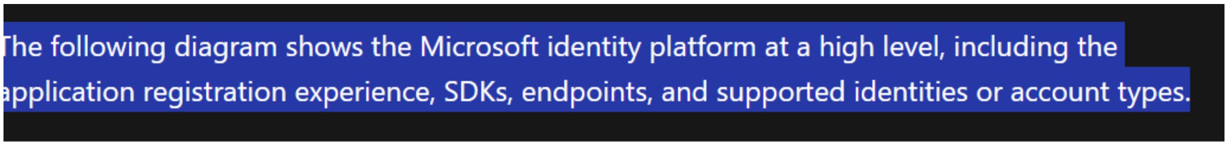
What is the Microsoft identity platform?

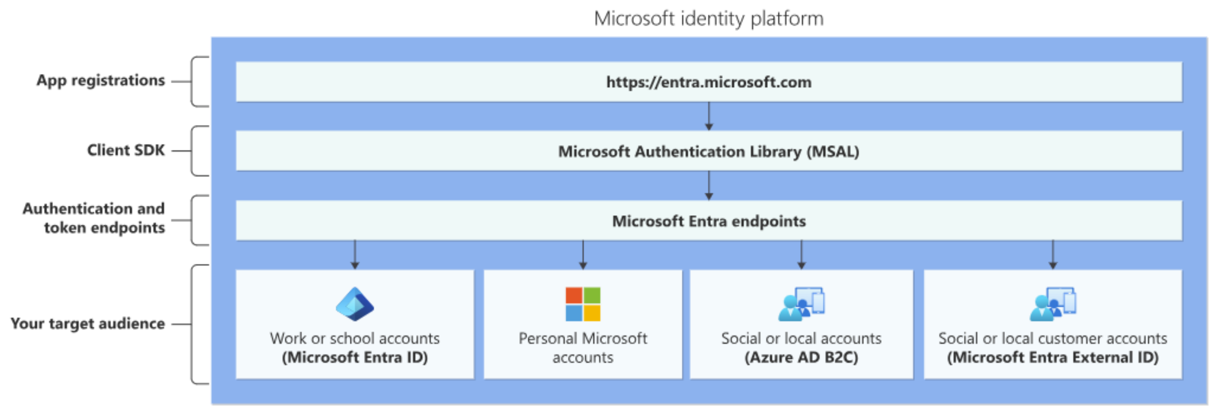
The Microsoft identity platform is a cloud identity service that allows you to build applications your users and customers can sign in to using their Microsoft identities or social accounts.

It authorizes access to your own APIs or Microsoft APIs like Microsoft Graph. The identity platform supports developers building single-tenant, line-of-business (LOB) applications, as well as multi-tenant software-as-a-service (SaaS) applications.
Microsoft Entra ID was previously known as Azure Active Directory (Azure AD).

The following diagram shows the Microsoft identity platform at a high level, including the application registration experience, SDKs, endpoints, and supported identities or account types.



The following diagram shows the Microsoft identity platform at a high level, including the application registration experience, SDKs, endpoints, and supported identities or account types.


Microsoft identity platform
App registrations
https://entra.microsoft.com
Client SDK
Microsoft Authentication Library (MSAL)
Authentication and token endpoints
Microsoft Entra endpoints
Your target audience
Work or school accounts (Microsoft Entra ID)
Personal Microsoft accounts
Social or local accounts (Azure AD B2C)
Social or local customer accounts (Microsoft Entra External ID)

There are several components that make up the Microsoft identity platform:

OAuth 2.0 and OpenID Connect standard-compliant authentication service enabling developers to authenticate several identity types, including:

- Work or school accounts, provisioned through Microsoft Entra ID
- Personal Microsoft accounts (Skype, Xbox, Outlook.com)
- Social or local accounts, by using Azure AD B2C
- Social or local customer accounts, by using Microsoft Entra External ID

