

Contents

Fundamentals documentation

Overview

What is Azure Active Directory?

Compare Azure AD with ADDS

What's new in Azure Active Directory

Quickstarts

Access the portal and create a tenant

View your groups with assigned members

Concepts

Groups and users

Groups and access management

Group-based licensing

Default user permissions

Custom security attributes

Architecture

Azure AD architecture

Integrating all your apps with Azure AD

Parallel identity options

Multi-tenant user management

Multi-tenant user management introduction

Common scenarios

Common considerations

Common solutions

Authentication and provisioning protocols

Overview

Header-based authentication

LDAP authentication

OAuth 2.0 authentication

Open ID Connect authentication

- [Password-based authentication](#)
- [RADIUS authentication](#)
- [Remote desktop gateway authentication](#)
- [SAML authentication](#)
- [SSH authentication](#)
- [Windows authentication - KCD](#)
- [Directory synchronization](#)
- [LDAP synchronization](#)
- [SCIM synchronization](#)
- [Build for resilience](#)
 - [Overview](#)
 - [Infrastructure guidance](#)
 - [Infrastructure overview](#)
 - [Credential management](#)
 - [Device states](#)
 - [Continuous access evaluation](#)
 - [External user authentication](#)
 - [Hybrid authentication](#)
 - [Application Proxy](#)
 - [Azure AD B2C guidance](#)
 - [Azure AD B2C introduction to resilience](#)
 - [End-user experience](#)
 - [Interfaces with external processes](#)
 - [Azure AD B2C developer best practices](#)
 - [Monitoring and analytics](#)
 - [Application development guidance](#)
 - [Development overview](#)
 - [Client applications](#)
 - [Daemon applications](#)
 - [OpenID Connect metadata refresh](#)
 - [Monitor application health for resilience](#)
- [Certificate authorities used in Azure](#)

Deployment guide

Deployment 30, 90, and beyond

Azure Active Directory deployment plans

Azure Active Directory B2C deployment plans

Frontline worker management

Azure AD Operations reference

Introduction

Identity and access management

Authentication management

Identity governance

Operations

Security

Security baseline

Security operations guide

 Security operations overview

 Security operations for user accounts

 Security operations for privileged accounts

 Security operations for PIM

 Security operations for applications

 Security operations for devices

 Security operations for Infrastructure

Protect Microsoft 365 from on-premises attacks

Secure external collaboration

 Secure external access overview

 1 Determine your security posture

 2 Determine your current state

 3 Create a security plan

 4 Secure access with groups

 5 Secure access with B2B collaboration

 6 Secure access with Entitlement Management

 7 Secure access with conditional access

 8 Secure access with sensitivity labels

9 Secure access to Teams, SharePoint, and OneDrive

Secure service accounts

Introduction to Azure service accounts

Secure managed identities

Secure service principals

Govern Azure service accounts

Introduction to on-premises service accounts

Secure group MSAs

Secure standalone MSAs

Secure computer accounts

Secure on-premises user service accounts

Govern on-premises user service accounts

Enable MFA

Security defaults

Block legacy authentication

Identity secure score

Secure remote workers

How-to guides

Organization

Sign up for Azure AD as an organization

Sign up for Azure AD Premium

Add a custom domain name

Add company branding

Add your privacy info

Configure 'Stay signed in?'

Associate an Azure subscription

Users

Add or delete a new user

Add or change user profile info

Reset a user's password

Assign roles to users

Assign or remove licenses from users

[Restore a deleted user](#)

[Groups](#)

[Create a group and add members](#)

[Add or remove group members](#)

[Delete a group and its members](#)

[Add or remove a group from another group](#)

[Edit group information](#)

[Add or remove group owners](#)

[Manage access to resources with groups](#)

[Custom security attributes](#)

[Add or deactivate attributes](#)

[Manage access to attributes](#)

[Troubleshoot attributes](#)

[Troubleshooting](#)

[How to find tenant ID](#)

[Get support for Azure Active Directory](#)

[Support and help options for Azure AD](#)

[Reference](#)

[What's new in Microsoft 365 Government](#)

[Archive for What's new? in Azure AD](#)

[Data storage](#)

[Identity data storage for Europe](#)

[Identity data storage for Australia and New Zealand](#)

What is Azure Active Directory?

4/10/2022 • 8 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure AD also helps them access internal resources. These are resources like apps on your corporate network and intranet, along with any cloud apps developed by your own organization. For more information about creating a tenant for your organization, see [Quickstart: Create a new tenant in Azure Active Directory](#).

To learn the difference between Azure AD and Active Directory Domain Services, see [Compare Active Directory to Azure Active Directory](#). You can also use the various [Microsoft Cloud for Enterprise Architects Series](#) posters to better understand the core identity services in Azure, Azure AD, and Microsoft 365.

Who uses Azure AD?

Azure AD is intended for:

- **IT admins:** As an IT admin, use Azure AD to control access to your apps and your app resources, based on your business requirements. For example, you can use Azure AD to require multi-factor authentication when accessing important organizational resources. You can also use Azure AD to automate user provisioning between your existing Windows Server AD and your cloud apps, including Microsoft 365. Finally, Azure AD gives you powerful tools to automatically help protect user identities and credentials and to meet your access governance requirements. To get started, sign up for a [free 30-day Azure Active Directory Premium trial](#).
- **App developers:** As an app developer, you can use Azure AD as a standards-based approach for adding single sign-on (SSO) to your app, allowing it to work with a user's pre-existing credentials. Azure AD also provides APIs that can help you build personalized app experiences using existing organizational data. To get started, sign up for a [free 30-day Azure Active Directory Premium trial](#). For more information, you can also see [Azure Active Directory for developers](#).
- **Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers:** As a subscriber, you're already using Azure AD. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant. You can immediately start to manage access to your integrated cloud apps.

What are the Azure AD licenses?

Microsoft Online business services, such as Microsoft 365 or Microsoft Azure, require Azure AD for sign-in activities and to help with identity protection. If you subscribe to any Microsoft Online business service, you automatically get Azure AD with access to all the free features.

To enhance your Azure AD implementation, you can also add paid capabilities by upgrading to Azure Active Directory Premium P1 or Premium P2 licenses. Azure AD paid licenses are built on top of your existing free directory. The licenses provide self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

NOTE

For the pricing options of these licenses, see [Azure Active Directory Pricing](#).

Azure Active Directory Premium P1 and Premium P2 are not currently supported in China. For more information about Azure AD pricing, contact the [Azure Active Directory Forum](#).

- **Azure Active Directory Free.** Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.
- **Azure Active Directory Premium P1.** In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager, and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Azure Active Directory Premium P2.** In addition to the Free and P1 features, P2 also offers [Azure Active Directory Identity Protection](#) to help provide risk-based Conditional Access to your apps and critical company data and [Privileged Identity Management](#) to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.
- **"Pay as you go" feature licenses.** You can also get additional feature licenses, such as Azure Active Directory Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps. For more information, see [Azure Active Directory B2C documentation](#).

For more information about associating an Azure subscription to Azure AD, see [Associate or add an Azure subscription to Azure Active Directory](#). For more information about assigning licenses to your users, see [How to: Assign or remove Azure Active Directory licenses](#).

