Microsoft

SC-300

Tag 3

Microsoft Identity and Access Administrator

Guten Morgen !

Microsoft

LP 3

Implement access management for apps

© Copyright Microsoft Corporation. All rights reserved.

Agenda

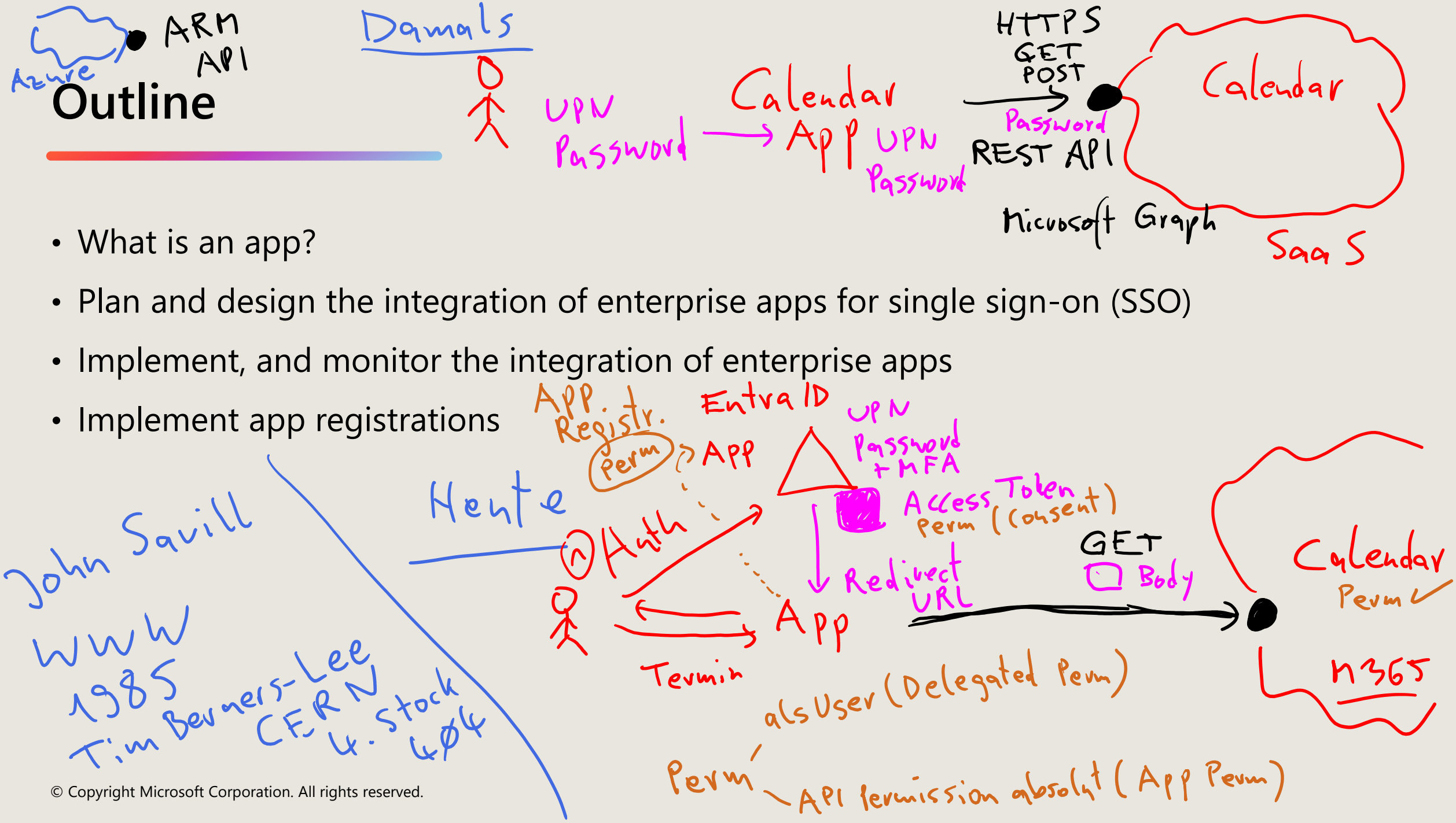
- LP 1 Implement an Identity Management Solution
- LP 2 Implement an Authentication and Access Management Solution
- LP 3 Implement Access Management for Apps
- LP 4 Plan and Implement an Identity Governance Strategy

Labs
- Skillable (LODs)
- GoDeploy

© Copyright Microsoft Corporation. All rights reserved.

Outline

- 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



© Copyright Microsoft Corporation. All rights reserved.

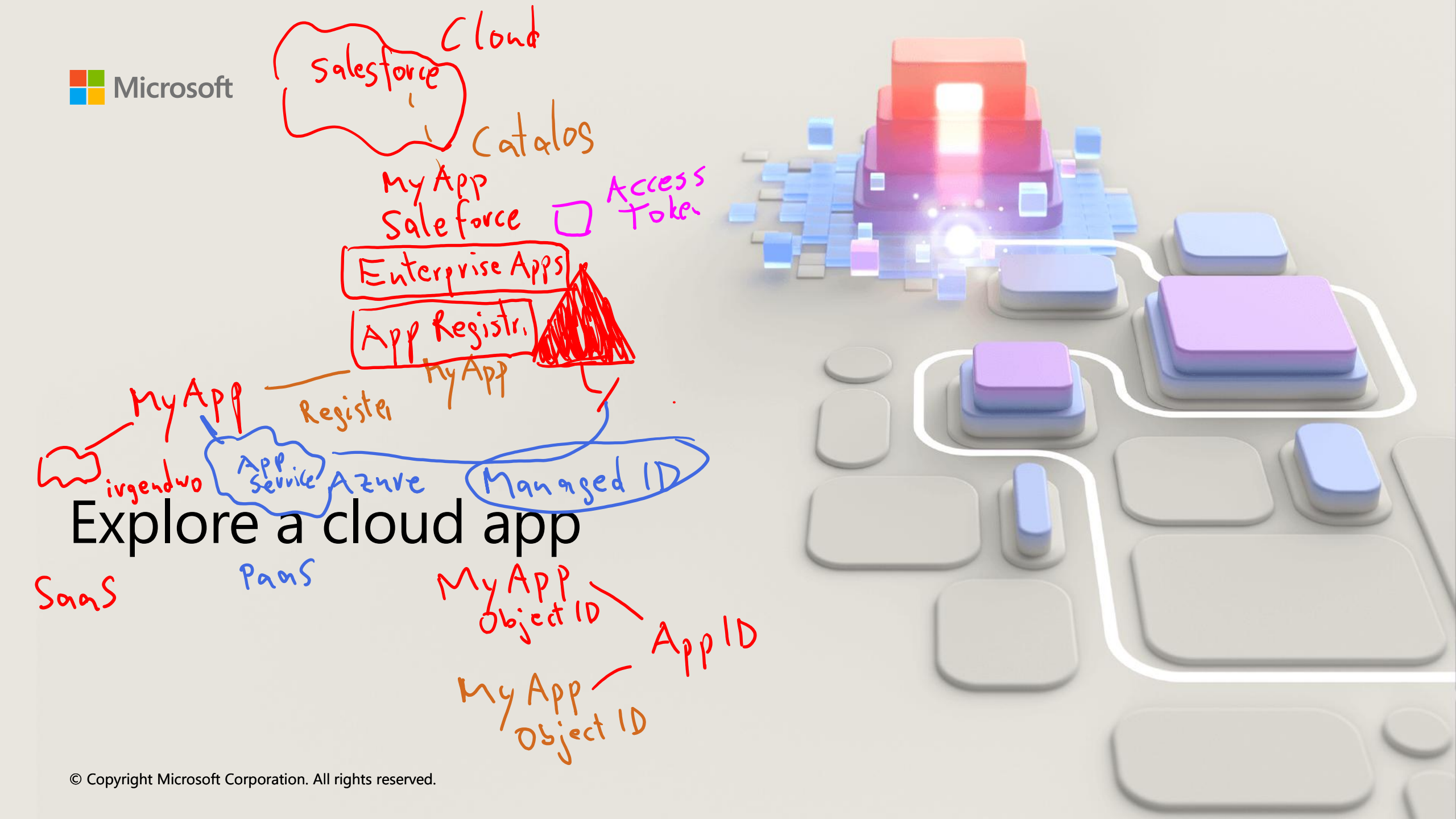
Learning objectives

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.

© Copyright Microsoft Corporation. All rights reserved.

Microsoft



Explore a cloud app

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

Benefits of registering an app

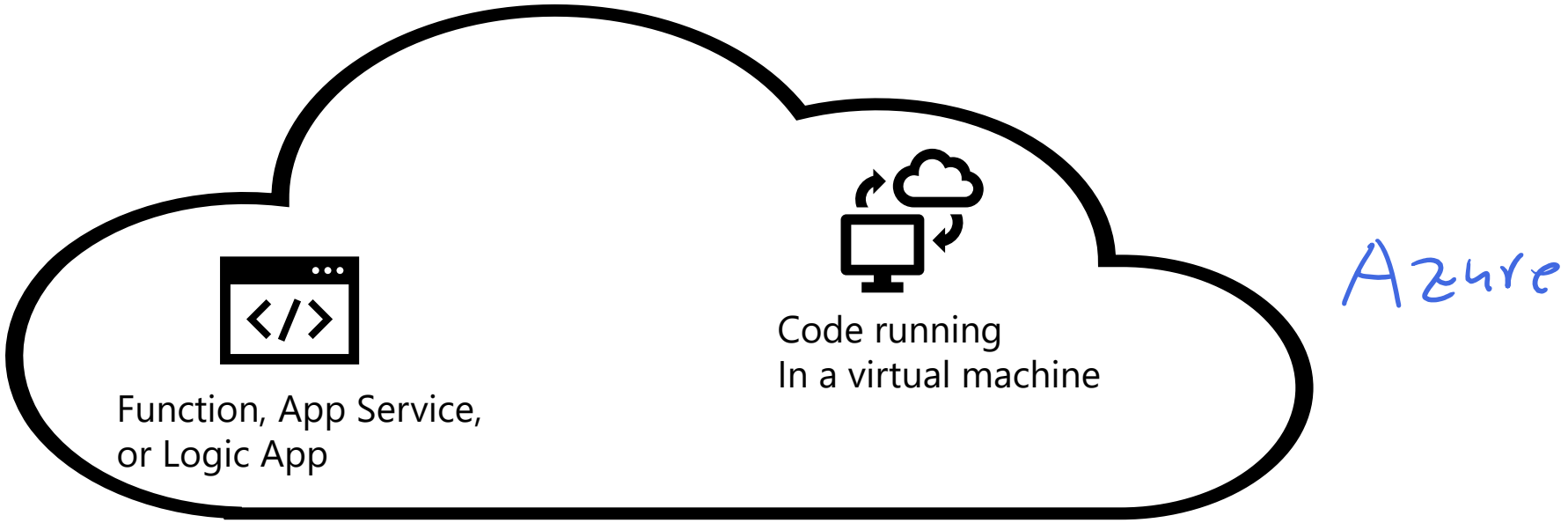
- Restrict which users and how they log into an application.
- Configure the scope permissions and API permissions available to the app.
- Configure and store secrets within the Microsoft identity platform.
- Enable custom branding of the application login.

© Copyright Microsoft Corporation. All rights reserved.

What is an app?

Code

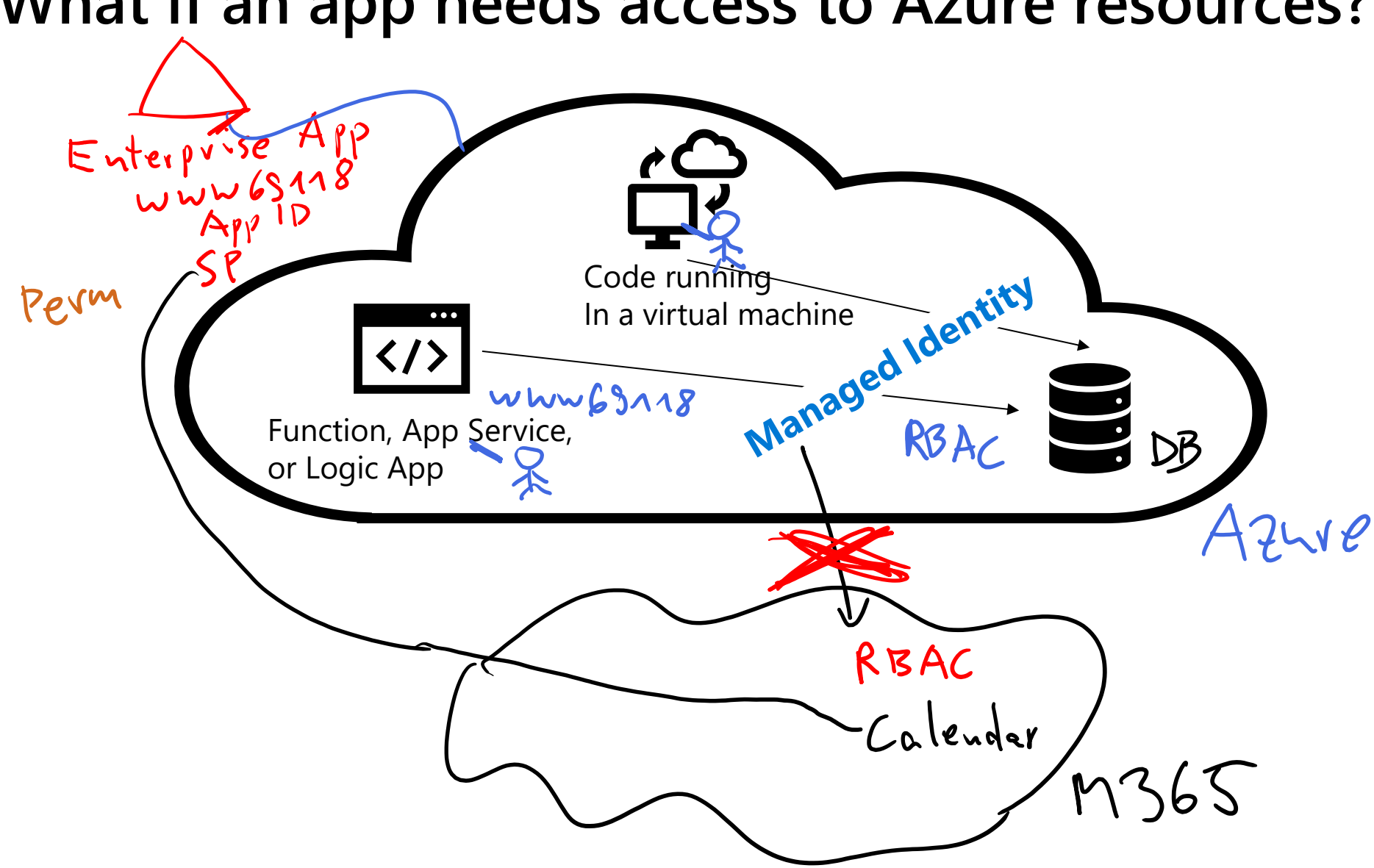
Entra SDKs

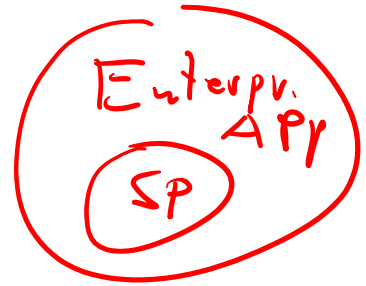


Azure

© Copyright Microsoft Corporation. All rights reserved.

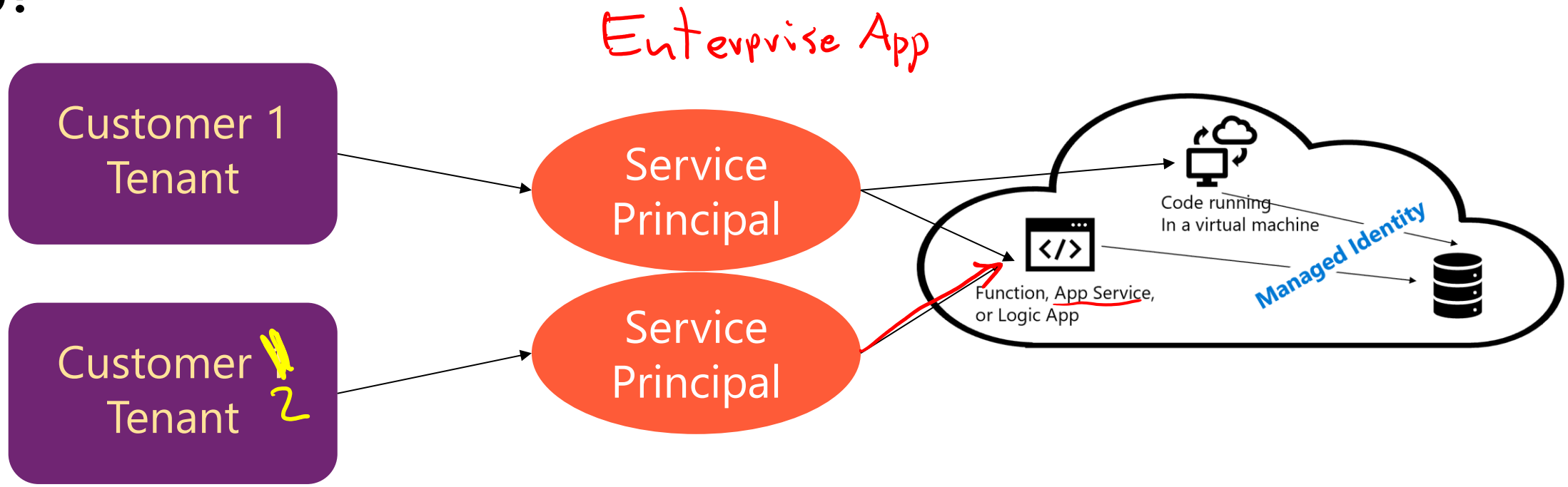
What if an app needs access to Azure resources?