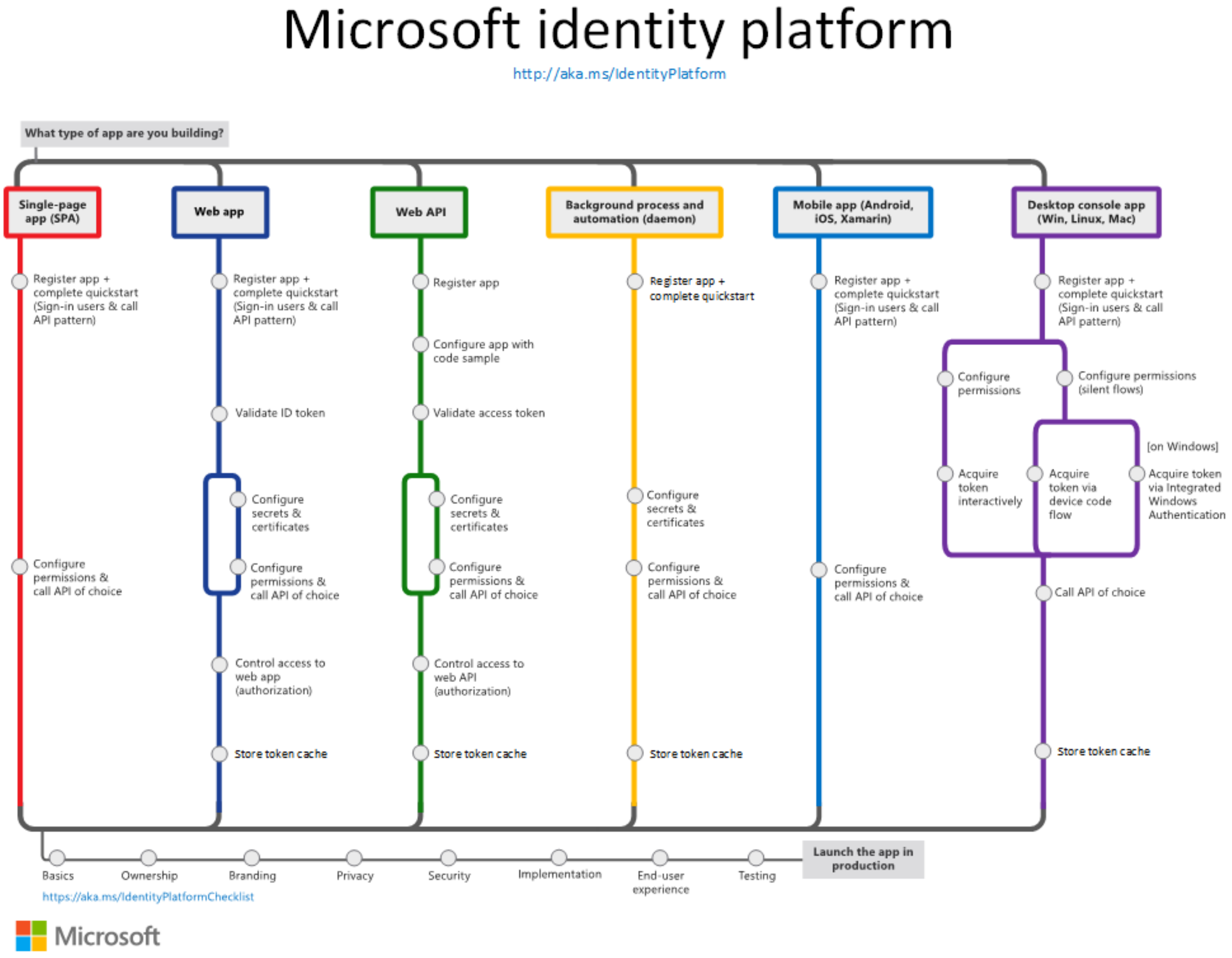
Open-source libraries: Microsoft Authentication Library (MSAL) and support for other standards-compliant libraries. The open source MSAL libraries are recommended as they provide built-in support for

Conditional Access scenarios, single sign-on (SSO) experiences for your users, built-in token caching support, and more. MSAL supports the different authorization grants and token flows used in different application types and scenarios.

Microsoft identity platform endpoint - The Microsoft identity platform endpoint is OIDC certified. It works with the Microsoft Authentication Libraries (MSAL) or any other standards-compliant library. It implements human readable scopes, in accordance with industry standards.

Application management portal: A registration and configuration experience in the Microsoft Entra admin center, along with the other application management capabilities.

Application configuration API and PowerShell: Programmatic configuration of your applications through the Microsoft Graph API and PowerShell so you can automate your DevOps tasks.


Microsoft identity platform
http://aka.ms/IdentityPlatform
What type of app are you building?
Single-page app (SPA)
Register app + complete quickstart (Sign-in users & call API pattern)
Configure permissions & call API of choice
Web app
Register app + complete quickstart (Sign-in users & call API pattern)
Validate ID token
Configure secrets & certificates
Configure permissions & call API of choice
Control access to web app (authorization)
Store token cache
Web API
Register app
Configure app with code sample
Validate access token
Configure secrets & certificates
Configure permissions & call API of choice
Control access to web API (authorization)
Store token cache
Background process and automation (daemon)
Register app + complete quickstart
Configure secrets & certificates
Configure permissions & call API of choice
Store token cache
Mobile app (Android, iOS, Xamarin)
Register app + complete quickstart (Sign-in users & call API pattern)
Configure permissions & call API of choice
Desktop console app (Win, Linux, Mac)
Register app + complete quickstart (Sign-in users & call API pattern)
Configure permissions
Configure permissions (silent flows)
Acquire token interactively
Acquire token via device code flow
[on Windows]
Acquire token via Integrated Windows Authentication
Call API of choice
Store token cache
Basics
Ownership
Branding
Privacy
Security
Implementation
End-user experience
Testing
Launch the app in production
https://aka.ms/IdentityPlatformChecklist
Microsoft