Which features work in Azure AD?

After you choose your Azure AD license, you'll get access to some or all of the following features for your organization:

CATEGORY	DESCRIPTION
Application management	Manage your cloud and on-premises apps using Application Proxy, single sign-on, the My Apps portal, and Software as a Service (SaaS) apps. For more information, see How to provide secure remote access to on-premises applications and Application Management documentation .
Authentication	Manage Azure Active Directory self-service password reset, Multi-Factor Authentication, custom banned password list, and smart lockout. For more information, see Azure AD Authentication documentation .
Azure Active Directory for developers	Build apps that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or custom APIs. For more information, see Microsoft identity platform (Azure Active Directory for developers) .
Business-to-Business (B2B)	Manage your guest users and external partners, while maintaining control over your own corporate data. For more information, see Azure Active Directory B2B documentation .

CATEGORY	DESCRIPTION
Business-to-Customer (B2C)	Customize and control how users sign up, sign in, and manage their profiles when using your apps. For more information, see Azure Active Directory B2C documentation .
Conditional Access	Manage access to your cloud apps. For more information, see Azure AD Conditional Access documentation .
Device Management	Manage how your cloud or on-premises devices access your corporate data. For more information, see Azure AD Device Management documentation .
Domain services	Join Azure virtual machines to a domain without using domain controllers. For more information, see Azure AD Domain Services documentation .
Enterprise users	Manage license assignments, access to apps, and set up delegates using groups and administrator roles. For more information, see Azure Active Directory user management documentation .
Hybrid identity	Use Azure Active Directory Connect and Connect Health to provide a single user identity for authentication and authorization to all resources, regardless of location (cloud or on-premises). For more information, see Hybrid identity documentation .
Identity governance	Manage your organization's identity through employee, business partner, vendor, service, and app access controls. You can also perform access reviews. For more information, see Azure AD identity governance documentation and Azure AD access reviews .
Identity protection	Detect potential vulnerabilities affecting your organization's identities, configure policies to respond to suspicious actions, and then take appropriate action to resolve them. For more information, see Azure AD Identity Protection .
Managed identities for Azure resources	Provide your Azure services with an automatically managed identity in Azure AD that can authenticate any Azure AD-supported authentication service, including Key Vault. For more information, see What is managed identities for Azure resources? .
Privileged identity management (PIM)	Manage, control, and monitor access within your organization. This feature includes access to resources in Azure AD and Azure, and other Microsoft Online Services, like Microsoft 365 or Intune. For more information, see Azure AD Privileged Identity Management .
Reports and monitoring	Gain insights into the security and usage patterns in your environment. For more information, see Azure Active Directory reports and monitoring .

Terminology

To better understand Azure AD and its documentation, we recommend reviewing the following terms.

TERM OR CONCEPT	DESCRIPTION
Identity	A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.
Account	An identity that has data associated with it. You can't have an account without an identity.
Azure AD account	An identity created through Azure AD or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Azure AD and accessible to your organization's cloud service subscriptions. This account is also sometimes called a Work or school account.
Account Administrator	This classic subscription administrator role is conceptually the billing owner of a subscription. This role enables you to manage all subscriptions in an account. For more information, see Classic subscription administrator roles , Azure roles , and Azure AD administrator roles .
Service Administrator	This classic subscription administrator role enables you to manage all Azure resources, including access. This role has the equivalent access of a user who is assigned the Owner role at the subscription scope. For more information, see Classic subscription administrator roles , Azure roles , and Azure AD administrator roles .
Owner	This role helps you manage all Azure resources, including access. This role is built on a newer authorization system called Azure role-based access control (Azure RBAC) that provides fine-grained access management to Azure resources. For more information, see Classic subscription administrator roles , Azure roles , and Azure AD administrator roles .
Azure AD Global administrator	This administrator role is automatically assigned to whomever created the Azure AD tenant. You can have multiple Global administrators, but only Global administrators can assign administrator roles (including assigning other Global administrators) to users. For more information about the various administrator roles, see Administrator role permissions in Azure Active Directory .
Azure subscription	Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
Azure tenant	A dedicated and trusted instance of Azure AD. The tenant is automatically created when your organization signs up for a Microsoft cloud service subscription. These subscriptions include Microsoft Azure, Microsoft Intune, or Microsoft 365. An Azure tenant represents a single organization.
Single tenant	Azure tenants that access other services in a dedicated environment are considered single tenant.

TERM OR CONCEPT	DESCRIPTION
Multi-tenant	Azure tenants that access other services in a shared environment, across multiple organizations, are considered multi-tenant.
Azure AD directory	Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.
Custom domain	Every new Azure AD directory comes with an initial domain name, for example <code>domainname.onmicrosoft.com</code> . In addition to that initial name, you can also add your organization's domain names. Your organization's domain names include the names you use to do business and your users use to access your organization's resources, to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as <code>alain@contoso.com</code> .
Microsoft account (also called, MSA)	Personal accounts that provide access to your consumer-oriented Microsoft products and cloud services. These products and services include Outlook, OneDrive, Xbox LIVE, or Microsoft 365. Your Microsoft account is created and stored in the Microsoft consumer identity account system that's run by Microsoft.

Next steps

- [Sign up for Azure Active Directory Premium](#)
- [Associate an Azure subscription to your Azure Active Directory](#)
- [Azure Active Directory Premium P2 feature deployment checklist](#)

Compare Active Directory to Azure Active Directory

4/10/2022 • 5 minutes to read • [Edit Online](#)

Azure Active Directory is the next evolution of identity and access management solutions for the cloud. Microsoft introduced Active Directory Domain Services in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.

Azure AD takes this approach to the next level by providing organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

Most IT administrators are familiar with Active Directory Domain Services concepts. The following table outlines the differences and similarities between Active Directory concepts and Azure Active Directory.

CONCEPT	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Users		
Provisioning: users	Organizations create internal users manually or use an in-house or automated provisioning system, such as the Microsoft Identity Manager, to integrate with an HR system.	Existing AD organizations use Azure AD Connect to sync identities to the cloud. Azure AD adds support to automatically create users from cloud HR systems . Azure AD can provision identities in SCIM enabled SaaS apps to automatically provide apps with the necessary details to allow access for users.
Provisioning: external identities	Organizations create external users manually as regular users in a dedicated external AD forest, resulting in administration overhead to manage the lifecycle of external identities (guest users)	Azure AD provides a special class of identity to support external identities. Azure AD B2B will manage the link to the external user identity to make sure they are valid.
Entitlement management and groups	Administrators make users members of groups. App and resource owners then give groups access to apps or resources.	Groups are also available in Azure AD and administrators can also use groups to grant permissions to resources. In Azure AD, administrators can assign membership to groups manually or use a query to dynamically include users to a group. Administrators can use Entitlement management in Azure AD to give users access to a collection of apps and resources using workflows and, if necessary, time-based criteria.