© Copyright Microsoft Corporation. All rights reserved.

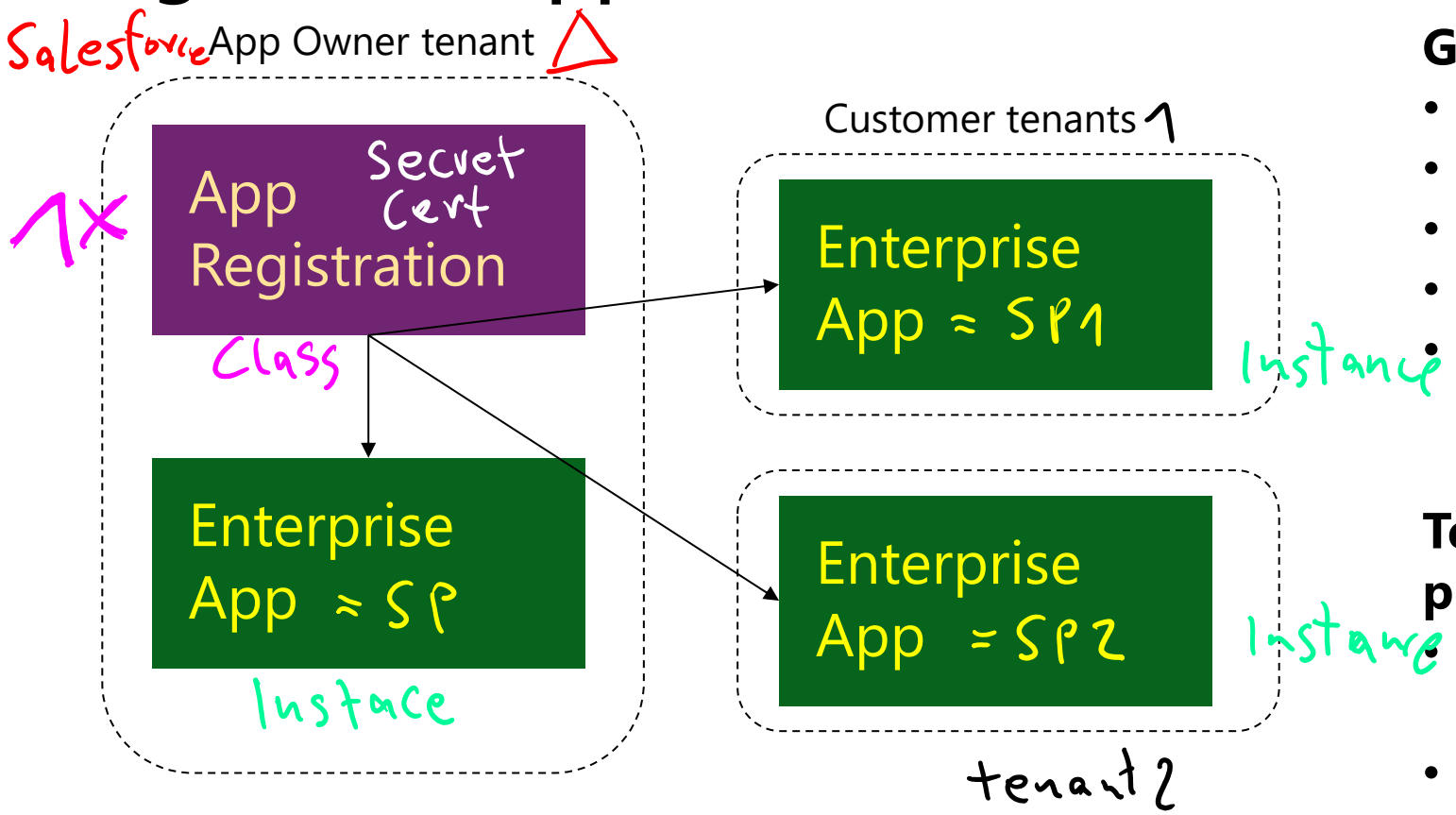
What if people from other tenants need access to your app?



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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Single tenant versus multitenant apps

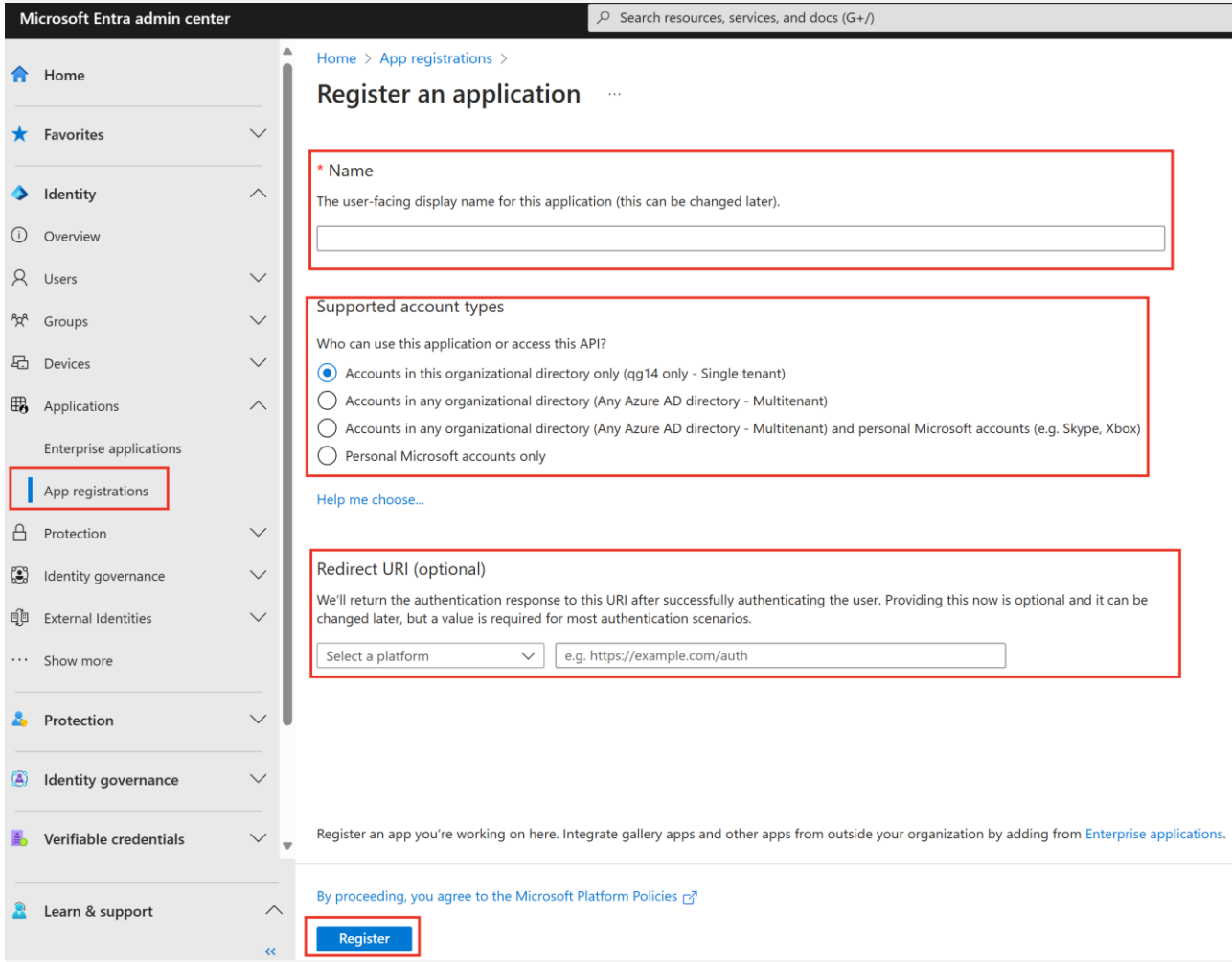
Audience	Single or Multi-tenant	Who can sign in
Accounts in this directory only	Single tenant	All user and guest accounts in your directory.
Accounts in any Microsoft Entra directory	Multi-tenant	All users and guests with a work or school account from Microsoft can use your application or API.
Accounts 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.

© Copyright Microsoft Corporation. All rights reserved.

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



© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Plan and design the integration of enterprise apps for SSO

© Copyright Microsoft Corporation. All rights reserved.

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)

© Copyright Microsoft Corporation. All rights reserved.

Discover apps by using MDCA or ADFS app report

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Cloud Apps

Cloud Access Security Broker (CASB)

Several different deployment modes:

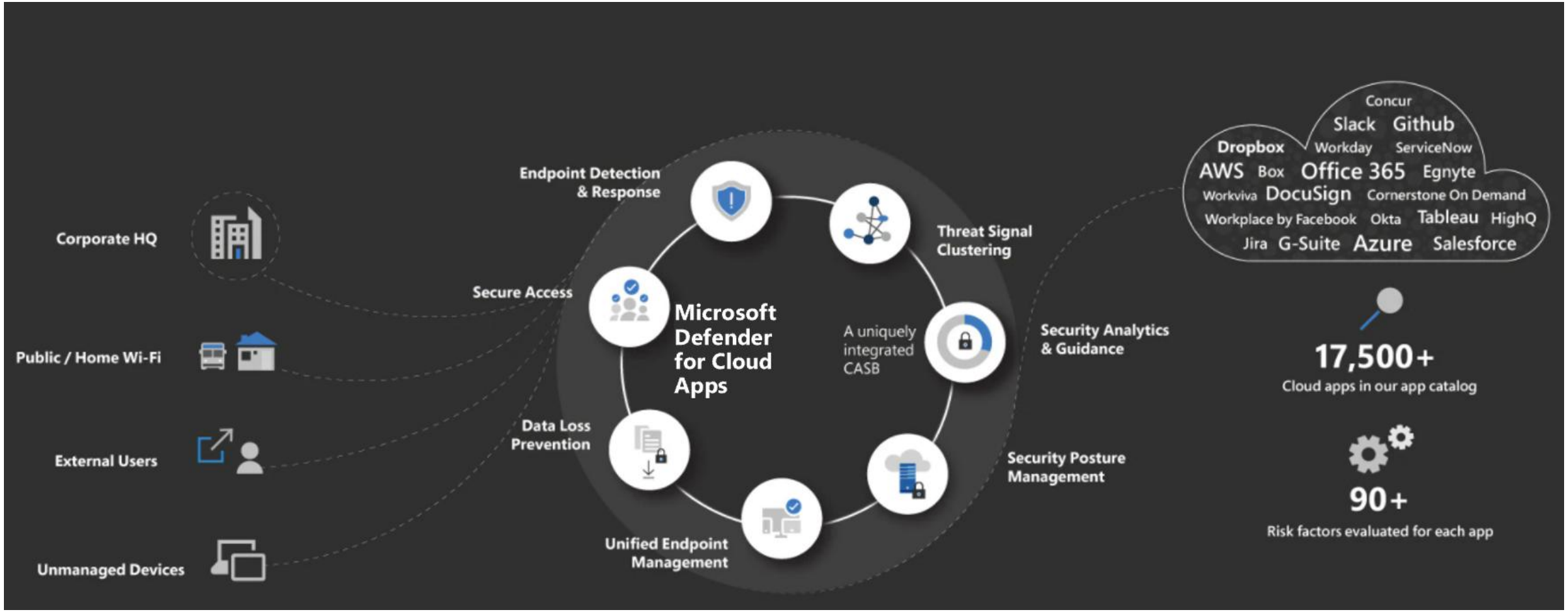
- Log collection
- API connectors
- Reverse proxy

Providing admins with:

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

© Copyright Microsoft Corporation. All rights reserved.

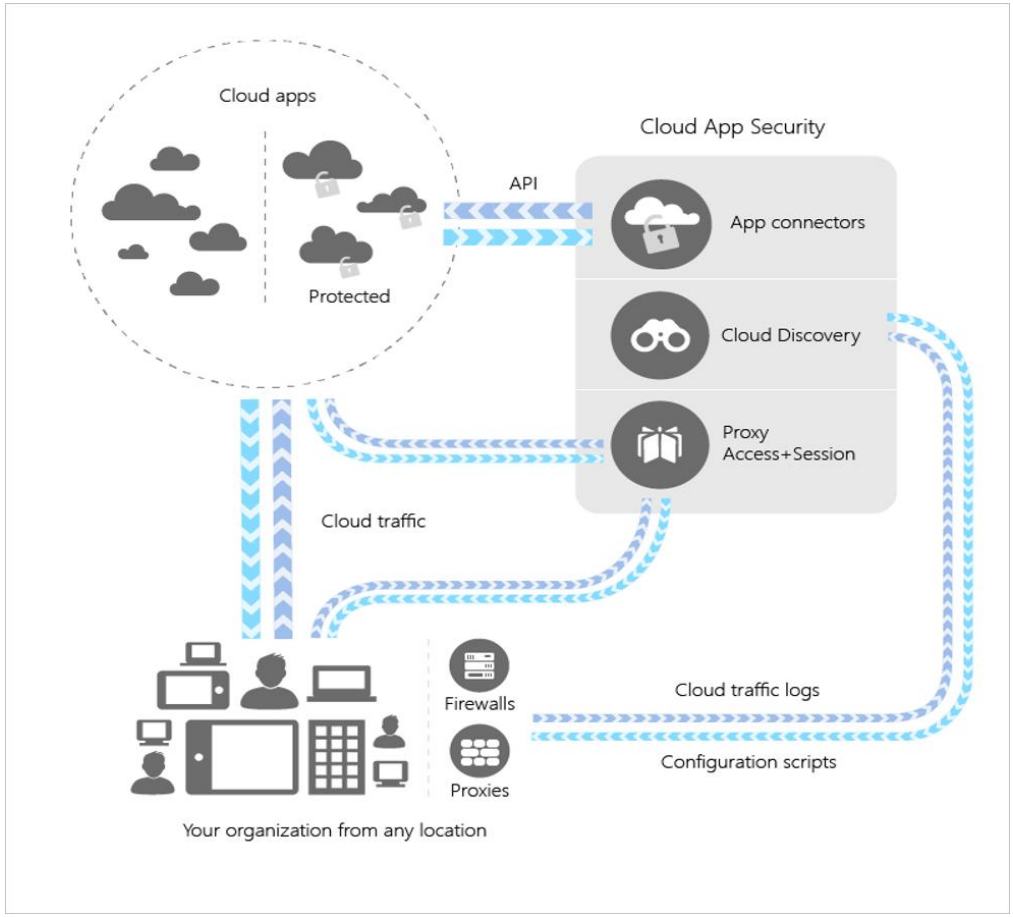
Microsoft Defender for Cloud Apps—process flow



© Copyright Microsoft Corporation. All rights reserved.