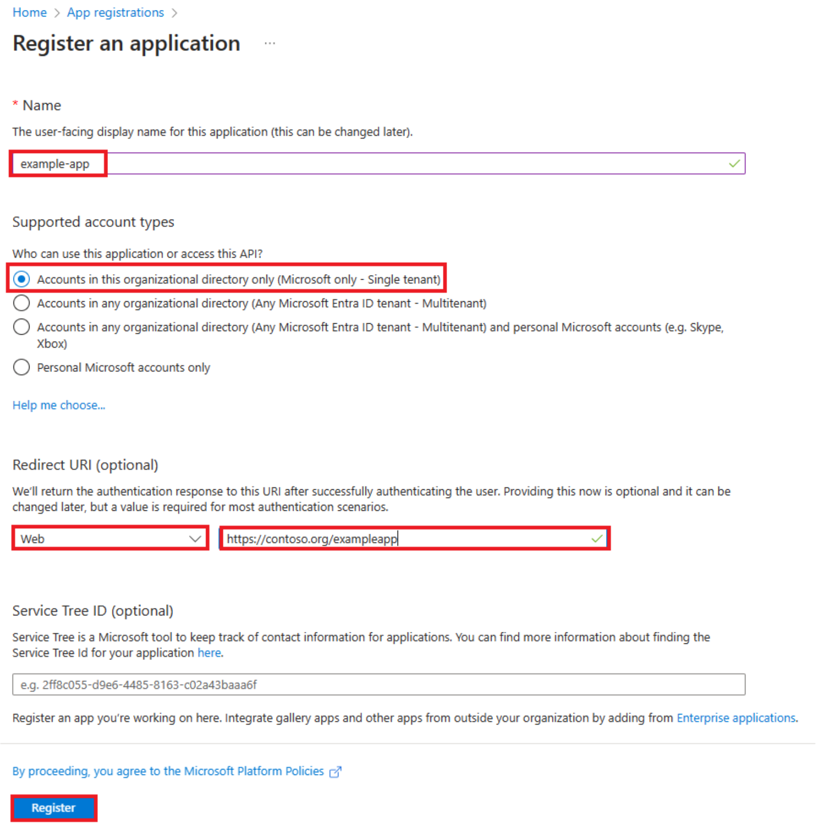
Azure AD B2C - Build customer-facing applications your users can sign in to using their social accounts like Facebook or Google, or by using an email address and password.

Microsoft Entra B2B - Invite external users into your Microsoft Entra tenant as "guest" users, and assign permissions for authorization while they use their existing credentials for authentication.

Microsoft Entra External ID - A customer identity and access management (CIAM) solution that lets you create secure, customized sign-in experiences for your customer-facing apps and services.

Register a Microsoft Entra app and create a service principal

Register an application with Microsoft Entra ID and create a service principal



Home > App registrations >

Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

example-app

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

https://contoso.org/exampleapp

Service Tree ID (optional)

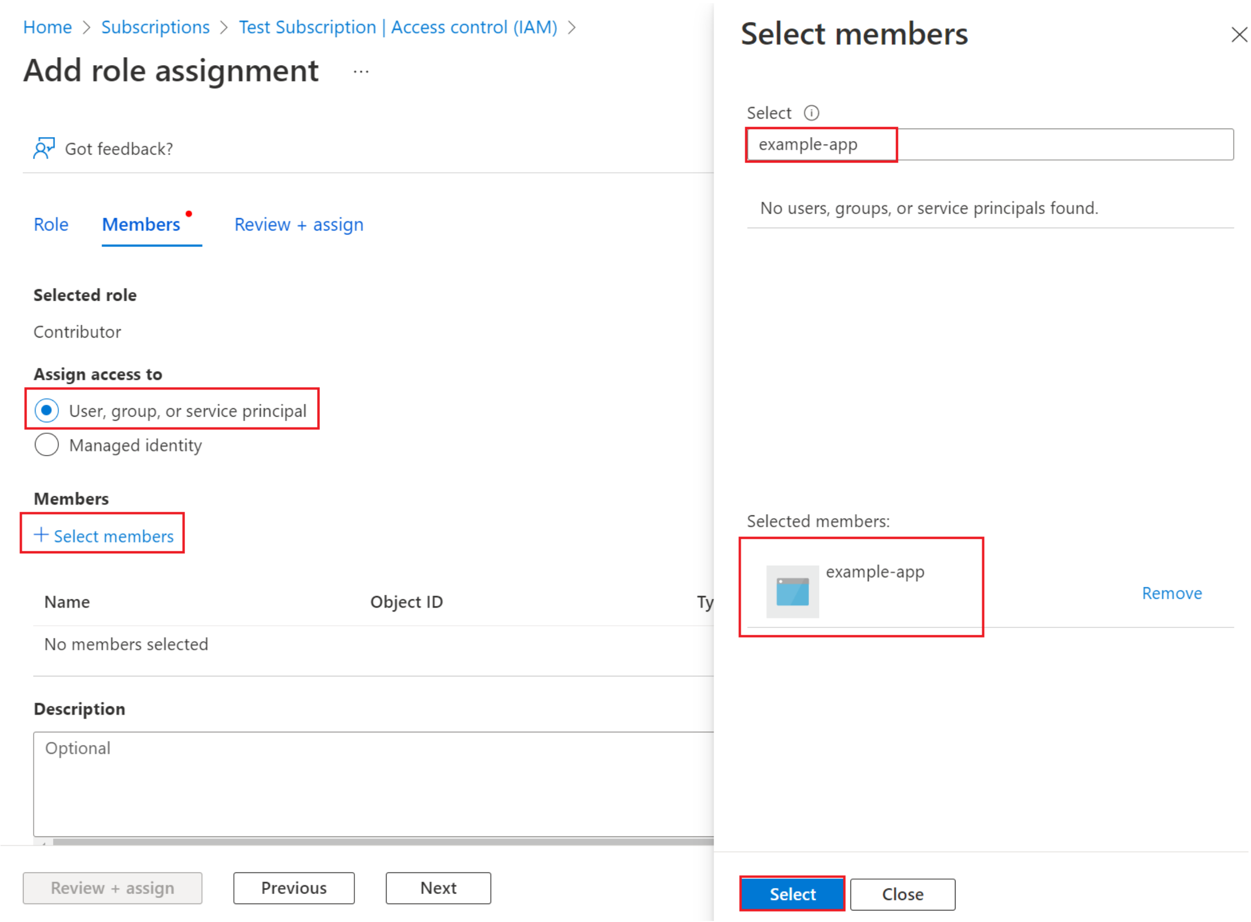
Service Tree is a Microsoft tool to keep track of contact information for applications. You can find more information about finding the Service Tree Id for your application here.