CONCEPT	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Admin management	Organizations will use a combination of domains, organizational units, and groups in AD to delegate administrative rights to manage the directory and resources it controls.	Azure AD provides built-in roles with its Azure AD role-based access control (Azure AD RBAC) system, with limited support for creating custom roles to delegate privileged access to the identity system, the apps, and resources it controls. Managing roles can be enhanced with Privileged Identity Management (PIM) to provide just-in-time, time-restricted, or workflow-based access to privileged roles.
Credential management	Credentials in Active Directory are based on passwords, certificate authentication, and smartcard authentication. Passwords are managed using password policies that are based on password length, expiry, and complexity.	Azure AD uses intelligent password protection for cloud and on-premises. Protection includes smart lockout plus blocking common and custom password phrases and substitutions. Azure AD significantly boosts security through Multi-factor authentication and passwordless technologies, like FIDO2. Azure AD reduces support costs by providing users a self-service password reset system.
Apps		
Infrastructure apps	Active Directory forms the basis for many infrastructure on-premises components, for example, DNS, DHCP, IPSec, WiFi, NPS, and VPN access	In a new cloud world, Azure AD, is the new control plane for accessing apps versus relying on networking controls. When users authenticate, Conditional access (CA) , will control which users, will have access to which apps under required conditions.
Traditional and legacy apps	Most on-premises apps use LDAP, Windows-Integrated Authentication (NTLM and Kerberos), or Header-based authentication to control access to users.	Azure AD can provide access to these types of on-premises apps using Azure AD application proxy agents running on-premises. Using this method Azure AD can authenticate Active Directory users on-premises using Kerberos while you migrate or need to coexist with legacy apps.
SaaS apps	Active Directory doesn't support SaaS apps natively and requires federation system, such as AD FS.	SaaS apps supporting OAuth2, SAML, and WS-* authentication can be integrated to use Azure AD for authentication.
Line of business (LOB) apps with modern authentication	Organizations can use AD FS with Active Directory to support LOB apps requiring modern authentication.	LOB apps requiring modern authentication can be configured to use Azure AD for authentication.

CONCEPT	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
Mid-tier/Daemon services	Services running in on-premises environments normally use AD service accounts or group Managed Service Accounts (gMSA) to run. These apps will then inherit the permissions of the service account.	Azure AD provides managed identities to run other workloads in the cloud. The lifecycle of these identities is managed by Azure AD and is tied to the resource provider and it can't be used for other purposes to gain backdoor access.
Devices		
Mobile	Active Directory doesn't natively support mobile devices without third-party solutions.	Microsoft's mobile device management solution, Microsoft Intune, is integrated with Azure AD. Microsoft Intune provides device state information to the identity system to evaluate during authentication.
Windows desktops	Active Directory provides the ability to domain join Windows devices to manage them using Group Policy, System Center Configuration Manager, or other third-party solutions.	Windows devices can be joined to Azure AD . Conditional access can check if a device is Azure AD joined as part of the authentication process. Windows devices can also be managed with Microsoft Intune . In this case, conditional access, will consider whether a device is compliant (for example, up-to-date security patches and virus signatures) before allowing access to the apps.
Windows servers	Active Directory provides strong management capabilities for on-premises Windows servers using Group Policy or other management solutions.	Windows servers virtual machines in Azure can be managed with Azure AD Domain Services . Managed identities can be used when VMs need access to the identity system directory or resources.
Linux/Unix workloads	Active Directory doesn't natively support non-Windows without third-party solutions, although Linux machines can be configured to authenticate with Active Directory as a Kerberos realm.	Linux/Unix VMs can use managed identities to access the identity system or resources. Some organizations, migrate these workloads to cloud container technologies, which can also use managed identities.

Next steps

- [What is Azure Active Directory?](#)
- [Compare self-managed Active Directory Domain Services, Azure Active Directory, and managed Azure Active Directory Domain Services](#)
- [Frequently asked questions about Azure Active Directory](#)
- [What's new in Azure Active Directory?](#)

What's new in Azure Active Directory?

4/10/2022 • 29 minutes to read • [Edit Online](#)

Get notified about when to revisit this page for updates by copying and pasting this URL:

`https://docs.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us`

into your  feed reader.

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, this article provides you with information about:

- The latest releases
- Known issues
- Bug fixes
- Deprecated functionality
- Plans for changes

This page is updated monthly, so revisit it regularly. If you're looking for items older than six months, you can find them in [Archive for What's new in Azure Active Directory](#).

March 2022

Tenant enablement of combined security information registration for Azure Active Directory

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

Clouds impacted: Public (Microsoft 365, GCC)

We announced in April 2020 General Availability of our new combined registration experience, enabling users to register security information for multi-factor authentication and self-service password reset at the same time, which was available for existing customers to opt in. We're happy to announce the combined security information registration experience will be enabled to all non-enabled customers after September 30th, 2022. This change does not impact tenants created after August 15th, 2020, or tenants located in the China region. For more information, see: [Combined security information registration for Azure Active Directory overview](#).

Public preview - New provisioning connectors in the Azure AD Application Gallery - March 2022

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [AlexisHR](#)
- [embed signage](#)
- [Joyn FSM](#)
- [KPN Grip](#)
- [MURAL Identity](#)
- [Palo Alto Networks SCIM Connector](#)
- [Tap App Security](#)

- **Yellowbox**

For more information about how to better secure your organization by using automated user account provisioning, see: [Automate user provisioning to SaaS applications with Azure AD](#).

Public preview - Azure AD Recommendations

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Clouds impacted: Public (Microsoft 365,GCC)

Azure AD Recommendations is now in public preview. This feature provides personalized insights with actionable guidance to help you identify opportunities to implement Azure AD best practices, and optimize the state of your tenant. For more information, see: [What is Azure Active Directory recommendations](#)

Public Preview: Dynamic administrative unit membership for users and devices

Type: New feature

Service category: RBAC

Product capability: Access Control

Clouds impacted: Public (Microsoft 365,GCC)

Administrative units now support dynamic membership rules for user and device members. Instead of manually assigning users and devices to administrative units, tenant admins can set up a query for the administrative unit. The membership will be automatically maintained by Azure AD. For more information, see: [Administrative units in Azure Active Directory](#).

Public Preview: Devices in Administrative Units

Type: New feature

Service category: RBAC

Product capability: AuthZ/Access Delegation

Clouds impacted: Public (Microsoft 365,GCC)

Devices can now be added as members of administrative units. This enables scoped delegation of device permissions to a specific set of devices in the tenant. Built-in and custom roles are also supported. For more information, see: [Administrative units in Azure Active Directory](#).