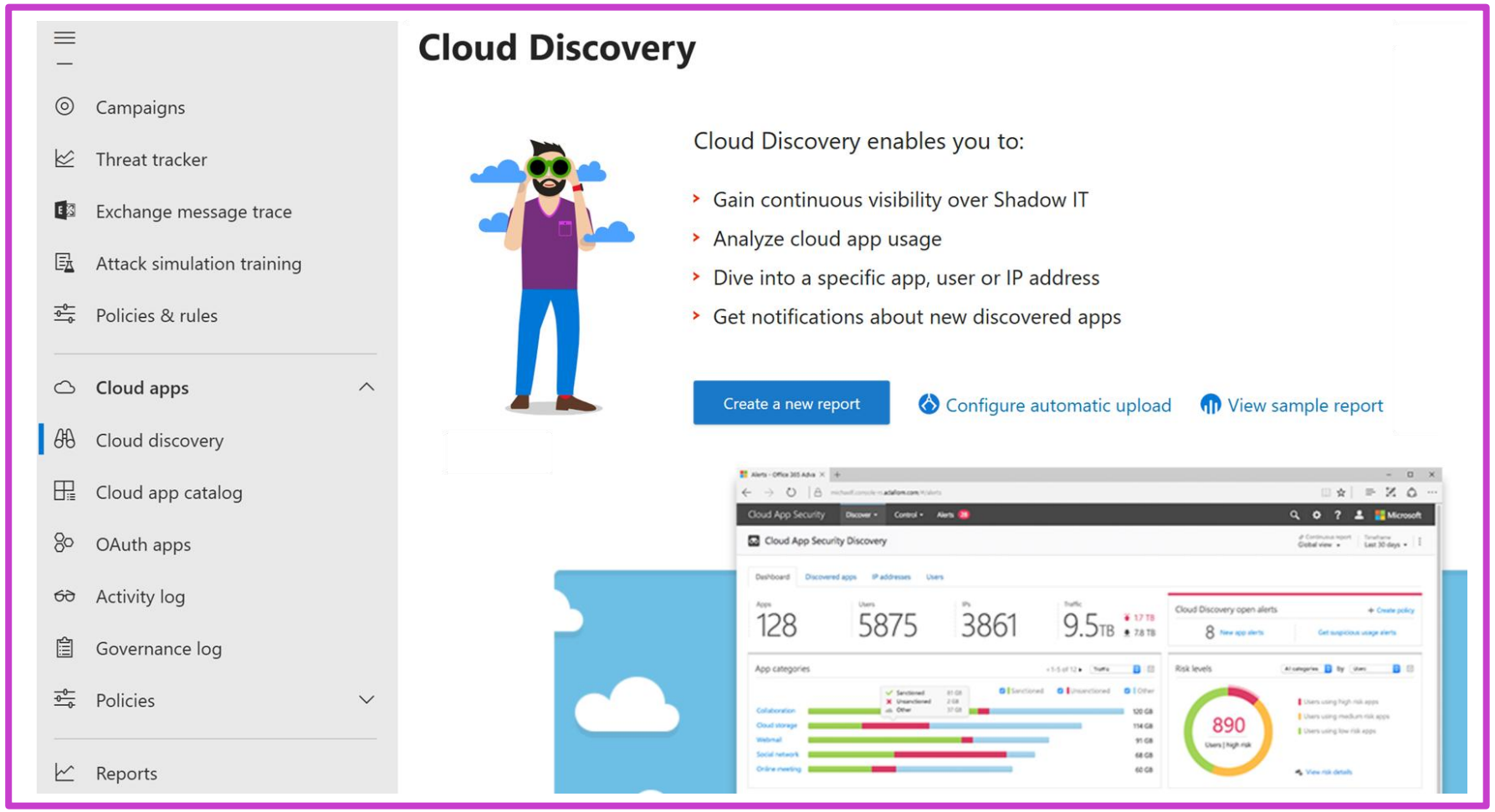
Microsoft Defender for Cloud Apps architecture

- **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



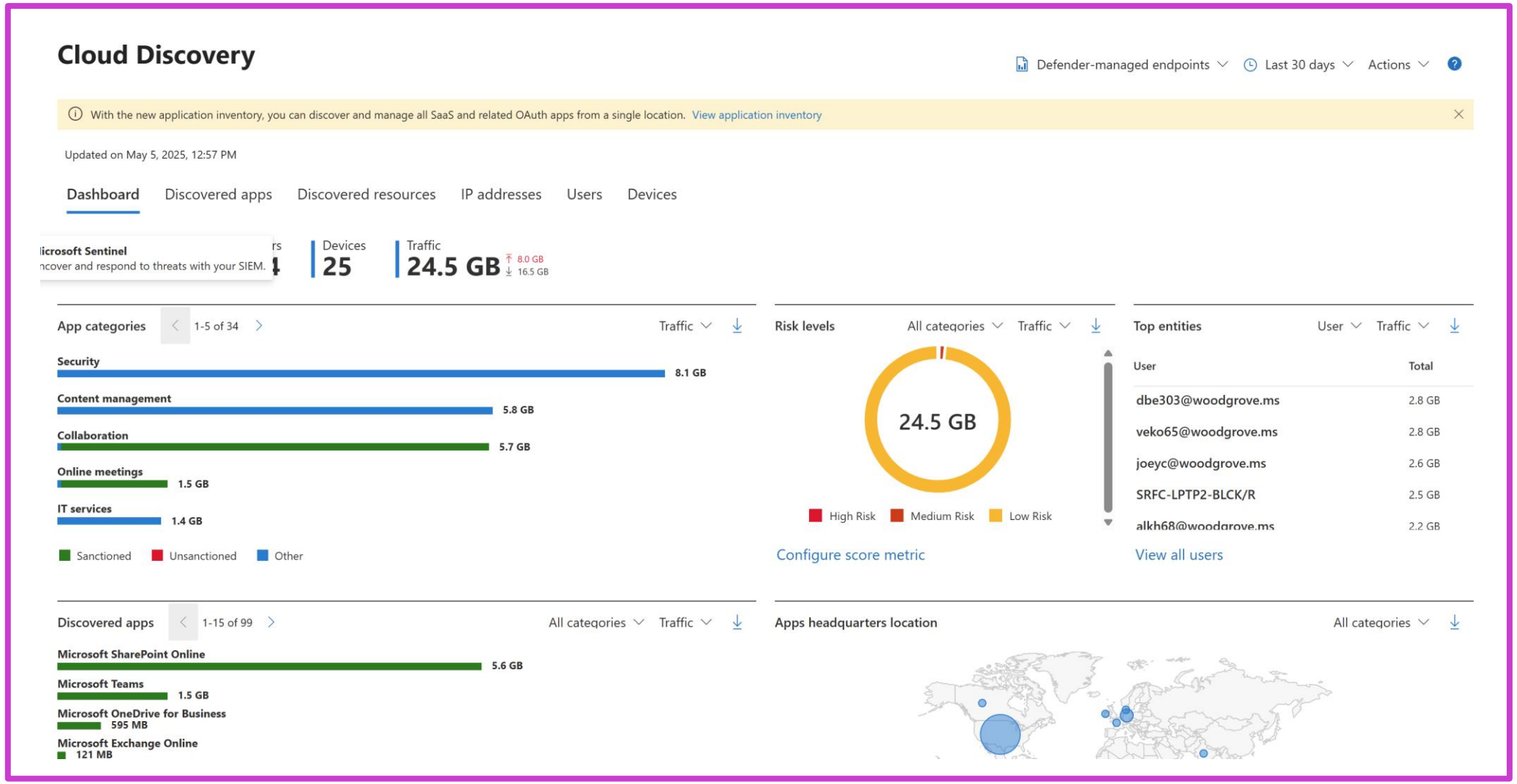
© Copyright Microsoft Corporation. All rights reserved.

Set up Cloud Discovery with Microsoft Defender for Cloud Apps



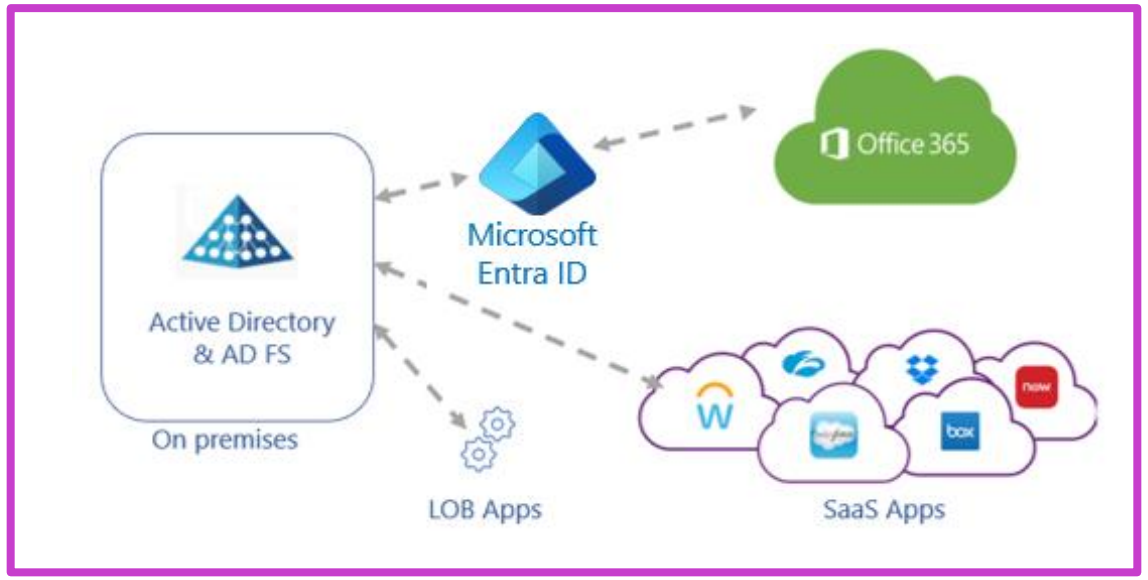
© Copyright Microsoft Corporation. All rights reserved.

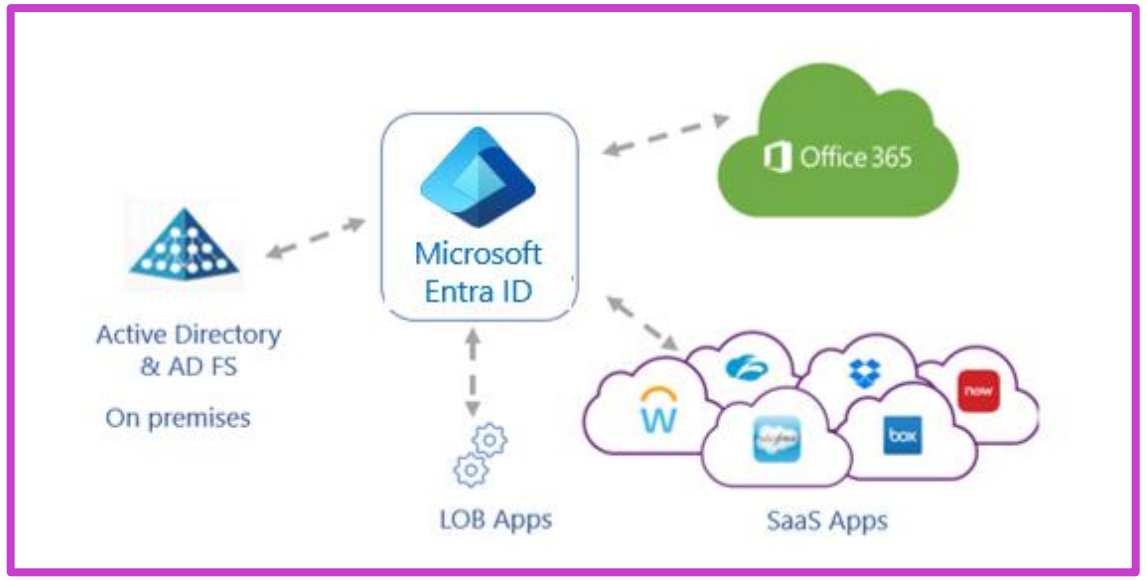
MDCA—discovering apps with Cloud Discovery



© 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.

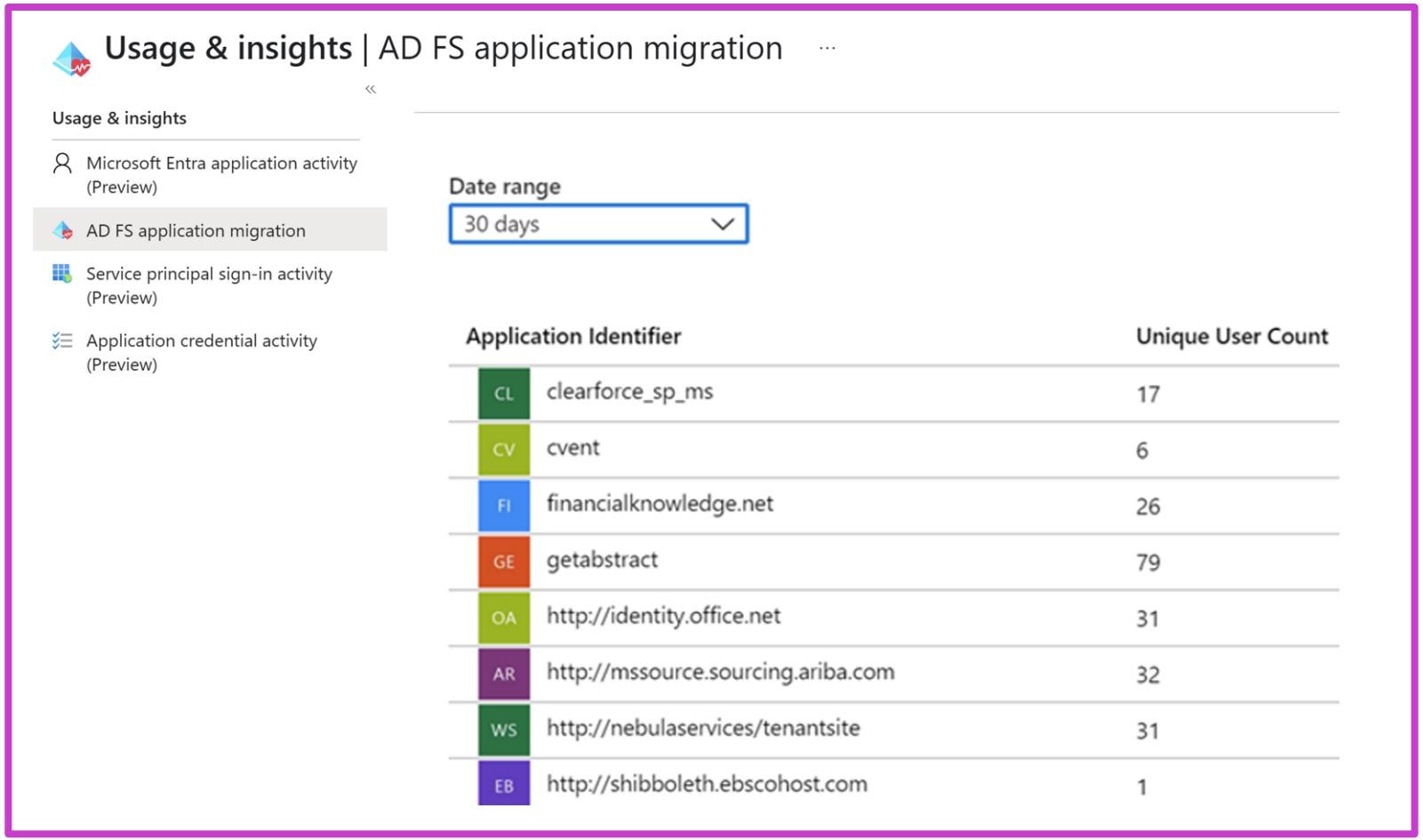
To increase application security, your goal is to have a single set of access controls and policies across your on-premises and cloud environments.

© Copyright Microsoft Corporation. All rights reserved.

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



© Copyright Microsoft Corporation. All rights reserved.

Configure connectors to apps in MDCA

© Copyright Microsoft Corporation. All rights reserved.

What is an app connector in Defender for Cloud Apps?

Capability
Connect to API provided by the app creator
Enables greater visibility into the apps
All communication over secure HTTPS
Common connector API limitations: • Throttling • API limits • Dynamic time-shifting • API windows
Services vary by app

Apps with MDCA connectors

Connectors:

- Atlassian
- Azure
- AWS
- Box
- DocuSign
- Dropbox
- GitHub
- Google Workspace
- Many others

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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.