e.g. 2ff8c055-d9e6-4485-8163-c02a43baaa6f

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Assign a role to the application



Selected role

Contributor

Assign access to

● User, group, or service principal

○ Managed identity

Members

Name	Object ID	Ty
No members selected		

Description

Optional

Select: example-app

No users, groups, or service principals found.

Selected members:

example-app

Sign in to the application

1. Open the Microsoft Entra admin center Home page.
2. Browse to Identity > Applications > App registrations, then select your application.
3. On the app's overview page, copy the Directory (tenant) ID value and store it in your application code.
4. Copy the Application (client) ID value and store it in your application code.

Set up authentication

- There are two types of authentication available for service principals: password-based authentication (application secret) and certificate-based authentication.

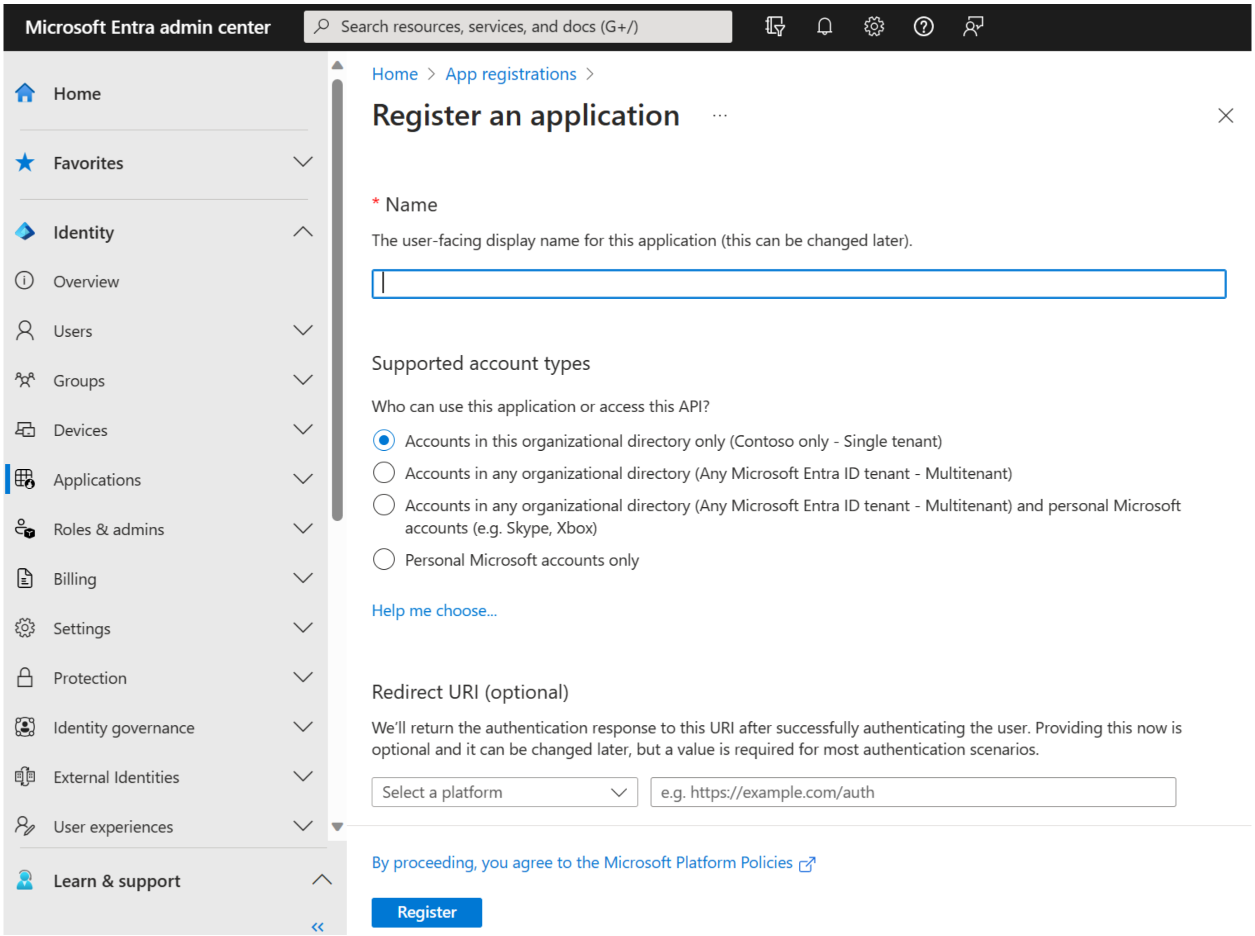
Configure access policies on resources

Quickstart: Register an application with the Microsoft identity platform

The Microsoft identity platform performs identity and access management (IAM) only for registered applications.

Whether it's a client application like a web or mobile app, or it's a web API that backs a client app, registering it establishes a trust relationship between your application and the identity provider, the Microsoft identity platform.

Register an application



Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Contoso only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the Microsoft Platform Policies

1.
2. Sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator.
3. If you have access to multiple tenants, use the **Settings** icon ⚙ in the top menu to switch to the tenant in which you want to register the application from the **Directories + subscriptions** menu.
4. Browse to **Identity** > **Applications** > **App registrations** and select **New registration**.
5. Enter a display **Name** for your application. Users of your application might see the display name when they use the app, for example during sign-in. You can change the display name at any time

and multiple app registrations can share the same name. The app registration's automatically generated Application (client) ID, not its display name, uniquely identifies your app within the identity platform.