New Federated Apps available in Azure AD Application gallery - March 2022

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In March 2022 we have added the following 29 new applications in our App gallery with Federation support:

[Informatica Platform](#), [Buttonwood Central SSO](#), [Blockbax](#), [Datto Workplace Single Sign On](#), [Atlas by Workland](#), [Simply.Coach](#), [Benevity](#), [Engage Absence Management](#), [LitLingo App Authentication](#), [ADP EMEA French HR Portal mon.adp.com](#), [Ready Room](#), [Rainmaker UPSMQDEV](#), [Axway CSOS](#), [Alloy](#), [U.S. Bank Prepaid](#), [EdApp](#), [GoSimplo](#), [Snow Atlas SSO](#), [Abacus.AI](#), [Culture Shift](#), [StaySafe Hub](#), [OpenLearning](#), [Draup, Inc](#), [Air](#), [Regulatory Lab](#), [SafetyLine](#), [Zest](#), [iGrafx Platform](#), [Tracker Software Technologies](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>,

For listing your application in the Azure AD app gallery, please read the details here

<https://aka.ms/AzureADAppRequest>

Public Preview - New APIs for fetching transitive role assignments and role permissions

Type: New feature

Service category: RBAC

Product capability: Access Control

1. **transitiveRoleAssignments** - Last year the ability to assign Azure AD roles to groups was created. Originally it took four calls to fetch all direct, and transitive, role assignments of a user. This new API call allows it all to be done via one API call. For more information, see: [List transitiveRoleAssignment - Microsoft Graph beta | Microsoft Docs](#).
 2. **unifiedRbacResourceAction** - Developers can use this API to list all role permissions and their descriptions in Azure AD. This API can be thought of as a dictionary that can help build custom roles without relying on UX. For more information, see: [List resourceActions - Microsoft Graph beta | Microsoft Docs](#).
-

February 2022

General Availability - France digital accessibility requirement

Type: Plan for change

Service category: Other

Product capability: End User Experiences

This change provides users who are signing into Azure Active Directory on iOS, Android, and Web UI flavors information about the accessibility of Microsoft's online services via a link on the sign-in page. This ensures that the France digital accessibility compliance requirements are met. The change will only be available for French language experiences.[Learn more](#)

General Availability - Downloadable access review history report

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

With Azure Active Directory (Azure AD) Access Reviews, you can create a downloadable review history to help your organization gain more insight. The report pulls the decisions that were taken by reviewers when a report is created. These reports can be constructed to include specific access reviews, for a specific time frame, and can be filtered to include different review types and review results.[Learn more](#)

Public Preview of Identity Protection for Workload Identities

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Azure AD Identity Protection is extending its core capabilities of detecting, investigating, and remediating identity-based risk to workload identities. This allows organizations to better protect their applications, service principals, and managed identities. We are also extending Conditional Access so you can block at-risk workload identities. [Learn more](#)

Public Preview - Cross-tenant access settings for B2B collaboration

Type: New feature

Service category: B2B

Product capability: Collaboration

Clouds impacted: China;Public (Microsoft 365, GCC);US Gov (GCC-H, DoD)

Cross-tenant access settings enable you to control how users in your organization collaborate with members of external Azure AD organizations. Now you'll have granular inbound and outbound access control settings that work on a per org, user, group, and application basis. These settings also make it possible for you to trust security claims from external Azure AD organizations like multi-factor authentication (MFA), device compliance, and hybrid Azure AD joined devices. [Learn more](#)

Public preview - Create Azure AD access reviews with multiple stages of reviewers

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

Use multi-stage reviews to create Azure AD access reviews in sequential stages, each with its own set of reviewers and configurations. Supports multiple stages of reviewers to satisfy scenarios such as: independent groups of reviewers reaching quorum, escalations to other reviewers, and reducing burden by allowing for later stage reviewers to see a filtered-down list. For public preview, multi-stage reviews are only supported on reviews of groups and applications. [Learn more](#)

New Federated Apps available in Azure AD Application gallery - February 2022

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In February 2022 we added the following 20 new applications in our App gallery with Federation support:

[Embark](#), [FENCE-Mobile RemoteManager SSO](#), [カオナビ](#), [Adobe Identity Management \(OIDC\)](#), [AppRemo](#), [Live Center](#), [Offishall](#), [MoveWORK Flow](#), [Cirros SL](#), [ePMX Procurement Software](#), [Vanta O365](#), [Hubble](#), [Medigold Gateway](#), [クラウドログ](#), [Amazing People Schools](#), [Salus](#), [XplicitTrust Network Access](#), [Spike Email - Mail & Team Chat](#), [AltheaSuite](#), [Balsamiq Wireframes](#).

You can also find the documentation of all the applications from here: <https://aka.ms/AppsTutorial>,

For listing your application in the Azure AD app gallery, please read the details here:

<https://aka.ms/AzureADAppRequest>

Two new MDA detections in Identity Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Identity Protection has added two new detections from Microsoft Defender for Cloud Apps, (formerly MCAS). The Mass Access to Sensitive Files detection detects anomalous user activity, and the Unusual Addition of Credentials to an OAuth app detects suspicious service principal activity. [Learn more](#)

Public preview - New provisioning connectors in the Azure AD Application Gallery - February 2022

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [BullseyeTDP](#)
- [GitHub Enterprise Managed User \(OIDC\)](#)

- [Gong](#)
- [LanSchool Air](#)
- [ProdPad](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

General Availability - Privileged Identity Management (PIM) role activation for SharePoint Online enhancements

Type: Changed feature

Service category: Privileged Identity Management

Product capability: Privileged Identity Management

We have improved the Privileged Identity management (PIM) time to role activation for SharePoint Online. Now, when activating a role in PIM for SharePoint Online, you should be able to use your permissions right away in SharePoint Online. This change will roll out in stages, so you might not yet see these improvements in your organization. [Learn more](#)

January 2022

Public preview - Custom security attributes

Type: New feature

Service category: Directory Management

Product capability: Directory

Enables you to define business-specific attributes that you can assign to Azure AD objects. These attributes can be used to store information, categorize objects, or enforce fine-grained access control. Custom security attributes can be used with Azure attribute-based access control. [Learn more](#).

Public preview - Filter groups in tokens using a substring match

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

In the past, Azure AD only permitted groups to be filtered based on whether they were assigned to an application. Now, you can also use Azure AD to filter the groups included in the token. You can filter with the substring match on the display name or onPremisesSAMAccountName attributes of the group object on the token. Only groups that the user is a member of will be included in the token. This token will be recognized whether it's on the ObjectID or the on premises SAMAccountName or security identifier (SID). This feature can be used together with the setting to include only groups assigned to the application if desired to further filter the list. [Learn more](#)

General availability - Continuous Access Evaluation

Type: New feature

Service category: Other

Product capability: Access Control

With Continuous access evaluation (CAE), critical security events and policies are evaluated in real time. This includes account disable, password reset, and location change. [Learn more](#).

General Availability - User management enhancements are now available

Type: New feature

Service category: User Management

Product capability: User Management

The Azure AD portal has been updated to make it easier to find users in the All users and Deleted users pages. Changes in the preview include:

- More visible user properties including object ID, directory sync status, creation type, and identity issuer.
- **Search now** allows substring search and combined search of names, emails, and object IDs.
- Enhanced filtering by user type (member, guest, and none), directory sync status, creation type, company name, and domain name.
- New sorting capabilities on properties like name, user principal name, creation time, and deletion date.
- A new total users count that updates with any searches or filters.

For more information, go to [User management enhancements \(preview\) in Azure Active Directory](#).

General Availability - My Apps customization of default Apps view

Type: New feature

Service category: My Apps

Product capability: End User Experiences

Customization of the default My Apps view is now in general availability. For more information on My Apps, you can go to [Sign in and start apps from the My Apps portal](#).

General Availability - Audited BitLocker Recovery

Type: New feature

Service category: Device Access Management

Product capability: Device Lifecycle Management

BitLocker keys are sensitive security items. Audited BitLocker recovery ensures that when BitLocker keys are read, an audit log is generated so that you can trace who accesses this information for given devices. [Learn more](#).