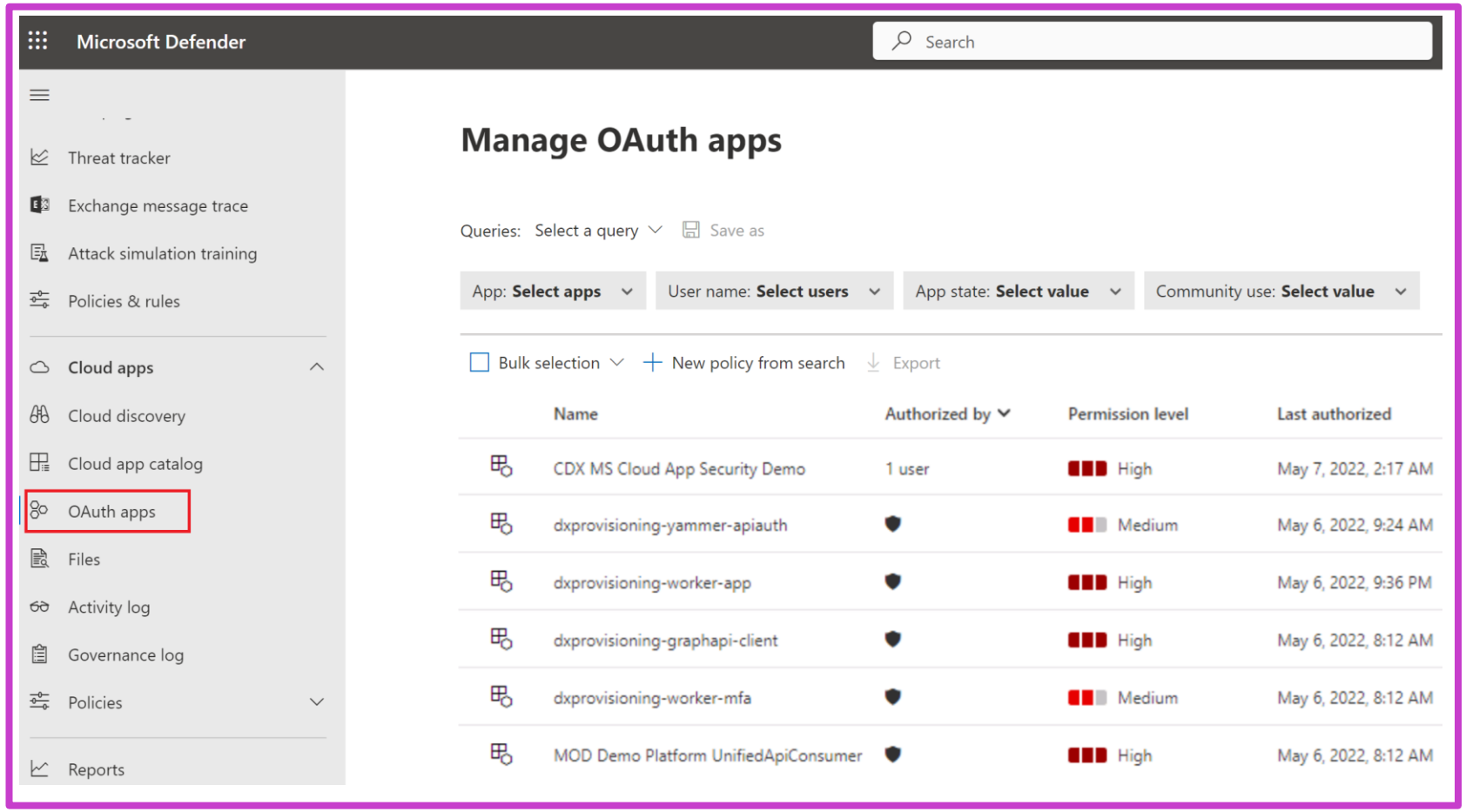
© Copyright Microsoft Corporation. All rights reserved.

Implement and manage policies for OAuth apps

© Copyright Microsoft Corporation. All rights reserved.

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.



© Copyright Microsoft Corporation. All rights reserved.

Design and implement access management for apps

© Copyright Microsoft Corporation. All rights reserved.

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

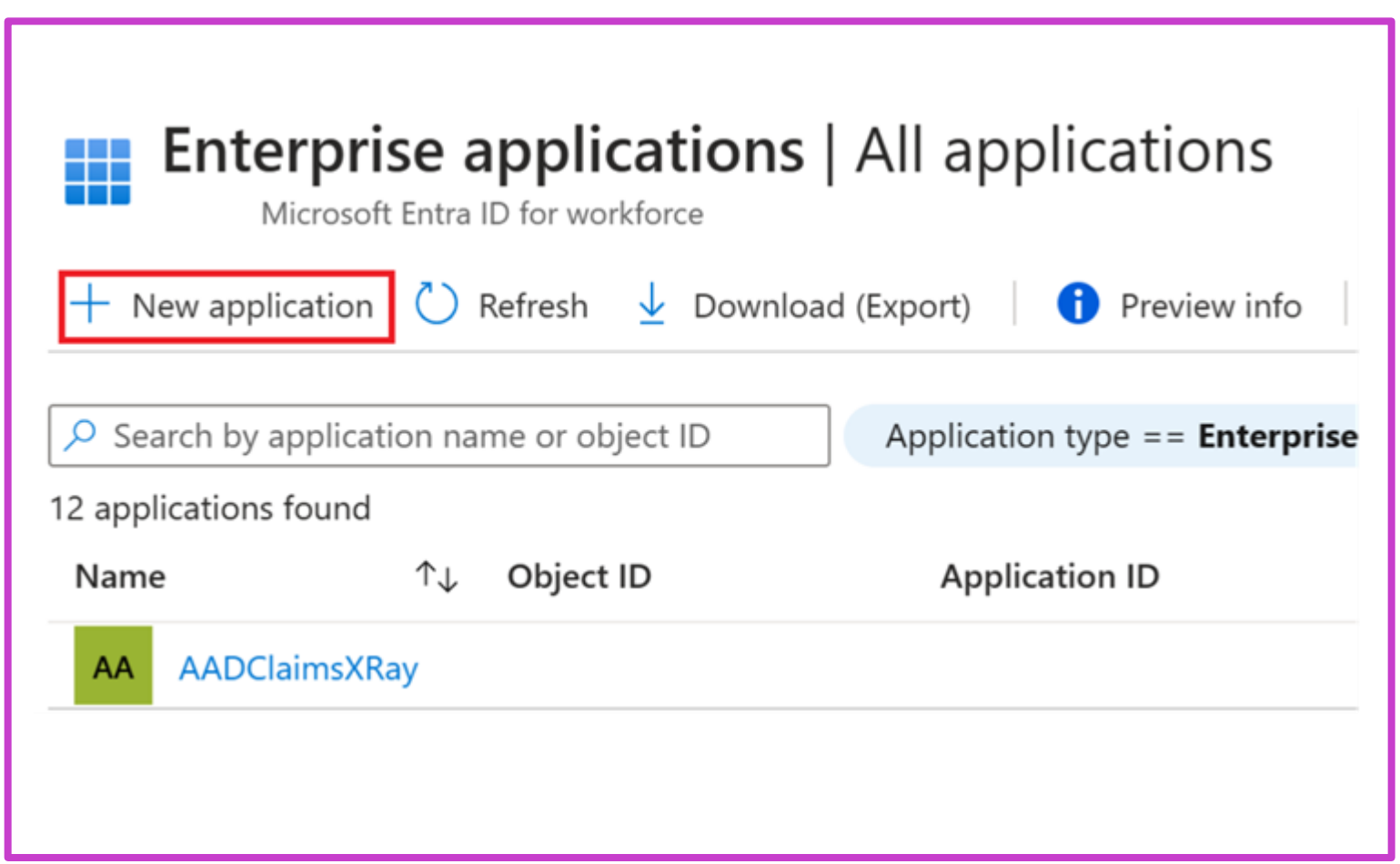
© Copyright Microsoft Corporation. All rights reserved.

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]



© Copyright Microsoft Corporation. All rights reserved.

Design and implement app management roles

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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.**

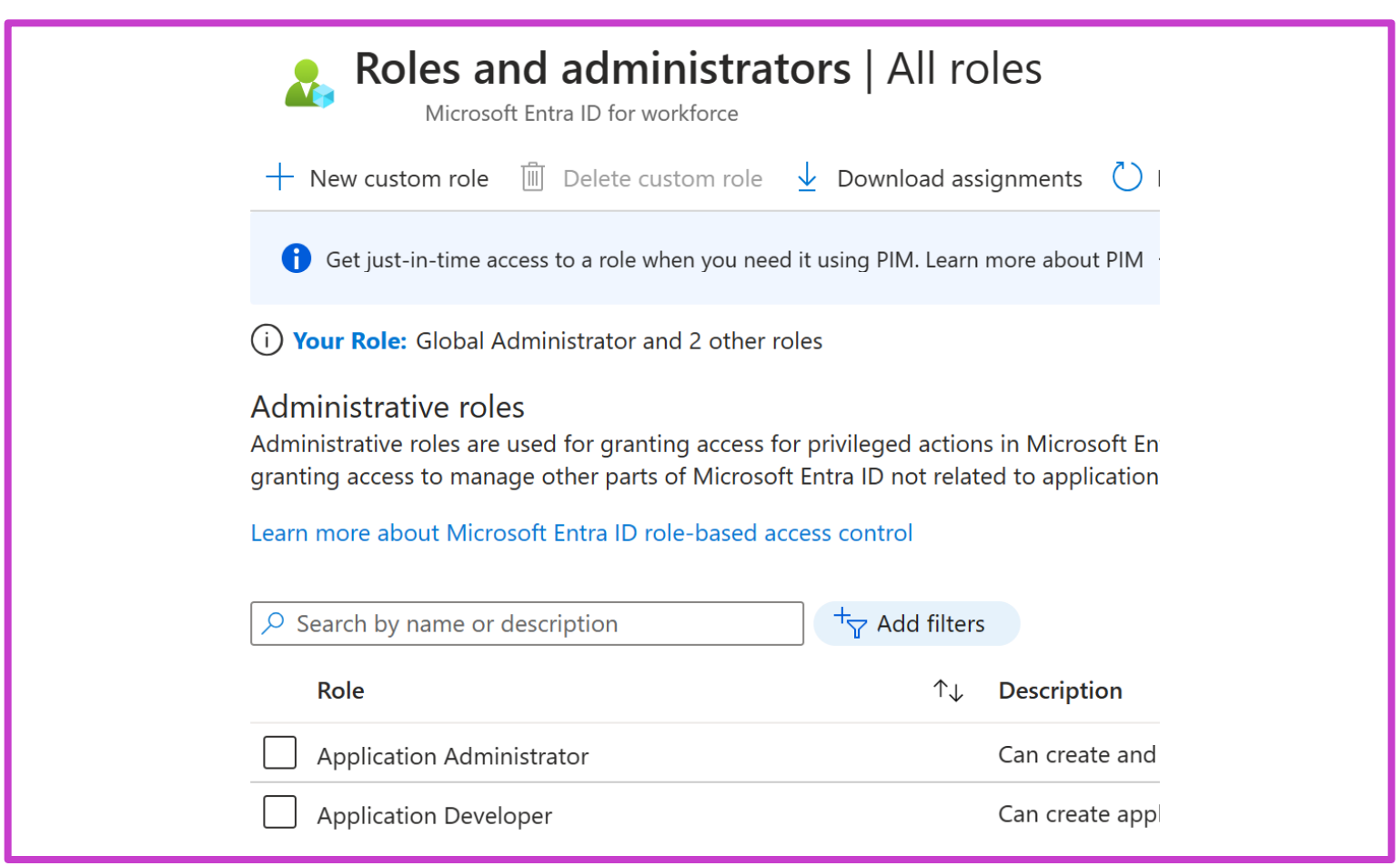
© Copyright Microsoft Corporation. All rights reserved.

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]



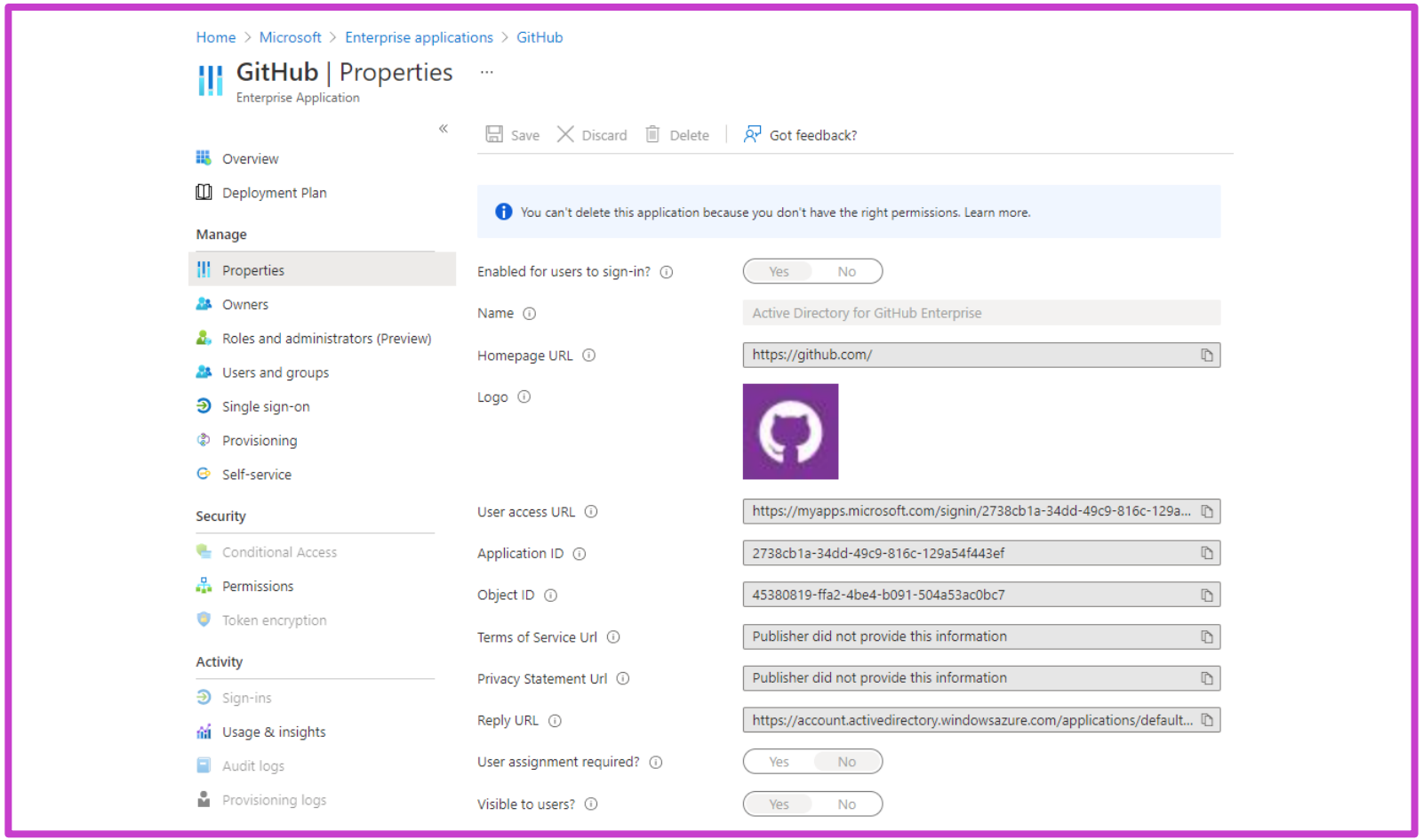
© Copyright Microsoft Corporation. All rights reserved.

Configure preintegrated (gallery) SaaS apps

© Copyright Microsoft Corporation. All rights reserved.

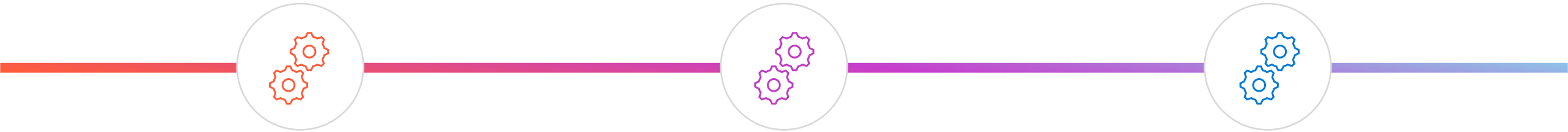
Enterprise application properties

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



© Copyright Microsoft Corporation. All rights reserved.

Configure app properties



Enabled for users to sign in?

User assignment required?