6. Specify who can use the application, sometimes called its *sign-in audience*.

Supported account types	Description
Accounts in this organizational directory only	Select this option **if you're building an application for use only by users (or guests) in *your* tenant**. Often called a *line-of-business* (LOB) application, this app is a *single-tenant* application in the Microsoft identity platform.
Accounts in any organizational directory	Select this option **if you want users in *any* Microsoft Entra tenant to be able to use your application**. This option is appropriate if, for example, you're building a software-as-a-service **(SaaS) application** that you intend to provide to multiple organizations. This type of app is known as a *multitenant* application in the Microsoft identity platform.
Accounts in any organizational directory and personal Microsoft accounts	Select this option to target the widest set of customers. **By selecting this option, you're registering a *multitenant* application that can also support users who have personal *Microsoft accounts*.** Personal Microsoft accounts include Skype, Xbox, Live, and Hotmail accounts.
Personal Microsoft accounts	Select this option **if you're building an application only for users who have personal Microsoft accounts**. Personal Microsoft accounts include Skype, Xbox, Live, and Hotmail accounts.

7. Leave **Redirect URI (optional)** alone for now as you configure a redirect URI in the next section.
8. Select **Register** to complete the initial app registration.

A redirect URI is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication.

In a production web application, for example, the redirect URI is often a public endpoint where your app is running, like *https://contoso.com/auth-response.*

During development, it's common to also add the endpoint where you run your app locally, like https://127.0.0.1/auth-response or http://localhost/auth-response.

Be sure that any unnecessary development environments/redirect URIs are not exposed in the production app. This can be done by having separate app registrations for development and production.

Configure optional claims

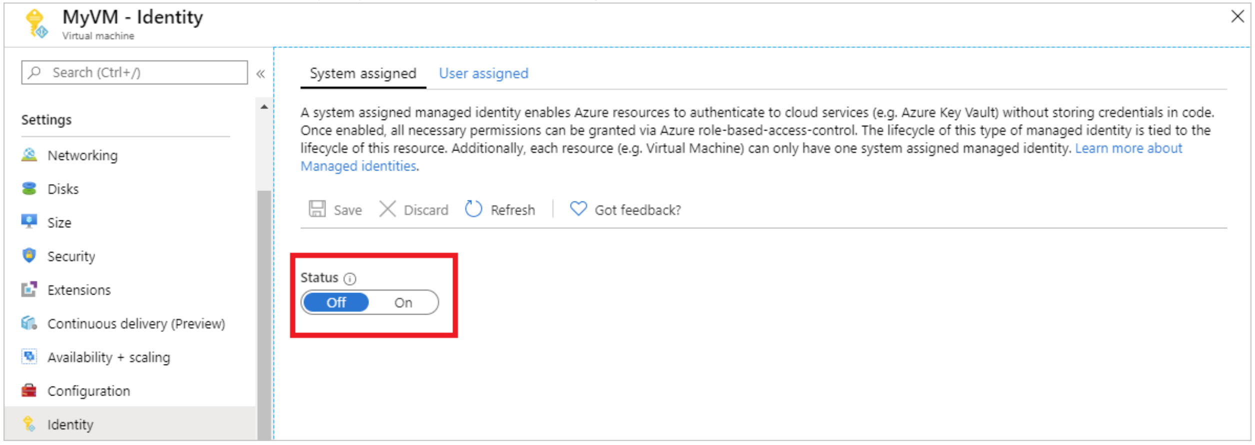
Tokens that Microsoft Entra returns are kept smaller to ensure optimal performance by clients that request them. As a result, several claims are no longer present in the token by default and must be asked for specifically on a per-application basis.