General Availability - Download a list of devices

Type: New feature

Service category: Device Registration and Management

Product capability: Device Lifecycle Management

Download a list of your organization's devices to a .csv file for easier reporting and management. [Learn more](#).

New provisioning connectors in the Azure AD Application Gallery - January 2022

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Autodesk SSO](#)
- [Evercate](#)
- [frankli.io](#)
- [Plandisc](#)
- [Swit](#)
- [TerraTrue](#)
- [TimeClock 365 SAML](#)

For more information about how to better secure your organization by using automated user account provisioning, go to [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD Application gallery - January 2022

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In January 2022, we've added the following 47 new applications in our App gallery with Federation support:

Jooto, PropriLi, Pace Scheduler, DRTrack, Dining Sidekick, Cryotos, Emergency Management Systems, Manifestly Checklists, eLearnPOSH, Scuba Analytics, Athena Systems Login Platform, TimeTrack, MiHCM, Health Note, Active Directory SSO for DoubleYou, Emplifi platform, Flexera One, Hypothesis, Recurly, XpressDox AU Cloud, Zoom for Intune, UPWARD AGENT, Linux Foundation ID, Asset Planner, Kiho, chezie, Excelity HCM, yuccaHR, Blue Ocean Brain, EchoSpan, Archie, Equifax Workforce Solutions, Palantir Foundry, ATP SpotLight and ChronicX, DigiSign, mConnect, BrightHR, Mural Identity, NordPass SSO, CloudClarity, Twic, Eduhouse Online, Bealink, Time Intelligence Bot, SentinelOne

You can also find the documentation of all the applications from: <https://aka.ms/AppsTutorial>,

For listing your application in the Azure AD app gallery, read the details in: <https://aka.ms/AzureADAppRequest>

Azure Ad access reviews reviewer recommendations now account for non-interactive sign-in information

Type: Changed feature

Service category: Access Reviews

Product capability: Identity Governance

Azure AD access reviews reviewer recommendations now account for non-interactive sign-in information, improving upon original recommendations based on interactive last sign-ins only. Reviewers can now make more accurate decisions based on the last sign-in activity of the users they're reviewing. To learn more about how to create access reviews, go to [Create an access review of groups and applications in Azure AD](#).

Risk reason for offline Azure AD Threat Intelligence risk detection

Type: Changed feature

Service category: Identity Protection

Product capability: Identity Security & Protection

The offline Azure AD Threat Intelligence risk detection can now have a risk reason that will help customers with the risk investigation. If a risk reason is available, it will show up as **Additional Info** in the risk details of that risk event. The information can be found in the Risk detections report. It will also be available through the additionalInfo property of the riskDetections API. [Learn more](#).

December 2021

Tenant enablement of combined security information registration for Azure Active Directory

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

We previously announced in April 2020, a new combined registration experience enabling users to register authentication methods for SSPR and multi-factor authentication at the same time was generally available for existing customer to opt in. Any Azure AD tenants created after August 2020 automatically have the default experience set to combined registration. Starting in 2022 Microsoft will be enabling the multi-factor

authentication and SSPR combined registration experience for existing customers. [Learn more](#).

Public Preview - Number Matching now available to reduce accidental notification approvals

Type: New feature

Service category: Microsoft Authenticator App

Product capability: User Authentication

To prevent accidental notification approvals, admins can now require users to enter the number displayed on the sign in screen when approving a multi-factor authentication notification in the Authenticator app. This feature adds an extra security measure to the Microsoft Authenticator app. [Learn more](#).

Pre-authentication error events removed from Azure AD Sign-in Logs

Type: Deprecated

Service category: Reporting

Product capability: Monitoring & Reporting

We're no longer publishing sign-in logs with the following error codes because these events are pre-authentication events that occur before our service has authenticated a user. Because these events happen before authentication, our service isn't always able to correctly identify the user. If a user continues on to authenticate, the user sign-in will show up in your tenant Sign-in logs. These logs are no longer visible in the Azure portal UX, and querying these error codes in the Graph API will no longer return results.

ERROR CODE	FAILURE REASON
50058	Session information isn't sufficient for single-sign-on.
16000	Either multiple user identities are available for the current request or selected account isn't supported for the scenario.
500581	Rendering JavaScript. Fetching sessions for single-sign-on on V2 with prompt=none requires JavaScript to verify if any MSA accounts are signed in.
81012	The user trying to sign in to Azure AD is different from the user signed into the device.

November 2021

Tenant enablement of combined security information registration for Azure Active Directory

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

We previously announced in April 2020, a new combined registration experience enabling users to register authentication methods for SSPR and multi-factor authentication at the same time was generally available for existing customer to opt in. Any Azure AD tenants created after August 2020 automatically have the default experience set to combined registration. Starting 2022, Microsoft will be enabling the MFA/SSPR combined registration experience for existing customers. [Learn more](#).

Windows users will see prompts more often when switching user accounts

Type: Fixed

Service category: Authentications (Logins)

Product capability: User Authentication

A problematic interaction between Windows and a local Active Directory Federation Services (ADFS) instance can result in users attempting to sign into another account, but be silently signed into their existing account instead, with no warning. For federated IdPs such as ADFS, that support the [prompt=login](#) pattern, Azure AD will now trigger a fresh login at ADFS when a user is directed to ADFS with a login hint. This ensures that the user is signed into the account they requested, rather than being silently signed into the account they're already signed in with.

For more information, see the [change notice](#).

Public preview - Conditional Access Overview Dashboard

Type: New feature

Service category: Conditional Access

Product capability: Monitoring & Reporting

The new Conditional Access overview dashboard enables all tenants to see insights about the impact of their Conditional Access policies without requiring an Azure Monitor subscription. This built-in dashboard provides tutorials to deploy policies, a summary of the policies in your tenant, a snapshot of your policy coverage, and security recommendations. [Learn more](#).

Public preview - SSPR writeback is now available for disconnected forests using Azure AD Connect cloud sync

Type: New feature

Service category: Azure AD Connect Cloud Sync

Product capability: Identity Lifecycle Management

The Public Preview feature for Azure AD Connect Cloud Sync Password writeback provides customers the capability to writeback a user's password changes in the cloud to the on-premises directory in real time using the lightweight Azure AD cloud provisioning agent. [Learn more](#).

Public preview - Conditional Access for workload identities

Type: New feature

Service category: Conditional Access for workload identities

Product capability: Identity Security & Protection

Previously, Conditional Access policies applied only to users when they access apps and services like SharePoint online or the Azure portal. This preview adds support for Conditional Access policies applied to service principals owned by the organization. You can block service principals from accessing resources from outside trusted-named locations or Azure Virtual Networks. [Learn more](#).

Public preview - Extra attributes available as claims

Type: Changed feature

Service category: Enterprise Apps

Product capability: SSO

Several user attributes have been added to the list of attributes available to map to claims to bring attributes available in claims more in line with what is available on the user object in Microsoft Graph. New attributes include mobilePhone and ProxyAddresses. [Learn more](#).