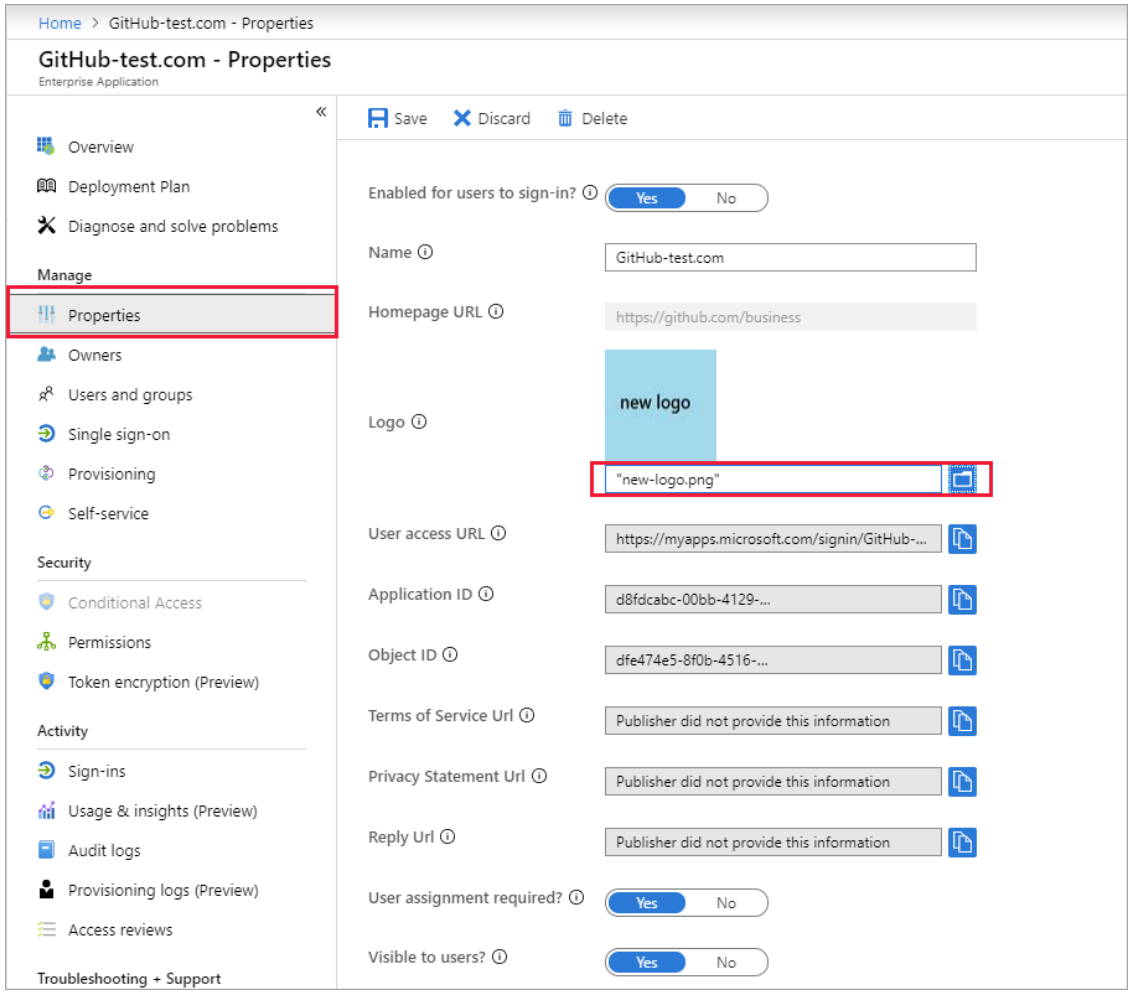
Visible to users?

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	• Assigned users can see the app and sign in. • Unassigned users cannot see the app and cannot sign in.
Yes	Yes	No	• Assigned users cannot see the app but they can sign in. • Unassigned users cannot see the app and cannot sign in.
Yes	No	Yes	• Assigned users can see the app and sign in. • Unassigned users cannot see the app but can sign in.

© Copyright Microsoft Corporation. All rights reserved.

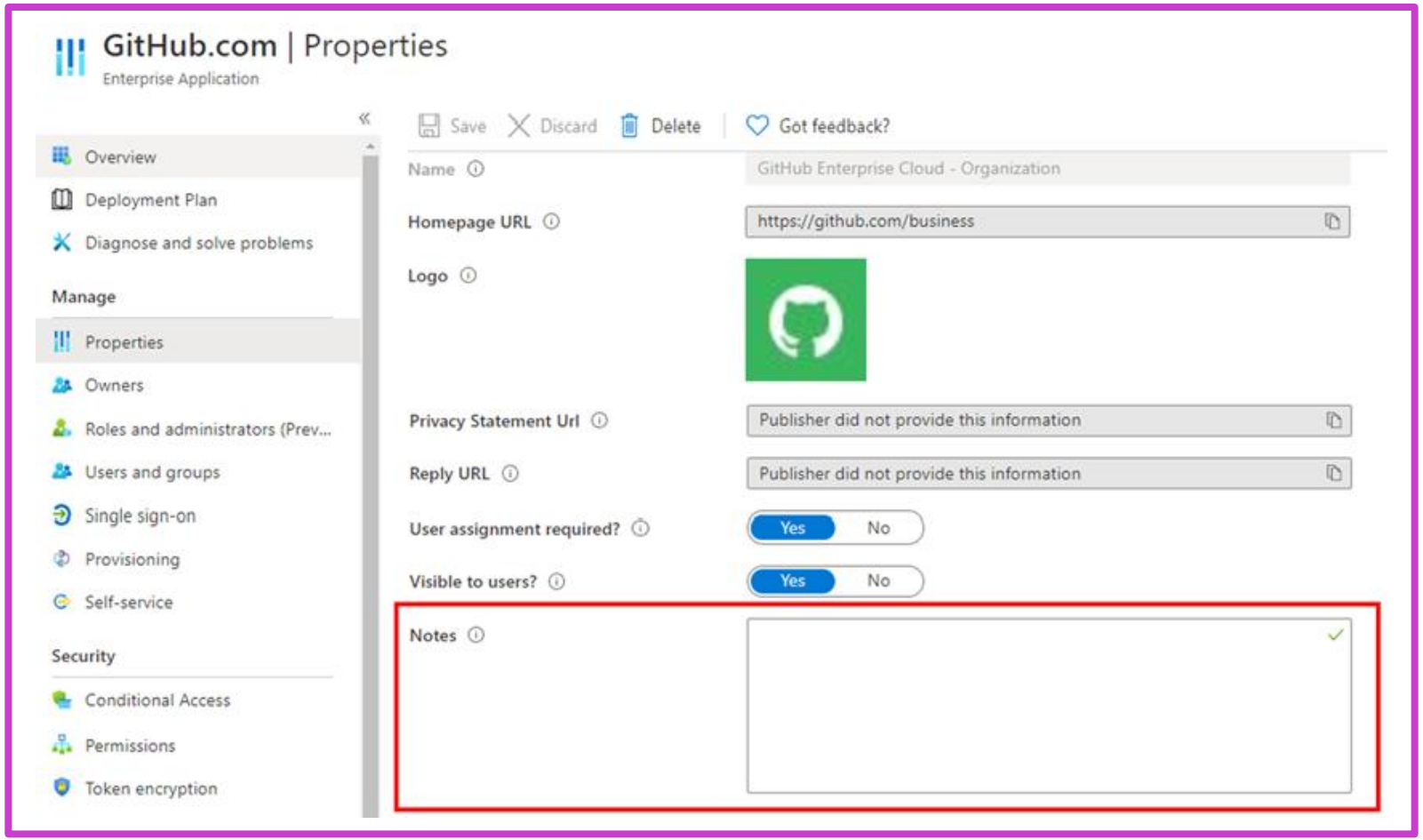
Custom logo



© Copyright Microsoft Corporation. All rights reserved.

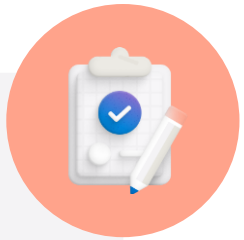
Add notes

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



© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

Implement and monitor the integration of enterprise apps for SSO

© Copyright Microsoft Corporation. All rights reserved.

Learning objectives

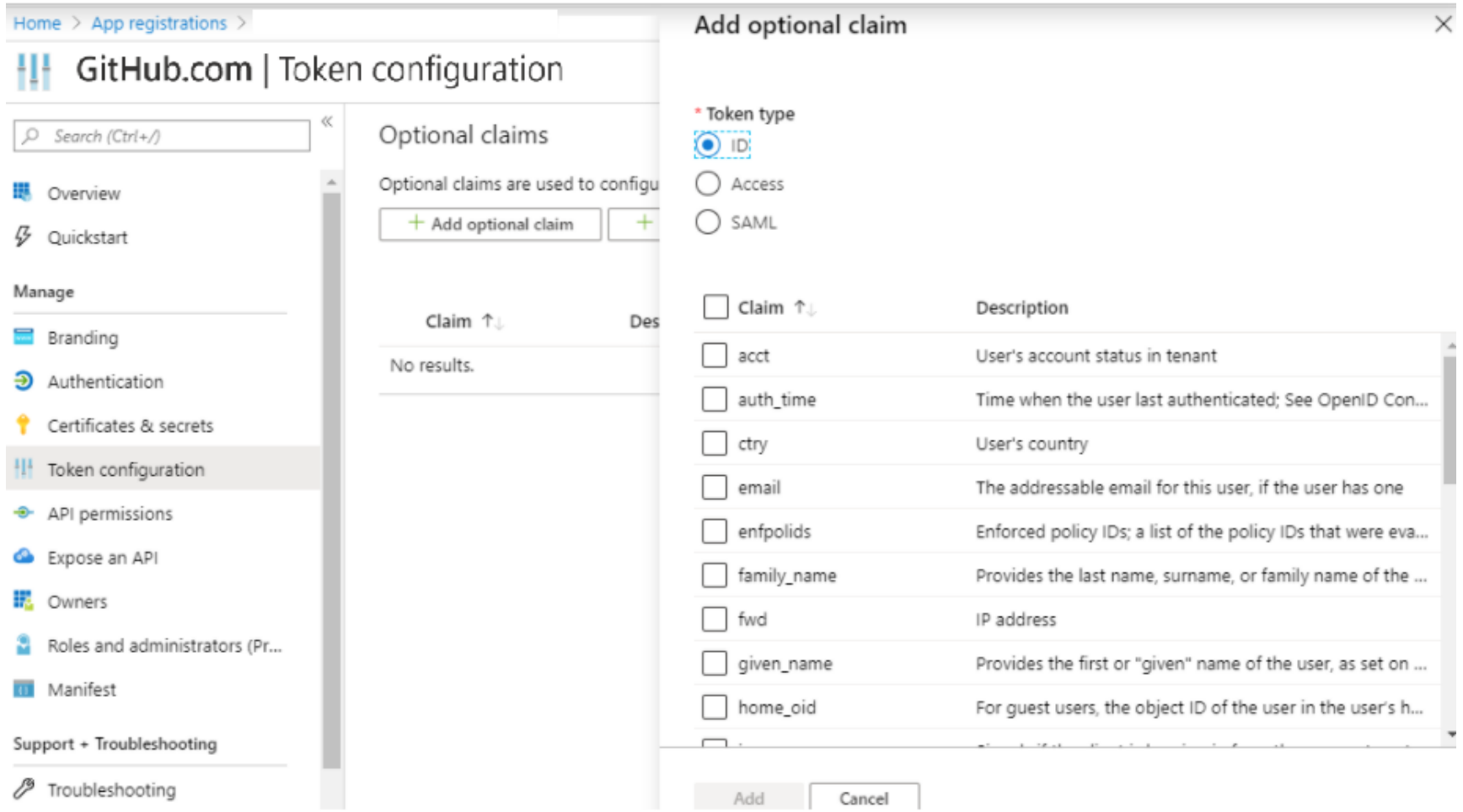
1. Implement token customizations
2. Implement and configure consent settings
3. Integrate on-premises apps by using Microsoft Entra application proxy
4. Integrate custom SaaS apps for SSO
5. Implement application user provisioning
6. Monitor and audit access/sign-on to Microsoft Entra ID integrated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

© Copyright Microsoft Corporation. All rights reserved.

Implement token customizations

© Copyright Microsoft Corporation. All rights reserved.

Token configuration – claims – SAML-based SSO



© Copyright Microsoft Corporation. All rights reserved.

Implement and configure consent settings

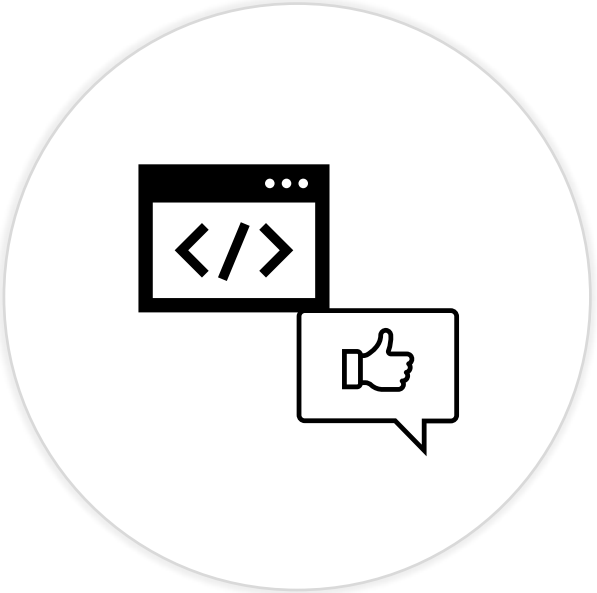
© Copyright Microsoft Corporation. All rights reserved.

Why is consent important?

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

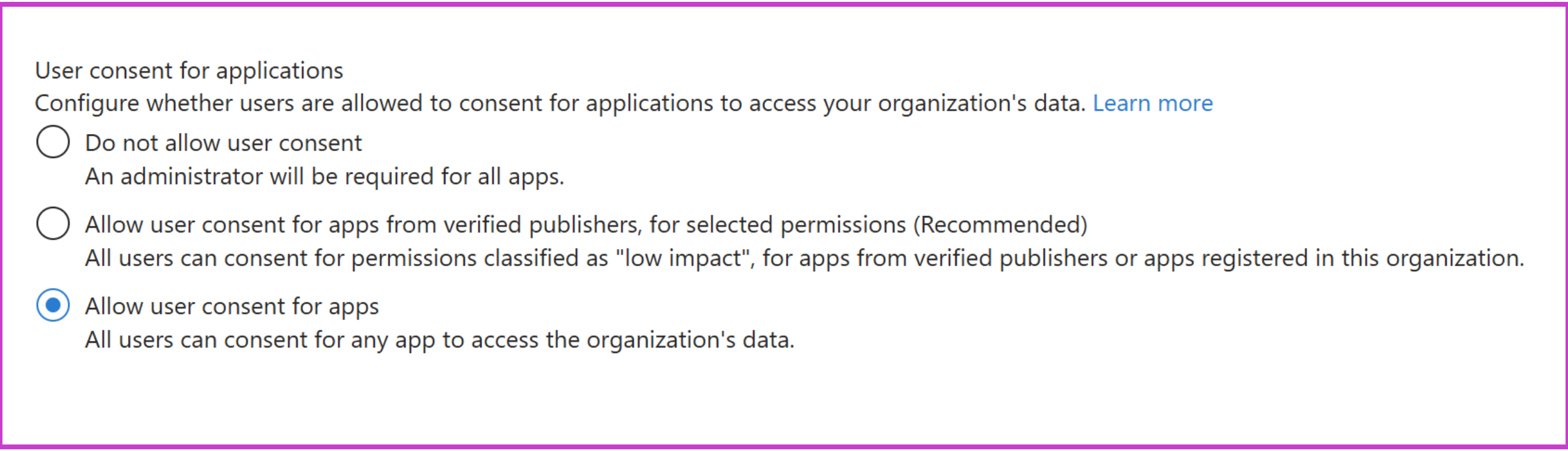
Users can allow apps access to specific information, like a mailbox, but not access to organization servers.

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



© Copyright Microsoft Corporation. All rights reserved.

What are Consent Settings?



- 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

© Copyright Microsoft Corporation. All rights reserved.

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

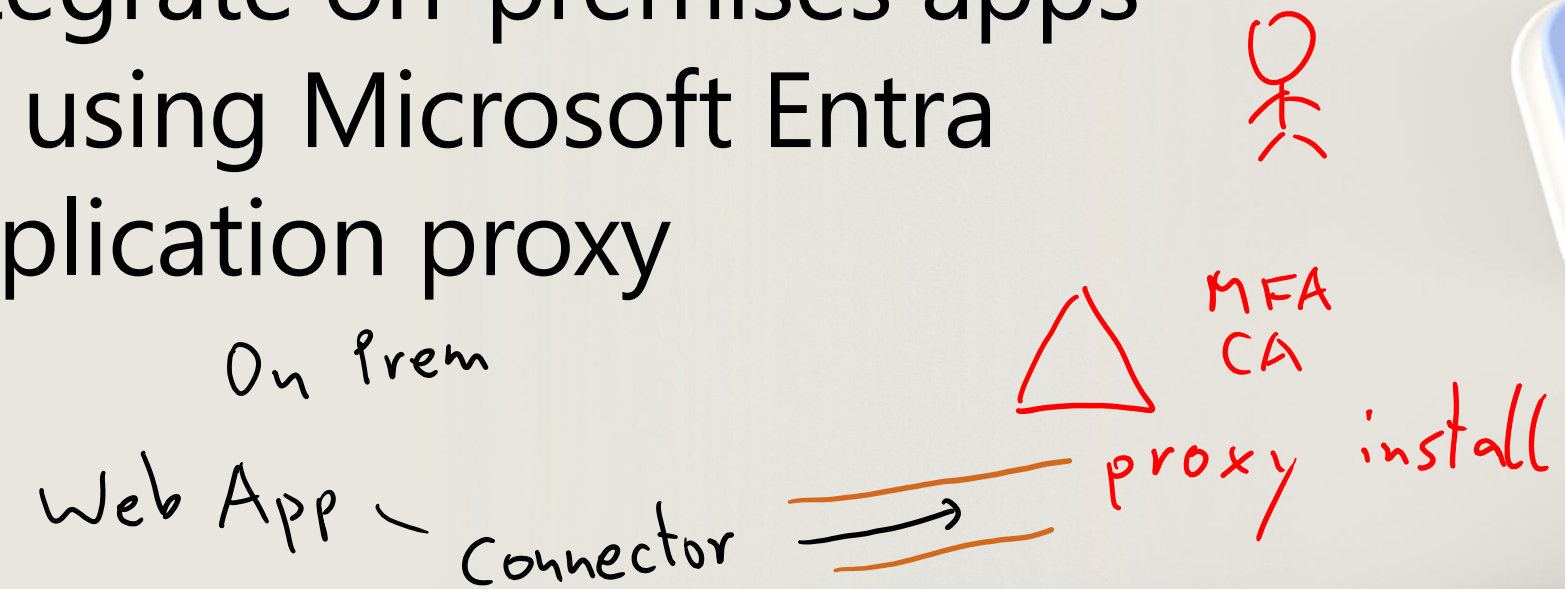
Users can consent to any permission.