Use a Windows VM/VMSS to access Azure resources

Managed identities for Azure resources is a feature of Microsoft Entra ID. Each of the Azure services that support managed identities for Azure resources are subject to their own timeline.

Enable

Enabling a system-assigned managed identity is a one-click experience. You can either enable it during the creation of a VM or in the properties of an existing VM.



A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. Learn more about Managed identities.

Status ⓘ [✓ Off] On

Grant access

You can grant your VM access to files and folders in an Azure Data Lake Store. For this step, you can use an existing Data Lake Store or create a new one.

Make a request to the local managed identities for Azure resources endpoint to get an access token for Azure Data Lake Store.

```
$response = Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fdatalake.azure.net%2F' -Method GET -Headers @{Metadata="true"}
```

Convert the response from a JSON object to a PowerShell object.

```
$content = $response.Content | ConvertFrom-Json
```

Extract the access token from the response.

```
$AccessToken = $content.access_token
```

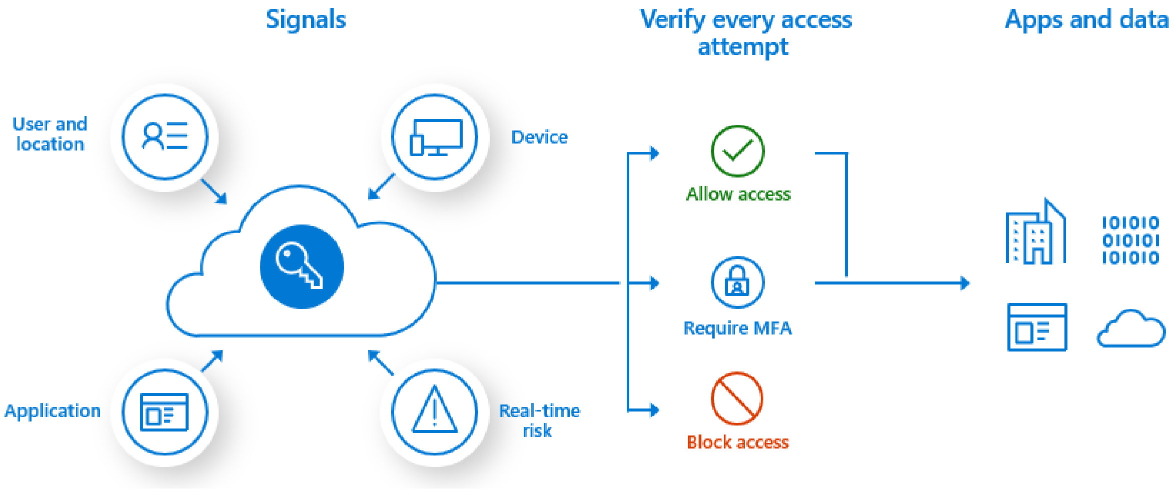
Tutorial: Secure user sign-in events with Microsoft Entra multifactor authentication

Multifactor authentication is a process in which a user is prompted for additional forms of identification during a sign-in event.

For example, the prompt could be to **enter a code on their cellphone** or to **provide a fingerprint scan**. When you require a second form of identification, security is increased because this additional factor isn't easy for an attacker to obtain or duplicate.

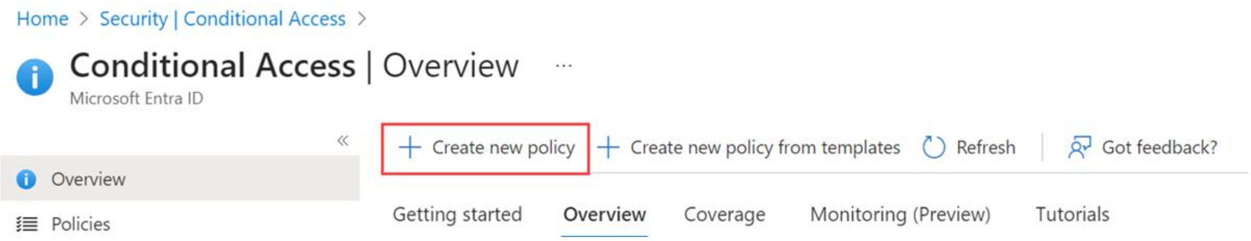
Microsoft Entra multifactor authentication and Conditional Access policies give you the flexibility to require MFA from users for specific sign-in events.

- Create a Conditional Access policy to enable Microsoft Entra multifactor authentication for a group of users.
- Configure the policy conditions that prompt for MFA.
- Test configuring and using multifactor authentication as a user.