Public preview - "Session Lifetime Policies Applied" property in the sign-in logs

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Security & Protection

We have recently added other property to the sign-in logs called "Session Lifetime Policies Applied". This property will list all the session lifetime policies that applied to the sign-in for example, Sign-in frequency, Remember multi-factor authentication and Configurable token lifetime. [Learn more.](#)

Public preview - Enriched reviews on access packages in entitlement management

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

Entitlement Management's enriched review experience allows even more flexibility on access packages reviews. Admins can now choose what happens to access if the reviewers don't respond, provide helper information to reviewers, or decide whether a justification is necessary. [Learn more.](#)

General availability - randomString and redact provisioning functions

Type: New feature

Service category: Provisioning

Product capability: Outbound to SaaS Applications

The Azure AD Provisioning service now supports two new functions, randomString() and Redact():

- randomString - generate a string based on the length and characters you would like to include or exclude in your string.
 - redact - remove the value of the attribute from the audit and provisioning logs. [Learn more.](#)
-

General availability - Now access review creators can select users and groups to receive notification on completion of reviews

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

Now access review creators can select users and groups to receive notification on completion of reviews. [Learn more.](#)

General availability - Azure AD users can now view and report suspicious sign-ins and manage their accounts within Microsoft Authenticator

Type: New feature

Service category: Microsoft Authenticator App

Product capability: Identity Security & Protection

This feature allows Azure AD users to manage their work or school accounts within the Microsoft Authenticator app. The management features will allow users to view sign-in history and sign-in activity. Users can also report any suspicious or unfamiliar activity, change their Azure AD account passwords, and update the account's security information.

For more information on how to use this feature visit [View and search your recent sign-in activity from the My Sign-ins page.](#)

General availability - New Microsoft Authenticator app icon

Type: New feature

Service category: Microsoft Authenticator App

Product capability: Identity Security & Protection

New updates have been made to the Microsoft Authenticator app icon. To learn more about these updates, see the [Microsoft Authenticator app](#) blog post.

General availability - Azure AD single Sign on and device-based Conditional Access support in Firefox on Windows 10/11

Type: New feature

Service category: Authentications (Logins)

Product capability: SSO

We now support native single sign-on (SSO) support and device-based Conditional Access to Firefox browser on Windows 10 and Windows Server 2019 starting in Firefox version 91. [Learn more](#).

New provisioning connectors in the Azure AD Application Gallery - November 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Appaegis Isolation Access Cloud](#)
- [BenQ IAM](#)
- [BIC Cloud Design](#)
- [Chaos](#)
- [directprint.io](#)
- [Documo](#)
- [Facebook Work Accounts](#)
- [introDus Pre and Onboarding Platform](#)
- [Kisi Physical Security](#)
- [Klaxoon](#)
- [Klaxoon SAML](#)
- [MX3 Diagnostics](#)
- [Netpresenter](#)
- [Peripass](#)
- [Real Links](#)
- [Sentry](#)
- [Teamgo](#)
- [Zero](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD Application gallery - November 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In November 2021, we have added following 32 new applications in our App gallery with Federation support:

[Tide - Connector](#), [Virtual Risk Manager - USA](#), [Xorlia Policy Management](#), [WorkPatterns](#), [GHAE](#), [Nodetrax Project](#), [Touchstone Benchmarking](#), [SURFsecureID - Azure MFA](#), [AiDEA,R](#) and [D Tax Credit Services: 10-wk Implementation](#), [Mapiq Essentials](#), [Celtra Authentication Service](#), [Compete HR](#), [Snackmagic](#), [FileOrbis](#), [ClarivateWOS](#), [RewardCo Engagement Cloud](#), [ZoneVu](#), [V-Client](#), [Netpresenter Next](#), [UserTesting](#), [InfinityQS](#)

ProFicient on Demand, Feedconomics, Customer Voice, Zanders Inside, Connecter, Paychex Flex, InsightSquared, Kiteline Health, Fabrikam Enterprise Managed User (OIDC), PROXESS for Office365, Coverity Static Application Security Testing

You can also find the documentation of all the applications [here](#).

For listing your application in the Azure AD app gallery, read the details [here](#).

Updated "switch organizations" user experience in My Account.

Type: Changed feature

Service category: My Profile/Account

Product capability: End User Experiences

Updated "switch organizations" user interface in My Account. This visually improves the UI and provides the end-user with clear instructions. Added a manage organizations link to blade per customer feedback. [Learn more](#).

October 2021

Limits on the number of configured API permissions for an application registration will be enforced starting in October 2021

Type: Plan for change

Service category: Other

Product capability: Developer Experience

Sometimes, application developers configure their apps to require more permissions than it's possible to grant. To prevent this from happening, a limit on the total number of required permissions that can be configured for an app registration will be enforced.

The total number of required permissions for any single application registration mustn't exceed 400 permissions, across all APIs. The change to enforce this limit will begin rolling out mid-October 2021.

Applications exceeding the limit can't increase the number of permissions they're configured for. The existing limit on the number of distinct APIs for which permissions are required remains unchanged and may not exceed 50 APIs.

In the Azure portal, the required permissions are listed under API permissions for the application you wish to configure. Using Microsoft Graph or Microsoft Graph PowerShell, the required permissions are listed in the requiredResourceAccess property of an [application](#) entity. [Learn more](#).

Email one-time passcode on by default change beginning rollout in November 2021

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

Previously, we announced that starting October 31, 2021, Microsoft Azure Active Directory [email one-time passcode](#) authentication will become the default method for inviting accounts and tenants for B2B collaboration scenarios. However, because of deployment schedules, we'll begin rolling out on November 1, 2021. Most of the tenants will see the change rolled out in January 2022 to minimize disruptions during the holidays and deployment lock downs. After this change, Microsoft will no longer allow redemption of invitations using Azure Active Directory accounts that are unmanaged. [Learn more](#).

Conditional Access Guest Access Blocking Screen

Type: Fixed

Service category: Conditional Access

Product capability: End User Experiences

If there's no trust relation between a home and resource tenant, a guest user would have previously been asked to re-register their device, which would break the previous registration. However, the user would end up in a registration loop because only home tenant device registration is supported. In this specific scenario, instead of this loop, we've created a new conditional access blocking page. The page tells the end user that they can't get access to conditional access protected resources as a guest user. [Learn more](#).

50105 Errors will now result in a UX error message instead of an error response to the application

Type: Fixed

Service category: Authentications (Logins)

Product capability: Developer Experience

Azure AD has fixed a bug in an error response that occurs when a user isn't assigned to an app that requires a user assignment. Previously, Azure AD would return error 50105 with the OIDC error code "interaction_required" even during interactive authentication. This would cause well-coded applications to loop indefinitely, as they do interactive authentication and receive an error telling them to do interactive authentication, which they would then do.

The bug has been fixed, so that during non-interactive auth an "interaction_required" error will still be returned. Also, during interactive authentication an error page will be directly displayed to the user.

For greater details, see the change notices for [Azure AD protocols](#).

