application. A red box highlights the 'Grant admin consent for Contoso' button. The table below lists the permissions granted:

Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Below the table, there is a link to manage permissions and user consent: [Enterprise applications](#).

# Implement application authorization

# Application roles

Application roles are used to assign permissions to users. You define app roles by using the Microsoft Entra admin center. When a user signs into the application, Microsoft Entra ID emits a roles claim for each role that the user has been granted individually and from their group membership.

There are two ways to declare app roles by using the Microsoft Entra admin center:

- App roles UI
  - Found on the App Registration/App roles
- App manifest editor

# Demo: Add app roles to an application

## Hello World Identity

 Search <<

 Overview

 Quickstart

 Integration assistant

### Manage

 Branding & properties

 Authentication

 Certificates & secrets

 Token configuration

 API permissions

 Expose an API

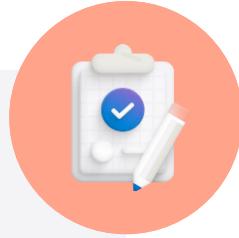
 App roles

 Owners

 Roles and administrators

 Manifest

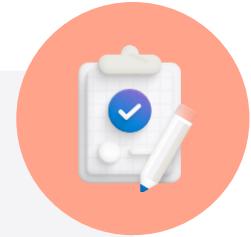
# Summary



**Now that you have reviewed this section, you should be able to:**

- Plan your line-of-business application registration strategy.
- Implement application registrations.
- Configure application permissions.
- Implement application authorization.

# Summary



## Plan and design single sign-on for apps

- MDCA and ADFS application location
- App discover
- App management roles
- Add on-premises app management

## Implement app registration

- Design and app registration strategy
- Register your applications
- Configure app permissions
- Assign app authorization

## Implement and monitor enterprise apps

- Consent settings
- Monitor enterprise applications
- Application collections
- Add on-premises app management

# Labs

09



Lab	Brief description	Length
17. App discovery	Use Defender for Cloud Apps application discovery and enforce a restriction.	15 minutes
18. App access policies	Configure app access policies in <u>Defender for Cloud Apps</u> .	10 minutes
19. Register an application	Registering your application establishes a trust relationship between your app and the Microsoft identity platform.	10 minutes
20. Implement access management for apps.	Add an enterprise app and assign your administrator account.	5 minutes
21. Grant tenant wide access to an app	For applications registered directly in your Microsoft Entra tenant, grant tenant-wide admin consent from app registrations in the Microsoft Entra admin center.	10 minutes

# Learning path recap

In this learning path, you learned how to:

Configure and implement identity solutions for applications in Azure.

Compare and contrast managed identities and service principals.

Register and manage both apps and enterprise apps.

# End of presentation