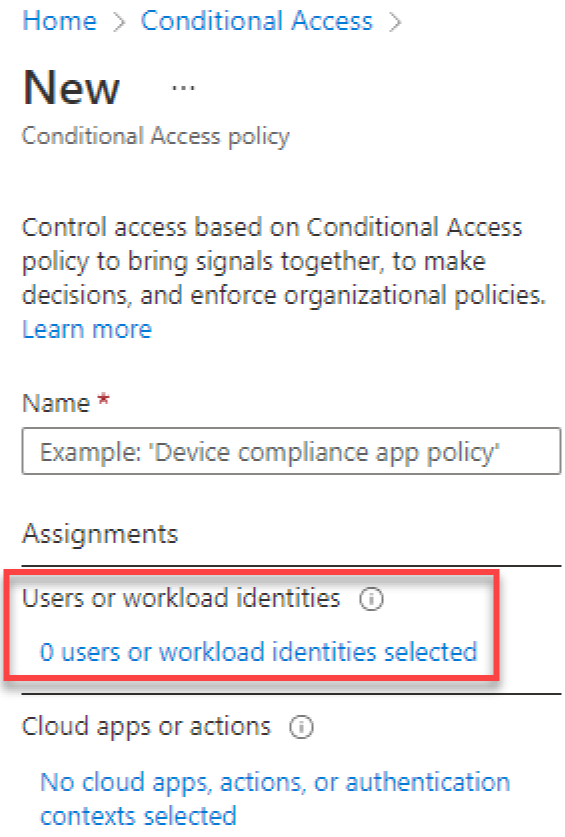
Conditional Access policies can be applied to specific users, groups, and apps. The goal is to protect your organization while also providing the right levels of access to the users who need it.

1. Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.
2. Browse to **Protection** > **Conditional Access**, select **+ New policy**, and then select **Create new policy**.



3. Enter a name for the policy, such as *MFA Pilot*.

4. Under **Assignments**, select the current value under **Users or workload identities**.



Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities

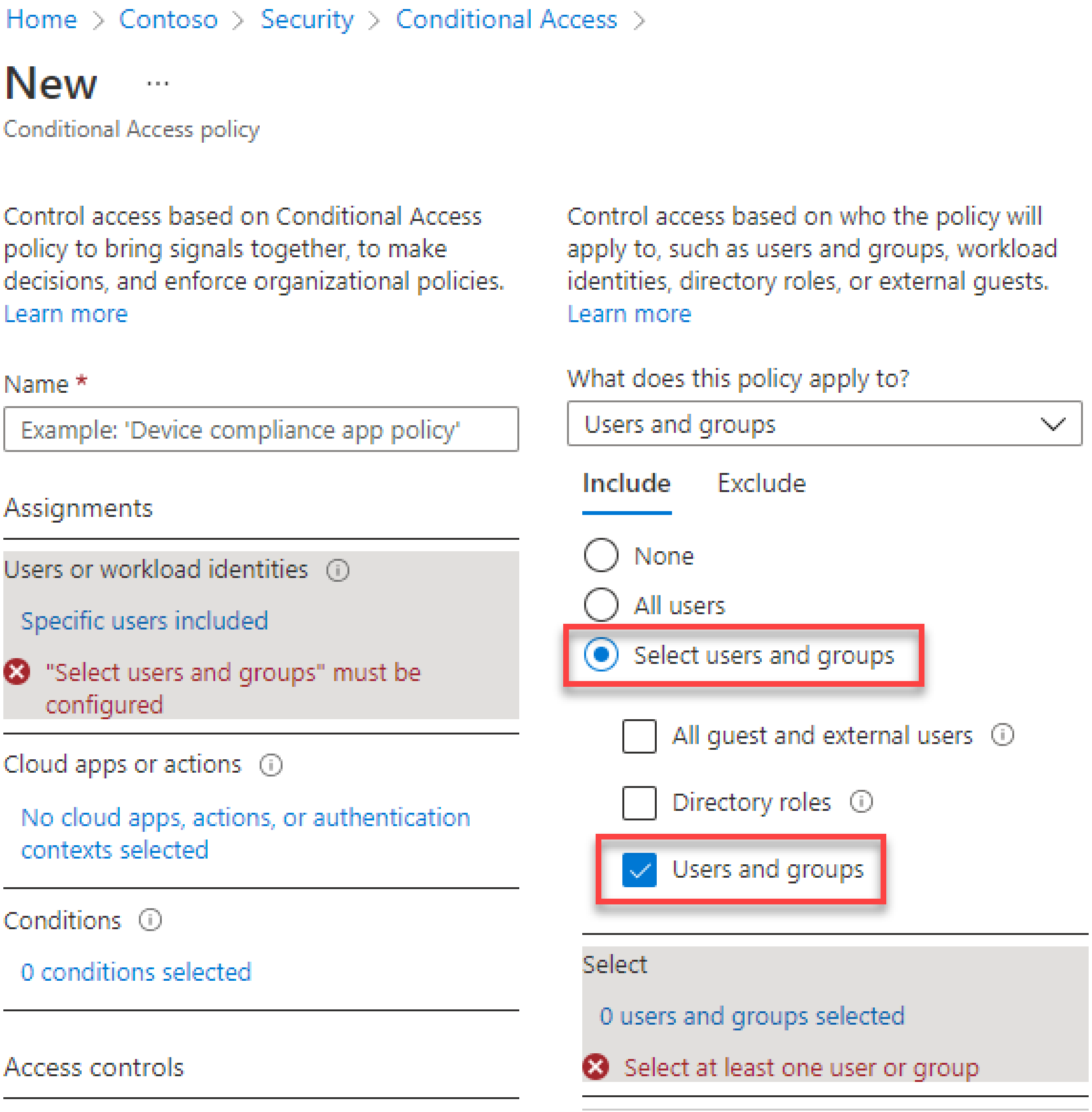
0 users or workload identities selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

5. Under **What does this policy apply to?**, verify that **Users and groups** is selected.

6. Under **Include**, choose **Select users and groups**, and then select **Users and groups**.



Home > Contoso > Security > Conditional Access >

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

Specific users included

"Select users and groups" must be configured

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

What does this policy apply to?