Public preview - New claims transformation capabilities

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

The following new capabilities have been added to the claims transformations available for manipulating claims in tokens issued from Azure AD:

- Join() on NameID. Used to be restricted to joining an email format address with a verified domain. Now Join() can be used on the NameID claim in the same way as any other claim, so NameID transforms can be used to create Windows account style NameIDs or any other string. For now if the result is an email address, the Azure AD will still validate that the domain is one that is verified in the tenant.
 - Substring(). A new transformation in the claims configuration UI allows extraction of defined position substrings such as five characters starting at character three - substring(3,5)
 - Claims transformations. These transformations can now be performed on Multi-valued attributes, and can emit multi-valued claims. Microsoft Graph can now be used to read/write multi-valued directory schema extension attributes. [Learn more](#).
-

Public Preview – Flagged Sign-ins

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Flagged sign-ins is a feature that will increase the signal to noise ratio for user sign-ins where users need help. The functionality is intended to empower users to raise awareness about sign-in errors they want help with. Also to help admins and help desk workers find the right sign-in events quickly and efficiently. [Learn more](#).

Public preview - Device overview

Type: New feature

Service category: Device Registration and Management

Product capability: Device Lifecycle Management

The new Device Overview feature provides actionable insights about devices in your tenant. [Learn more.](#)

Public preview - Azure Active Directory workload identity federation

Type: New feature

Service category: Enterprise Apps

Product capability: Developer Experience

Azure AD workload identity federation is a new capability that's in public preview. It frees developers from handling application secrets or certificates. This includes secrets in scenarios such as using GitHub Actions and building applications on Kubernetes. Rather than creating an application secret and using that to get tokens for that application, developers can instead use tokens provided by the respective platforms such as GitHub and Kubernetes without having to manage any secrets manually.[Learn more.](#)

Public Preview - Updates to Sign-in Diagnostic

Type: Changed feature

Service category: Reporting

Product capability: Monitoring & Reporting

With this update, the diagnostic covers more scenarios and is made more easily available to admins.

New scenarios covered when using the Sign-in Diagnostic:

- Pass Through Authentication sign-in failures
- Seamless Single-Sign On sign-in failures

Other changes include:

- Flagged Sign-ins will automatically appear for investigation when using the Sign-in Diagnostic from Diagnose and Solve.
 - Sign-in Diagnostic is now available from the Enterprise Apps Diagnose and Solve blade.
 - The Sign-in Diagnostic is now available in the Basic Info tab of the Sign-in Log event view for all sign-in events. [Learn more.](#)
-

General Availability - Privileged Role Administrators can now create Azure AD access reviews on role-assignable groups

Type: Fixed

Service category: Access Reviews

Product capability: Identity Governance

Privileged Role Administrators can now create Azure AD access reviews on Azure AD role-assignable groups, in addition to Azure AD roles. [Learn more.](#)

General Availability - Azure AD single Sign on and device-based Conditional Access support in Firefox on Windows 10/11

Type: New feature

Service category: Authentications (Logins)

Product capability: SSO

We now support native single sign-on (SSO) support and device-based Conditional Access to Firefox browser on Windows 10 and Windows Server 2019 starting in Firefox version 91. [Learn more.](#)

General Availability - New app indicator in My Apps

Type: New feature

Service category: My Apps

Product capability: End User Experiences

Apps that have been recently assigned to the user show up with a "new" indicator. When the app is launched or the page is refreshed, this indicator disappears. [Learn more](#).

General availability - Custom domain support in Azure AD B2C

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

Azure AD B2C customers can now enable custom domains so their end-users are redirected to a custom URL domain for authentication. This is done via integration with Azure Front Door's custom domains capability. [Learn more](#).

General availability - Edge Administrator built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users in this role can create and manage the enterprise site list required for Internet Explorer mode on Microsoft Edge. This role grants permissions to create, edit, and publish the site list and additionally allows access to manage support tickets. [Learn more](#)

General availability - Windows 365 Administrator built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users with this role have global permissions on Windows 365 resources, when the service is present. Additionally, this role contains the ability to manage users and devices to associate a policy, and create and manage groups. [Learn more](#)

New Federated Apps available in Azure AD Application gallery - October 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In October 2021 we've added the following 10 new applications in our App gallery with Federation support:

[Adaptive Shield](#), [SocialChorus Search](#), [Hiretal-SSO](#), [TeamSticker by Communitio](#), [embed signage](#), [JoinedUp](#), [VECOS Releezme Locker management system](#), [Altoura](#), [Dagster Cloud](#), [Qualaroo](#)

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the following article:

<https://aka.ms/AzureADAppRequest>

Continuous Access Evaluation migration with Conditional Access

Type: Changed feature

Service category: Conditional Access

Product capability: User Authentication

A new user experience is available for our CAE tenants. Tenants will now access CAE as part of Conditional Access. Any tenants that were previously using CAE for some (but not all) user accounts under the old UX or had previously disabled the old CAE UX will now be required to undergo a one time migration experience.[Learn more.](#)

Improved group list blade

Type: Changed feature

Service category: Group Management

Product capability: Directory

The new group list blade offers more sort and filtering capabilities, infinite scrolling, and better performance. [Learn more.](#)

General availability - Google deprecation of Gmail sign-in support on embedded webviews on September 30, 2021

Type: Changed feature

Service category: B2B

Product capability: B2B/B2C

Google has deprecated Gmail sign-ins on Microsoft Teams mobile and custom apps that run Gmail authentications on embedded webviews on Sept. 30th, 2021.

If you would like to request an extension, impacted customers with affected OAuth client ID(s) should have received an email from Google Developers with the following information regarding a one-time policy enforcement extension, which must be completed by Jan 31, 2022.

To continue allowing your Gmail users to sign in and redeem, we strongly recommend that you refer to [Embedded vs System Web](#) in the MSAL.NET documentation and modify your apps to use the system browser for sign-in. All MSAL SDKs use the system web-view by default.

As a workaround, we are deploying the device login flow by October 8. Between today and until then, it is likely that it may not be rolled out to all regions yet (in which case, end-users will be met with an error screen until it gets deployed to your region.)

For more details on the device login flow and details on requesting extension to Google, see [Add Google as an identity provider for B2B guest users.](#)

Identity Governance Administrator can create and manage Azure AD access reviews of groups and applications

Type: Changed feature

Service category: Access Reviews

Product capability: Identity Governance

Identity Governance Administrator can create and manage Azure AD access reviews of groups and applications. [Learn more.](#)

Quickstart: Create a new tenant in Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

You can do all of your administrative tasks using the Azure Active Directory (Azure AD) portal, including creating a new tenant for your organization.

In this quickstart, you'll learn how to get to the Azure portal and Azure Active Directory, and you'll learn how to create a basic tenant for your organization.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create a new tenant for your organization

After you sign in to the Azure portal, you can create a new tenant for your organization. Your new tenant represents your organization and helps you to manage a specific instance of Microsoft cloud services for your internal and external users.

To create a new tenant

1. Sign in to your organization's [Azure portal](#).
2. From the Azure portal menu, select **Azure Active Directory**.
3. On the overview page, select **Manage tenants**
4. Select **Create**.