Custom app consent policy

Users can consent to custom app consent policies.

© Copyright Microsoft Corporation. All rights reserved.

Integrate on-premises apps by using Microsoft Entra application proxy



© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

Value of Application Proxy

Protocol translation to/from modern authentication

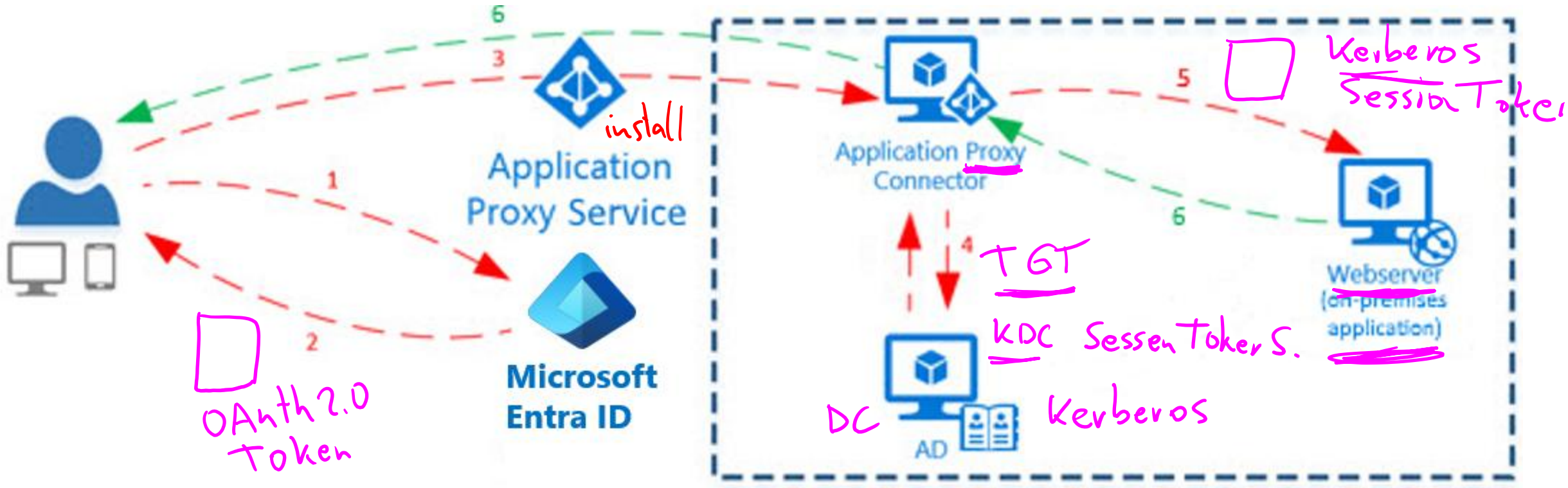
Example: Convert Kerberos token to a modern auth token

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

© Copyright Microsoft Corporation. All rights reserved.

Application Proxy



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

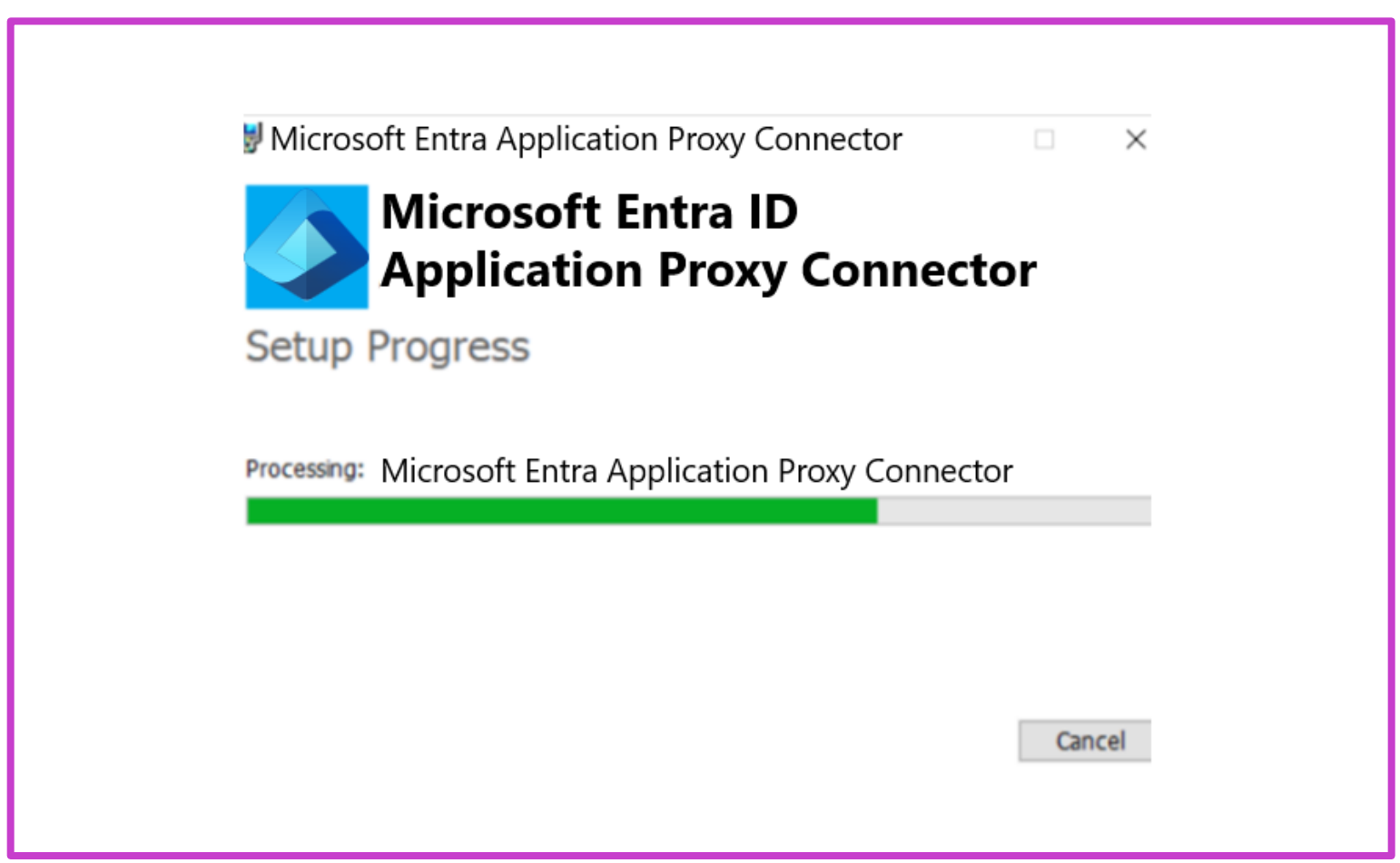
© Copyright Microsoft Corporation. All rights reserved.

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]



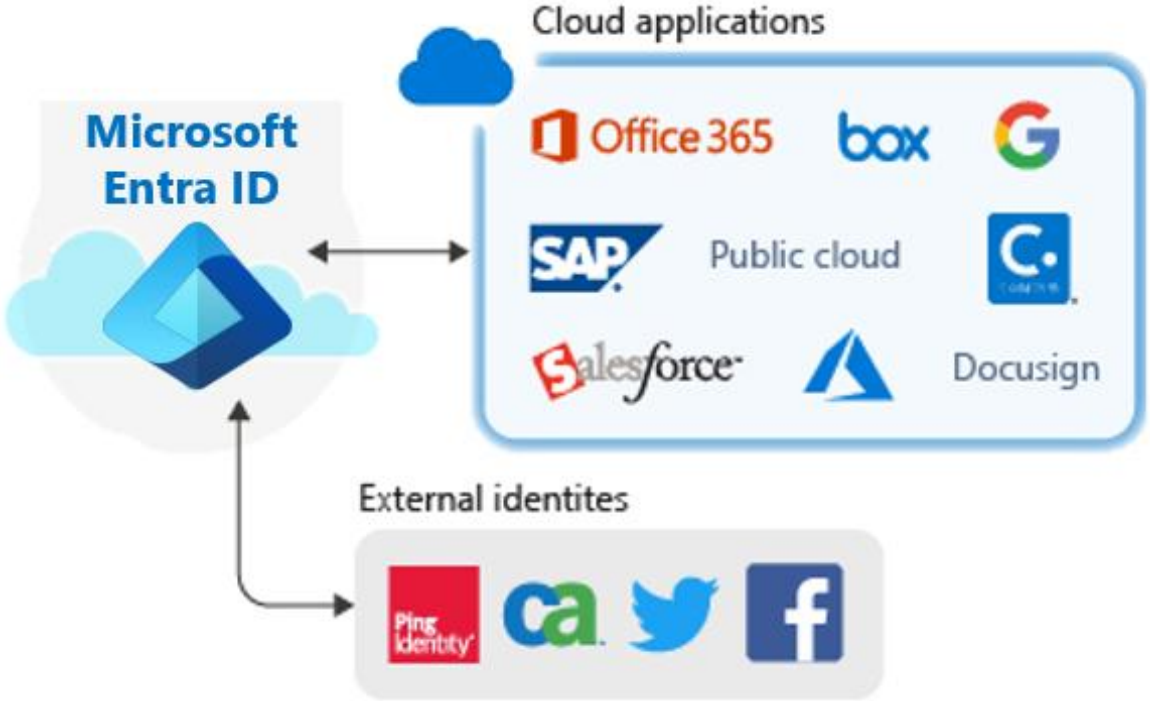
© Copyright Microsoft Corporation. All rights reserved.

Integrate custom SaaS apps for SSO

© Copyright Microsoft Corporation. All rights reserved.

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

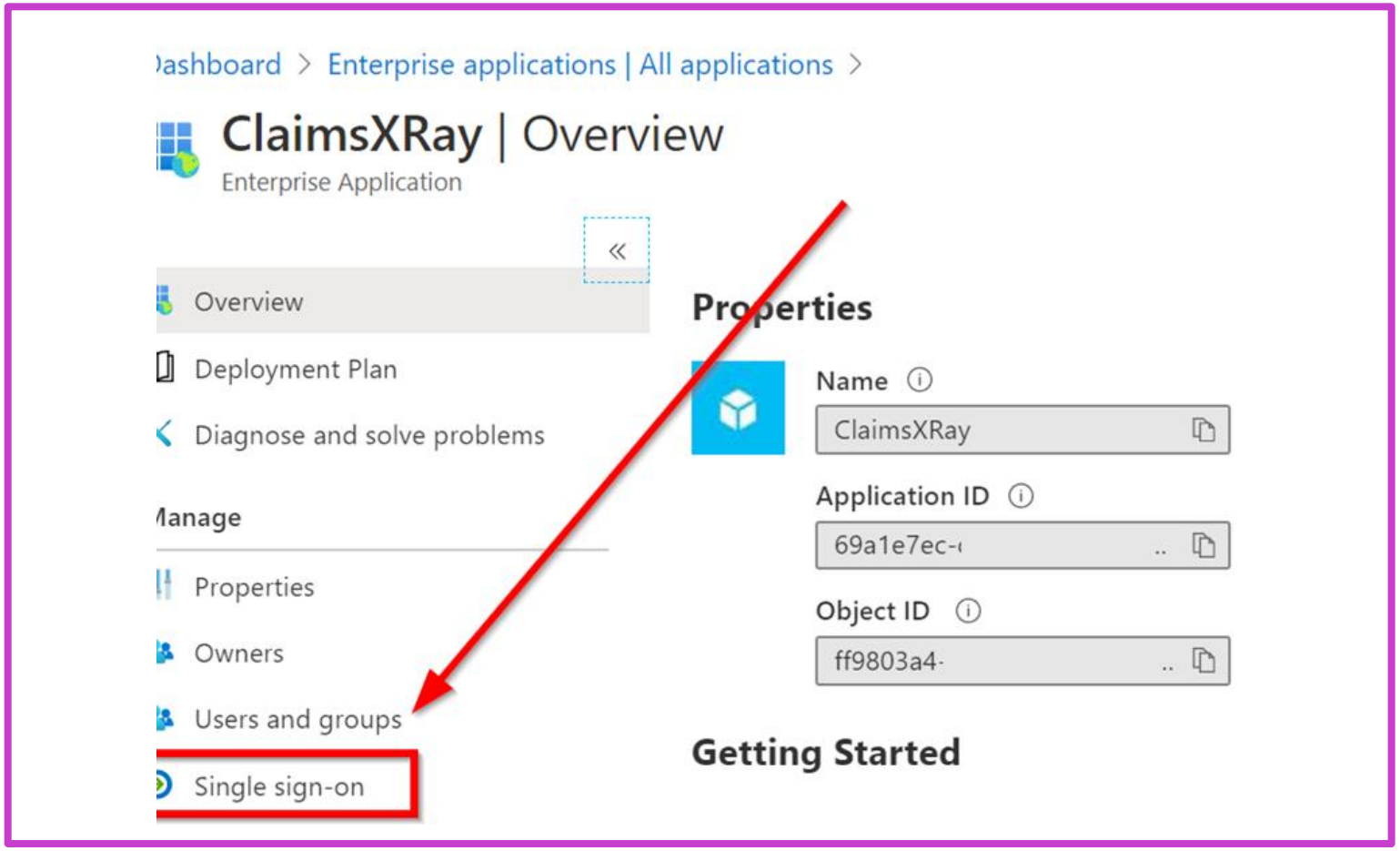
© Copyright Microsoft Corporation. All rights reserved.

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]

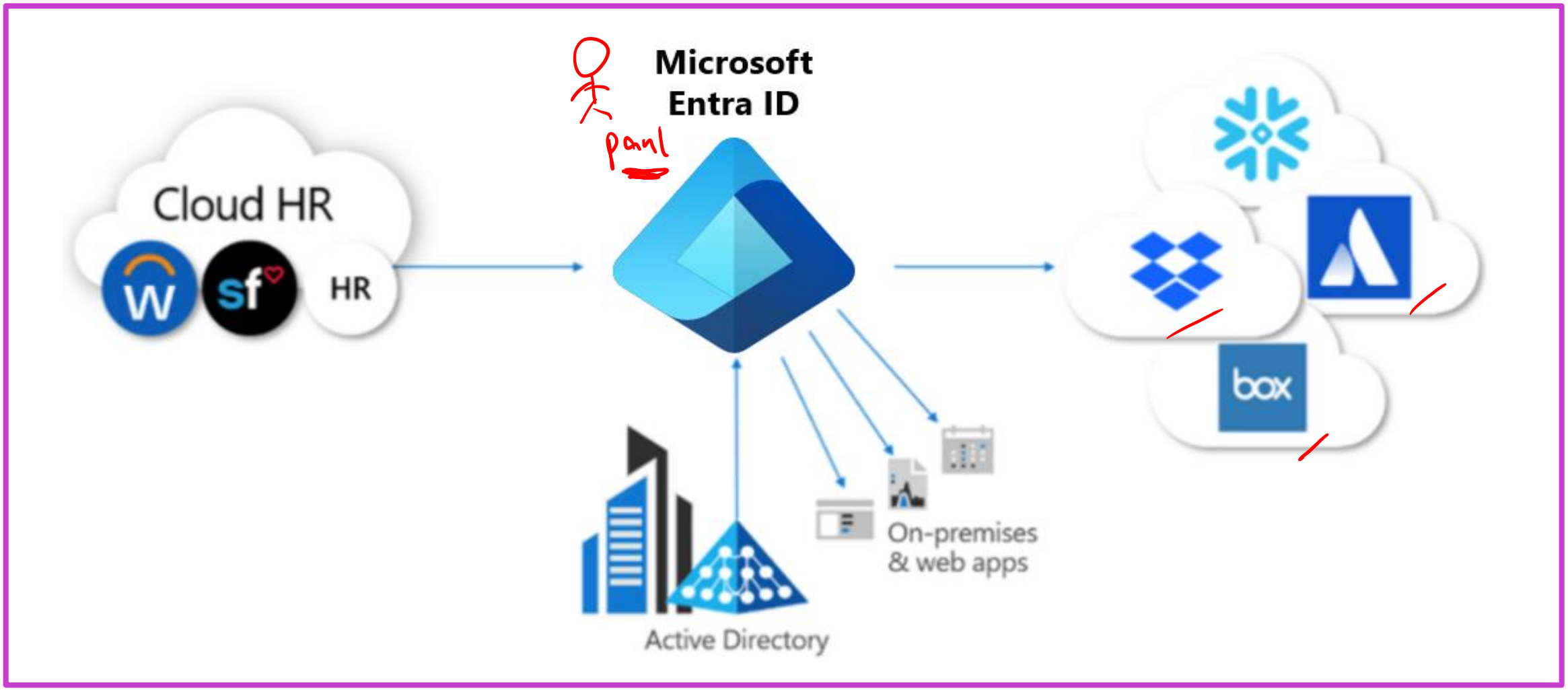


© Copyright Microsoft Corporation. All rights reserved.