Users and groups

Include Exclude

○ None

○ All users

● Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☑ Users and groups

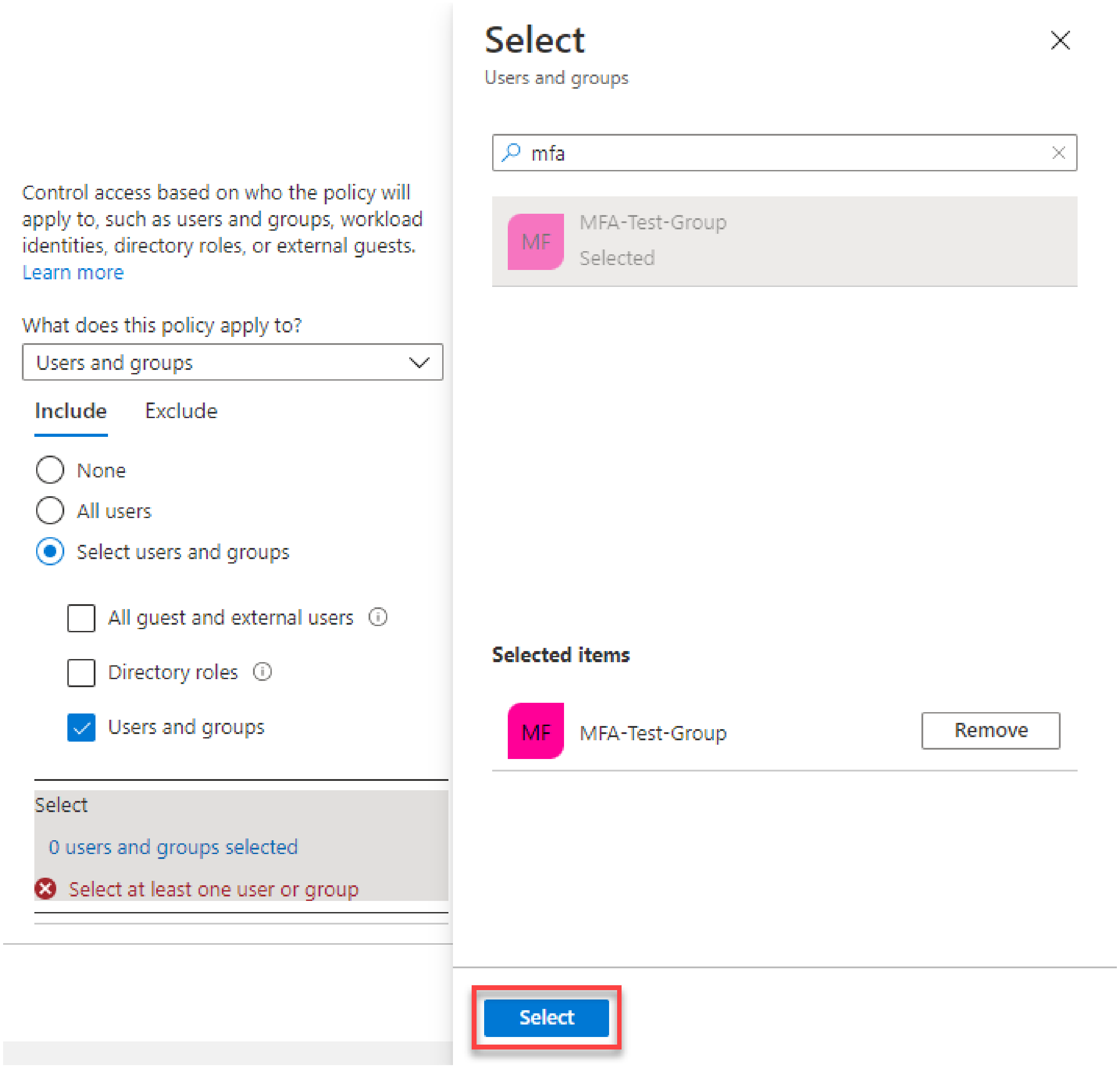
Select

0 users and groups selected

Select at least one user or group

Since no one is assigned yet, the list of users and groups (shown in the next step) opens automatically.

7. Browse for and select your Microsoft Entra group, such as *MFA-Test-Group*, then choose **Select**.



Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

What does this policy apply to?

Users and groups

Include | Exclude

○ None

○ All users

● Select users and groups

□ All guest and external users ⓘ

□ Directory roles ⓘ

☑ Users and groups

Select

0 users and groups selected

Select at least one user or group

Select

Users and groups

mfa

MF MFA-Test-Group

Selected

Selected items

MF MFA-Test-Group — Remove