Implement application user provisioning

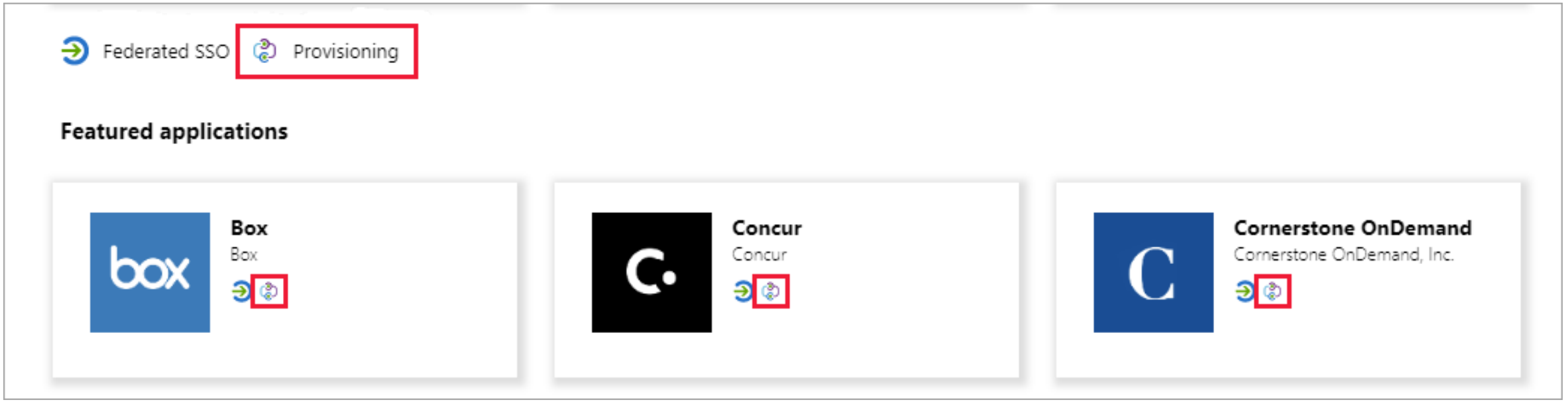
© Copyright Microsoft Corporation. All rights reserved.

Application user provisioning



© Copyright Microsoft Corporation. All rights reserved.

Manual vs. automatic provisioning



Manual provisioning

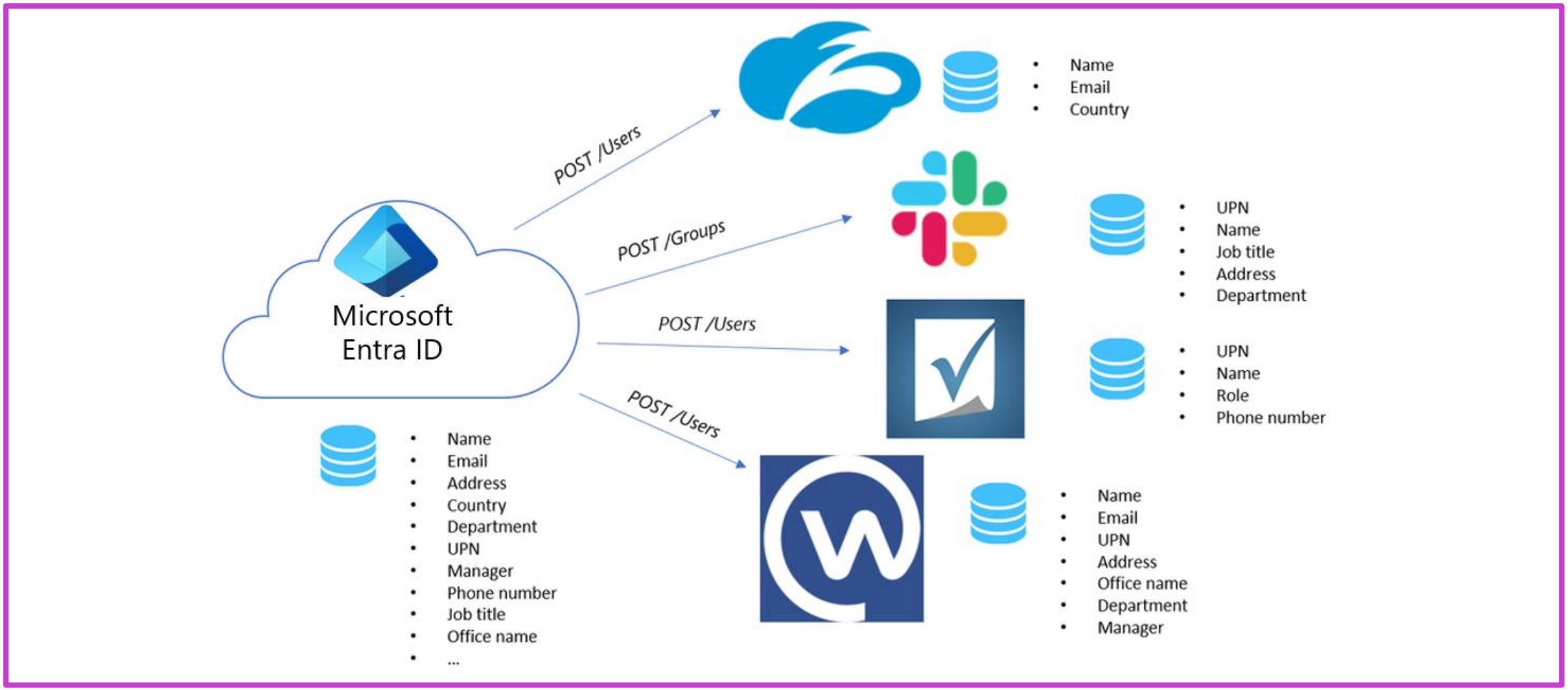
As yet, there is no automatic Microsoft Entra provisioning connector for the app yet. User accounts must be created manually.

Automatic provisioning

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

© Copyright Microsoft Corporation. All rights reserved.

SCIM provisioning overview



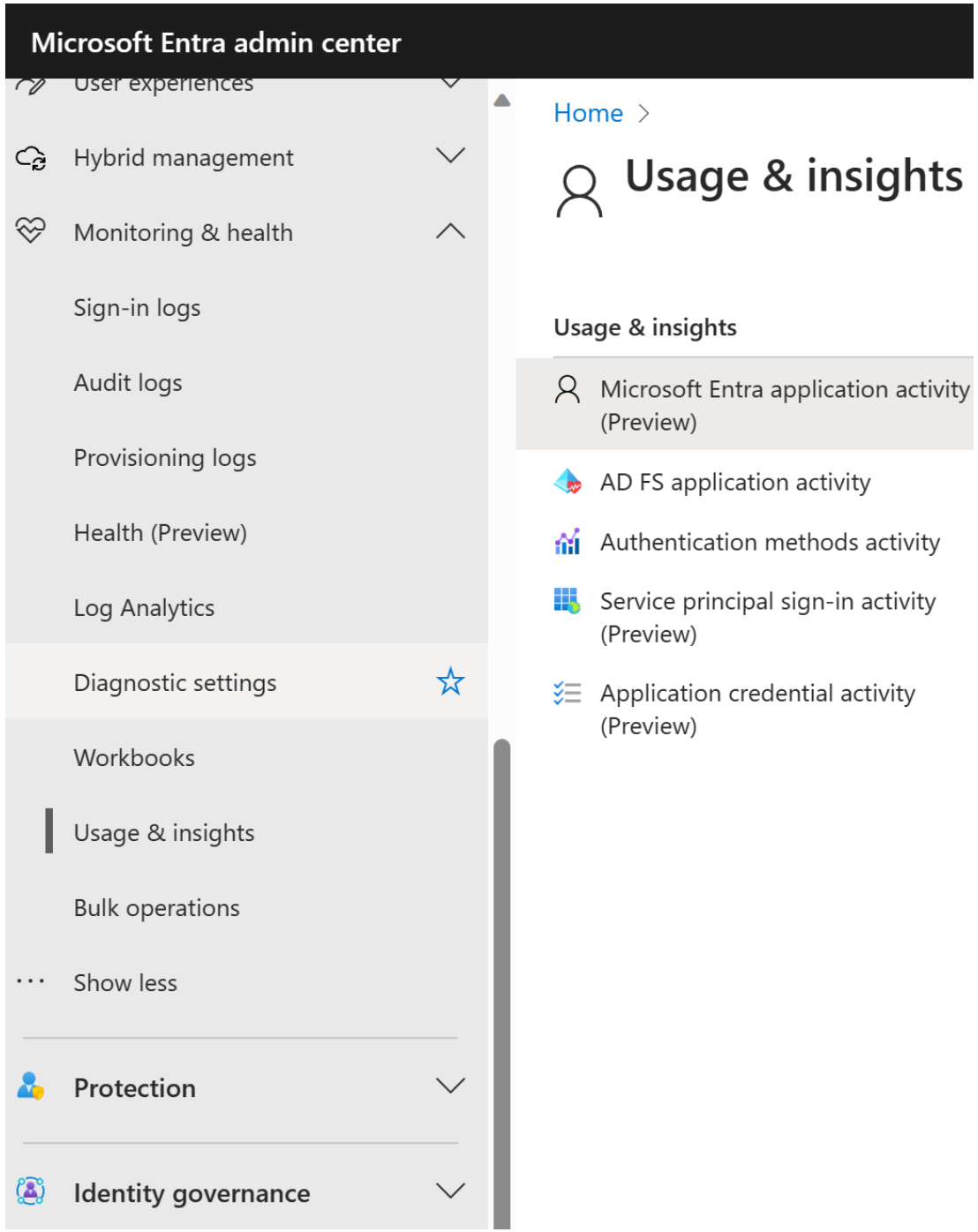
© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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?

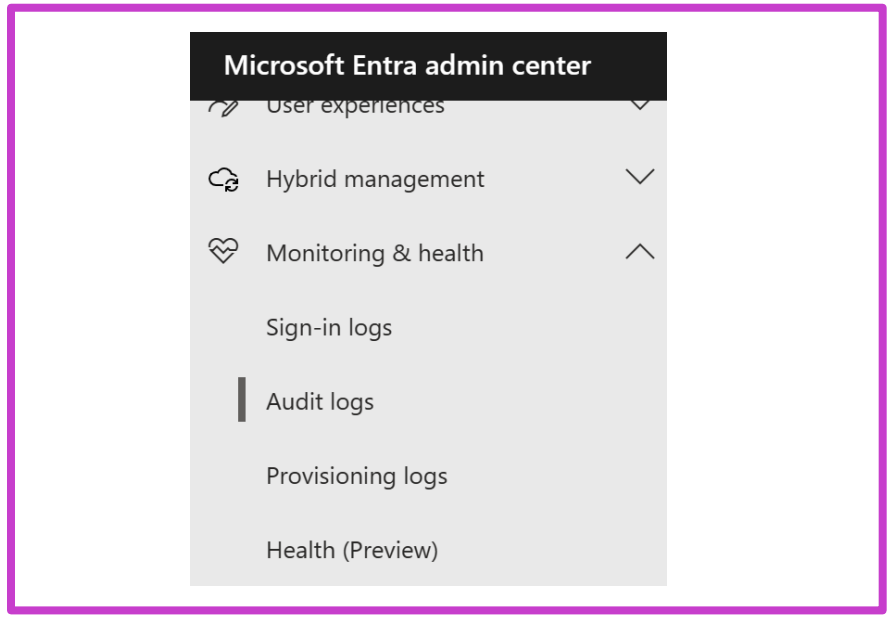


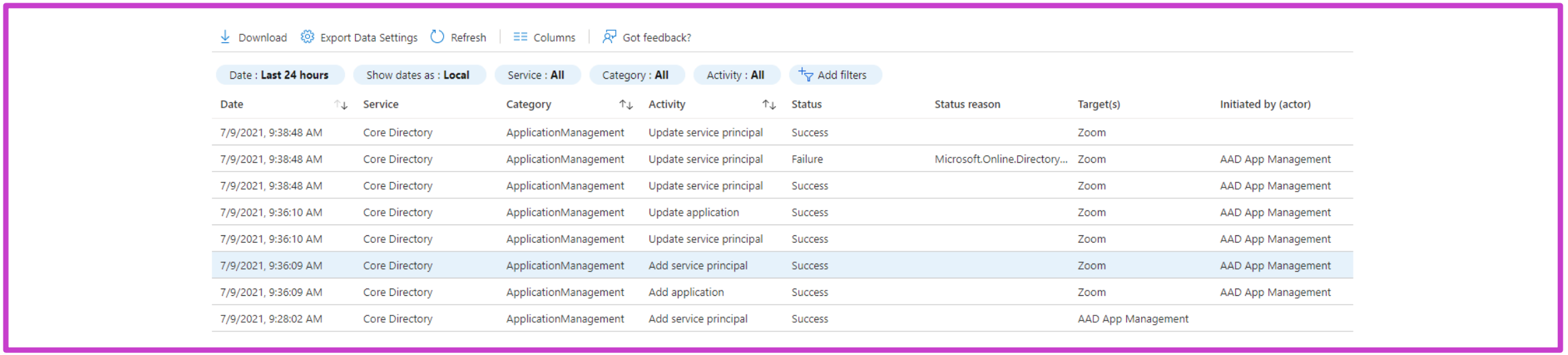
© Copyright Microsoft Corporation. All rights reserved.

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





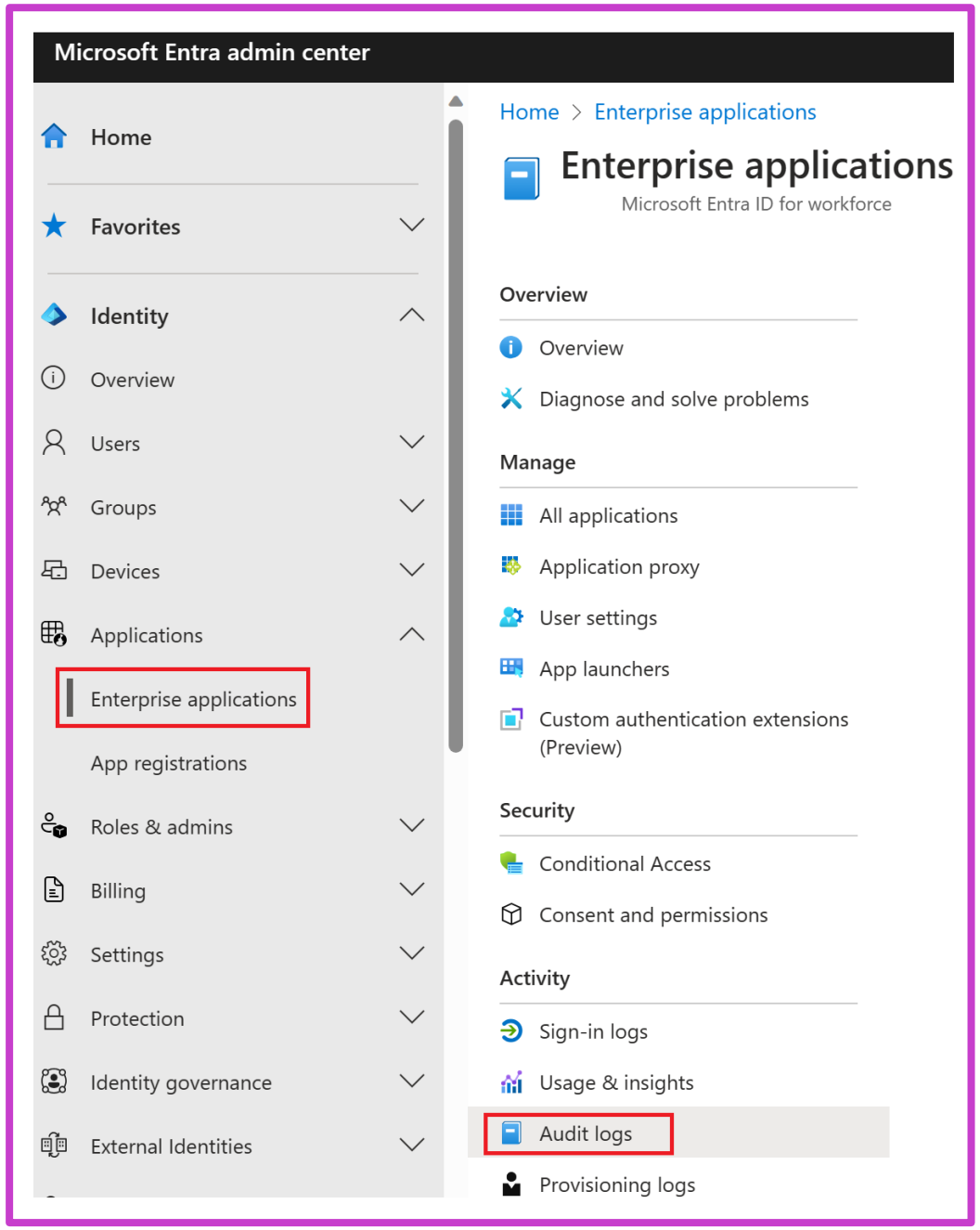
Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
7/9/2021, 9:38:48 AM	Core Directory	ApplicationManagement	Update service principal	Success		Zoom	
7/9/2021, 9:38:48 AM	Core Directory	ApplicationManagement	Update service principal	Failure	Microsoft.Online.Directory...	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	

© Copyright Microsoft Corporation. All rights reserved.

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?



© Copyright Microsoft Corporation. All rights reserved.

Create and manage application collections

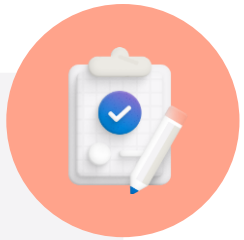
© Copyright Microsoft Corporation. All rights reserved.

Create app collections

Create an admin application collection	Create a collection using the My Apps portal
1. Go to Microsoft Entra ID then select Enterprise Applications. 2. Under Manage, select App Launchers. 3. Select New collection. 4. In the New collection page, enter a Name and Description. 5. Select the Applications tab. Select + Add application to open the Add applications page. 6. Select all the applications you want to add. 7. When you're finished adding applications, select Add. 8. Select the Owners tab. Select + Add users and groups. 9. Select Review + Create. The properties for the new collection appear.	1. Open the My Apps portal. 2. Select the ellipsis (...) on the apps screen. 3. Choose Manage collections. 4. Select Create collection. 5. Select the + Add apps option to add all the apps you want in the collection. 6. After picking your apps, select the Add selected apps button. 7. Give the collection a name and choose Create collection.

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Implement app registrations

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Plan your line-of-business application registration strategy

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Application objects and service principals

Application objects:

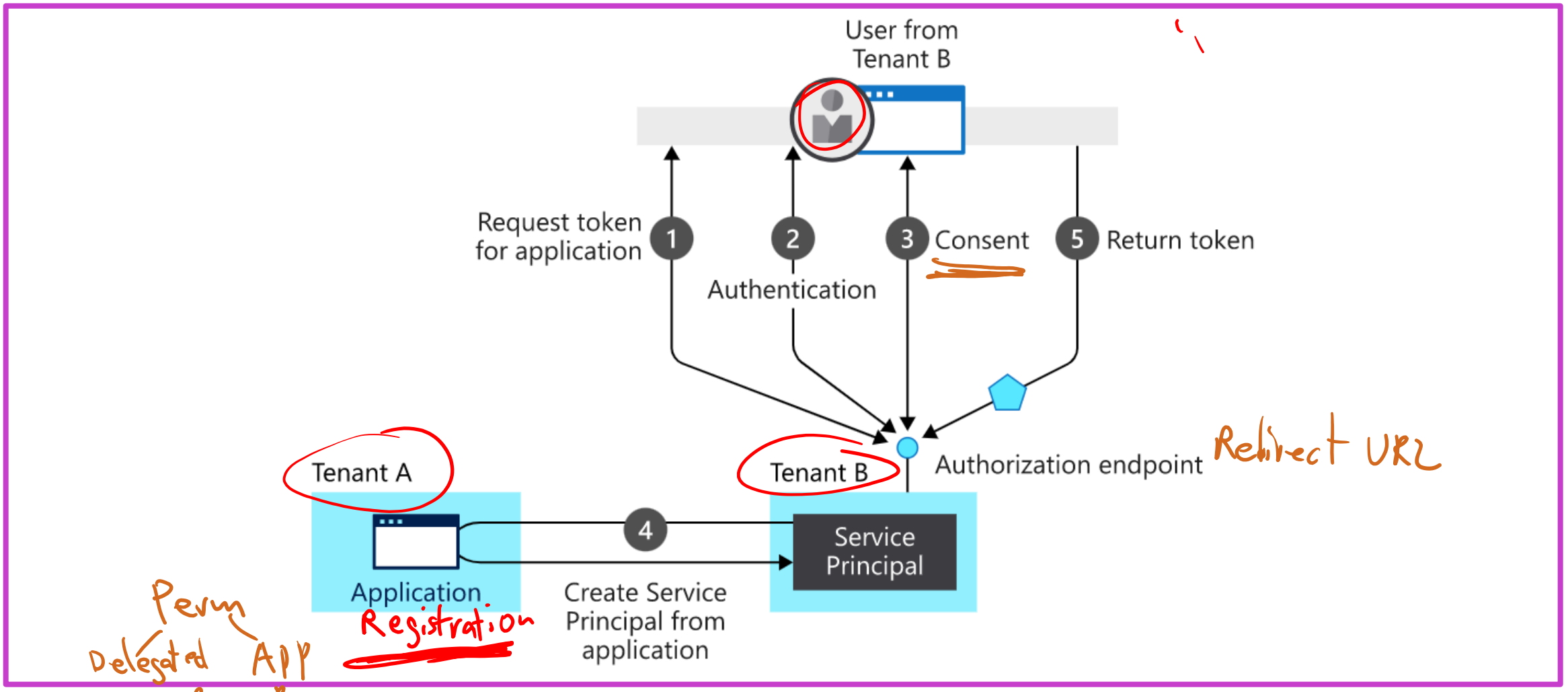
- Define and describe the application to Microsoft Entra ID, enabling it to know how to issue tokens based on its settings
- Will only exist in their tenant

Service principals

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

© Copyright Microsoft Corporation. All rights reserved.

New app registration



© Copyright Microsoft Corporation. All rights reserved.

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

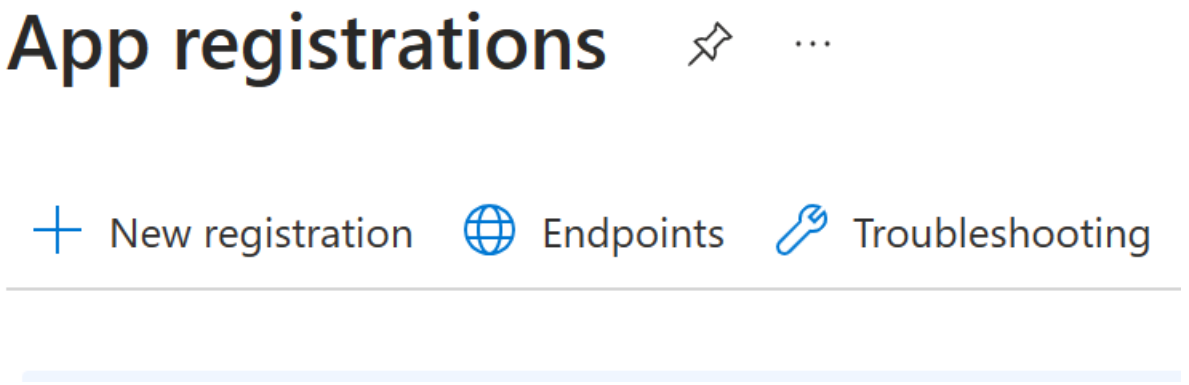
- By default, all users in your directory have rights to register application objects they are developing, and they have discretion over which applications they share or give access to their organizational data through consent.
- When the first user in your directory signs into an application and grants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

© Copyright Microsoft Corporation. All rights reserved.

Implement application registrations

© Copyright Microsoft Corporation. All rights reserved.

Demo: Register and application



© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

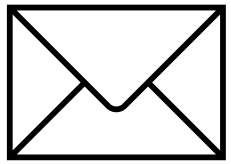
Configure application permissions

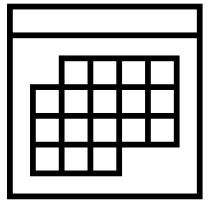
© Copyright Microsoft Corporation. All rights reserved.

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





© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

OpenID connect scopes

Access Token
Claim scp:
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.

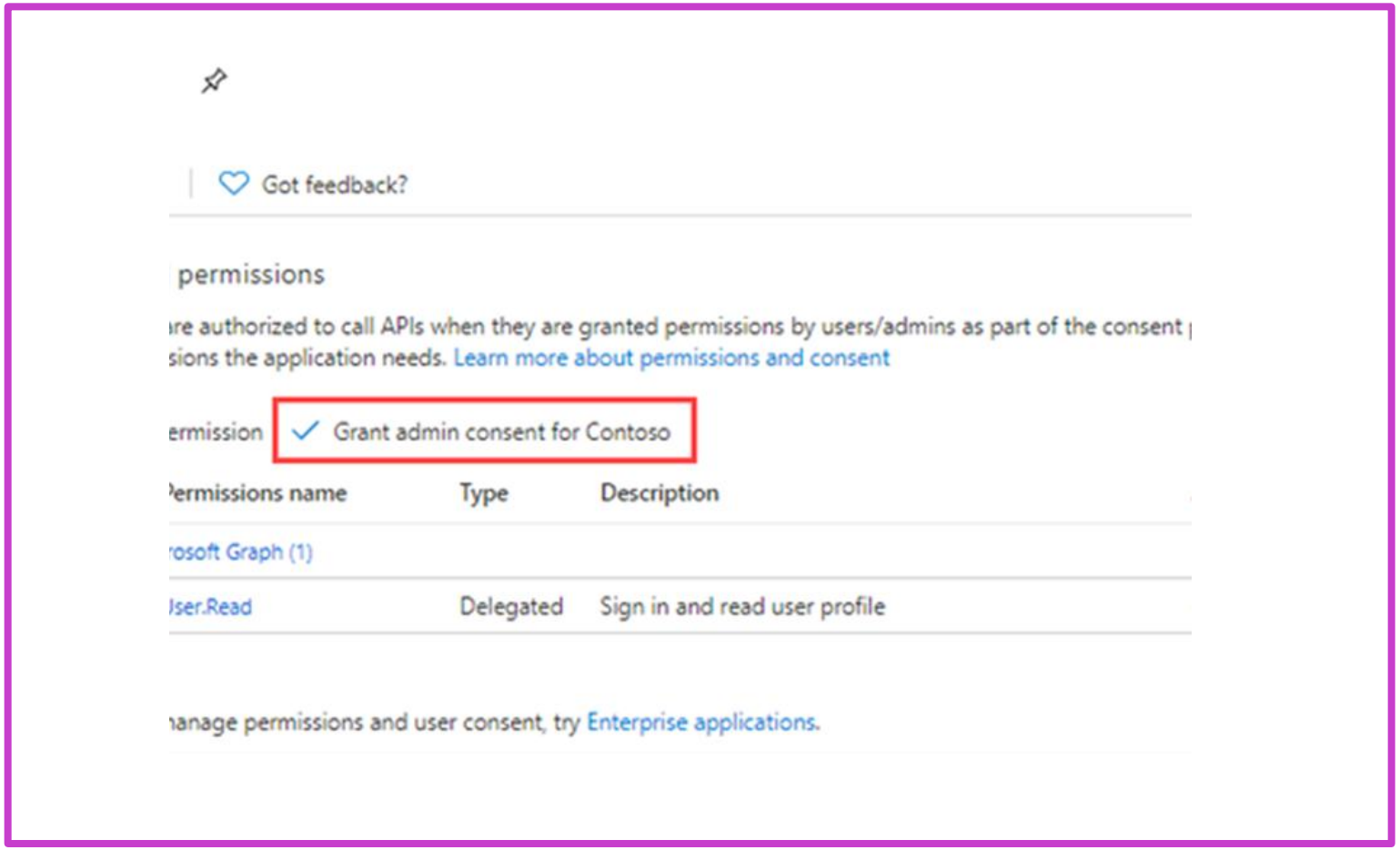
© Copyright Microsoft Corporation. All rights reserved.

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]



© Copyright Microsoft Corporation. All rights reserved.

Implement application authorization

© Copyright Microsoft Corporation. All rights reserved.

Application roles

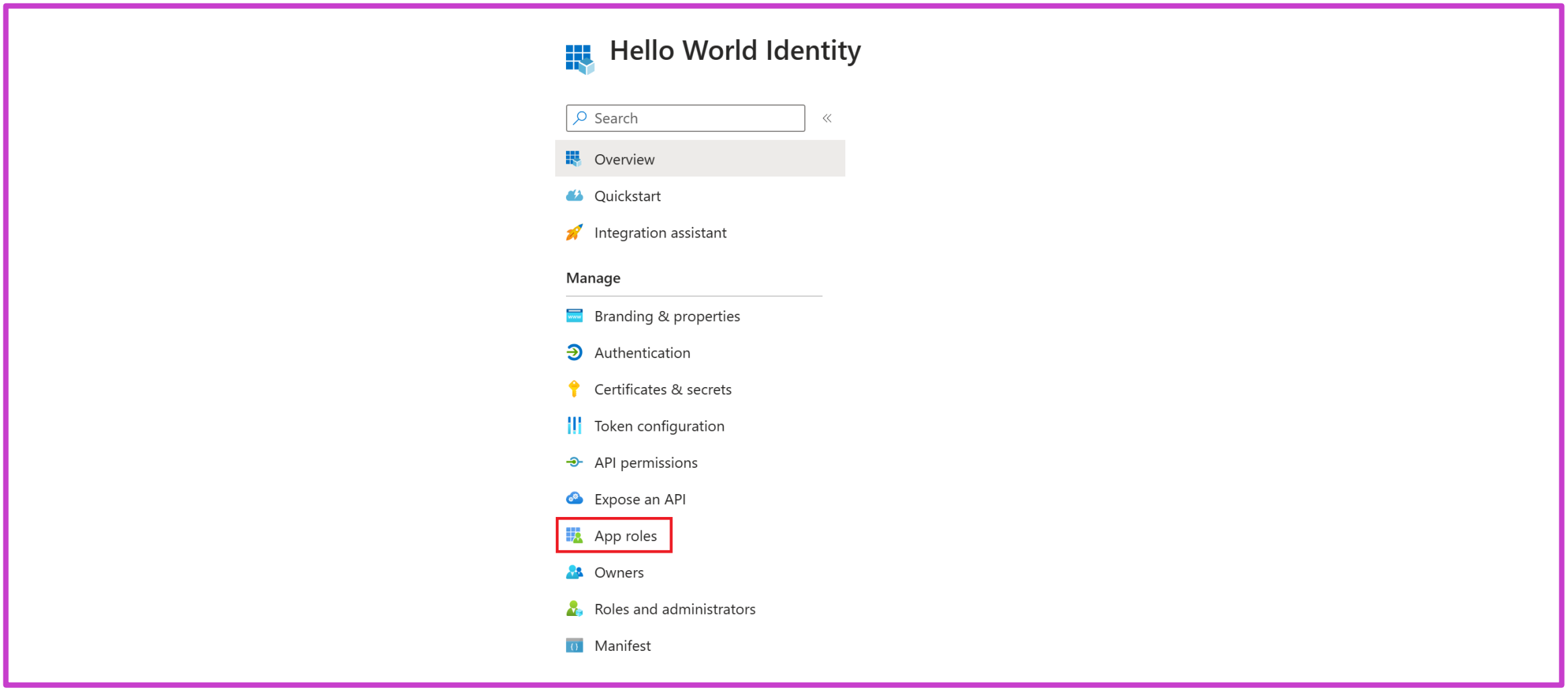
Application roles are used to assign permissions to users. You define app roles by using the Microsoft Entra admin center. When a user signs into the application, Microsoft Entra ID emits a roles claim for each role that the user has been granted individually and from their group membership.

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

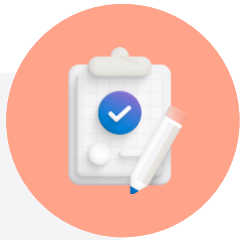
© Copyright Microsoft Corporation. All rights reserved.

Demo: Add app roles to an application



© Copyright Microsoft Corporation. All rights reserved.

Summary

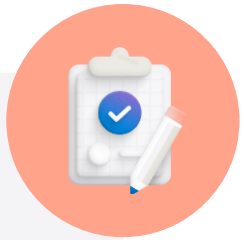


Now that you have reviewed this section, you should be able to:

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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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 Defender for Cloud Apps.	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

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

End of presentation

© Copyright Microsoft Corporation. All rights reserved.