The screenshot shows the Azure Active Directory 'Manage tenants' page. At the top, there is a navigation bar with 'Microsoft Azure' and a search bar. Below the navigation bar, it says 'Home > Fourth Coffee >'. There is a 'Switch tenant' dropdown and a red box highlights the '+ Create' button. The main area shows a table with one row of data:

Organization name	Domain name	Tenant type	Organization ID	Favorite
Fourth Coffee (Default)	fourthcoffee.club	Azure Active Directory	340d0dd4-7adc-4196-b880-8b6f865aa6...	

5. On the Basics tab, select the type of tenant you want to create, either **Azure Active Directory** or **Azure Active Directory (B2C)**.
6. Select **Next: Configuration** to move on to the Configuration tab.

The screenshot shows the 'Create a tenant' configuration step in the Microsoft Azure portal. The 'Configuration' tab is selected. The 'Directory details' section contains fields for 'Organization name' (Contoso Organization), 'Initial domain name' (contosoorg.onmicrosoft.com), and 'Country/Region' (United States). A note below the country field states 'Datacenter location is based on the country/region selected above.' At the bottom, there are 'Review + create' and 'Next : Review + create >' buttons.

7. On the Configuration tab, enter the following information:

- Type *Contoso Organization* into the **Organization name** box.
- Type *Contosoorg* into the **Initial domain name** box.
- Leave the *United States* option in the **Country or region** box.

8. Select **Next: Review + Create**. Review the information you entered and if the information is correct, select **Create**.

Your new tenant is created with the domain contoso.onmicrosoft.com.

Your user account in the new tenant

When you create a new Azure AD tenant, you become the first user of that tenant. As the first user, you're automatically assigned the **Global Admin** role. Check out your user account by navigating to the [Users](#) page.

By default, you're also listed as the **technical contact** for the tenant. Technical contact information is something you can change in [Properties](#).

WARNING

Ensure your directory has at least two accounts with global administrator privileges assigned to them. This will help in the case that one global administrator is locked out. For more detail see the article, [Manage emergency access accounts in Azure AD](#).

Clean up resources

If you're not going to continue to use this application, you can delete the tenant using the following steps:

- Ensure that you're signed in to the directory that you want to delete through the **Directory + subscription** filter in the Azure portal. Switch to the target directory if needed.
- Select **Azure Active Directory**, and then on the **Contoso - Overview** page, select **Delete directory**.

The tenant and its associated information is deleted.

Home > Fourth Coffee >

Switch tenant ... X

[Create](#) [Refresh](#) [Columns](#) | [Switch](#) [Delete](#) [Leave tenant](#) [Make default tenant](#) [More information](#) | [Got feedback?](#)

Current tenant: Fourth Coffee

[Add filters](#)

Showing 2 of 2 results

<input type="checkbox"/> Organization name	Domain name	Tenant type	Organization ID	Favorite
<input checked="" type="checkbox"/> Contoso Organization	contosoorg298.onmicrosoft.com	Azure Active Directory	4adf7813-43cf-4819-a879-d25f4db5943b	
<input type="checkbox"/> Fourth Coffee (Default)	fourthcoffee.club	Azure Active Directory	340d0dd4-7adc-4196-b880-8b6f865aa6...	

Next steps

- Change or add additional domain names, see [How to add a custom domain name to Azure Active Directory](#)
- Add users, see [Add or delete a new user](#)
- Add groups and members, see [Create a basic group and add members](#)
- Learn about [Azure role-based access control \(Azure RBAC\)](#) and [Conditional Access](#) to help manage your organization's application and resource access.
- Learn about Azure AD, including [basic licensing information, terminology, and associated features](#).

Quickstart: View your organization's groups and members in Azure Active Directory

4/10/2022 • 3 minutes to read • [Edit Online](#)

You can view your organization's existing groups and group members using the Azure portal. Groups are used to manage users (members) that all need the same access and permissions for potentially restricted apps and services.

In this quickstart, you'll view all of your organization's existing groups and view the assigned members.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

Before you begin, you'll need to:

- Create an Azure Active Directory tenant. For more information, see [Access the Azure Active Directory portal and create a new tenant](#).

Sign in to the Azure portal

You must sign in to the [Azure portal](#) using a Global administrator account for the directory.

Create a new group

Create a new group, named *MDM policy - West*. For more information about creating a group, see [How to create a basic group and add members](#).

1. Select **Azure Active Directory**, **Groups**, and then select **New group**.
2. Complete the **Group** page:
 - **Group type:** Select **Security**
 - **Group name:** Type *MDM policy - West*
 - **Membership type:** Select **Assigned**.
3. Select **Create**.

Create a new user

Create a new user, named *Alain Charon*. A user must exist before being added as a group member. Check the "Custom domain names" tab first to get the verified domain name in which to create users. For more information about creating a user, see [How to add or delete users](#).

1. Select **Azure Active Directory**, **Users**, and then select **New user**.
2. Complete the **User** page:
 - **Name:** Type *Alain Charon*.
 - **User name:** Type *alain@contoso.com*.
3. Copy the auto-generated password provided in the **Password** box, and then select **Create**.

Add a group member

Now that you have a group and a user, you can add *Alain Charon* as a member to the *MDM policy - West* group. For more information about adding group members, see [How to add or remove group members](#).

1. Select **Azure Active Directory > Groups**.
2. From the **Groups - All groups** page, search for and select the **MDM policy - West** group.
3. From the **MDM policy - West Overview** page, select **Members** from the **Manage** area.
4. Select **Add members**, and then search and select **Alain Charon**.
5. Choose **Select**.

View all groups

You can see all the groups for your organization in the **Groups - All groups** page of the Azure portal.

- Select **Azure Active Directory > Groups**.

The **Groups - All groups** page appears, showing all your active groups.

NAME	GROUP TYPE	MEMBERSHIP TYPE
ADSyncAdmins	Security	Synced
ADSyncBrowse	Security	Synced
ADSyncOperators	Security	Synced
ADSyncPasswordSet	Security	Synced
AzureADPremiumP2-ALL	Security	Synced
Converged	Security	Assigned
DnsAdmins	Security	Synced
DnsAdmins	Security	Synced

Search for the group

Search the **Groups – All groups** page to find the **MDM policy – West** group.

1. From the **Groups - All groups** page, type **MDM** into the **Search** box.

The search results appear under the **Search** box, including the **MDM policy - West** group.

NAME	GROUP TYPE	MEMBERSHIP TYPE
MDM policy - All org	Security	Assigned
MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned
MDM policy - West	Security	Assigned

2. Select the group **MDM policy – West**.
3. View the group info on the **MDM policy - West Overview** page, including the number of members of that group.

Membership type	Type
Assigned	Security
Source	Object ID
Cloud	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

View group members

Now that you've found the group, you can view all the assigned members.

- Select **Members** from the **Manage** area, and then review the complete list of member names assigned to that specific group, including *Alain Charon*.

Home > Contoso > Groups - All groups > MDM policy - West - Members

MDM policy - West - Members

Group

Overview Add members Refresh

Manage

Properties (highlighted)

Members (highlighted)

Owners

Group memberships

Applications

Licenses

Azure resources

Activity

Access reviews

Audit logs

Troubleshooting + Support

Troubleshoot

New support request

NAME	TYPE
AC Alain Charon	User
DM Danielle McKay	User
ES Egbert Schafer	User

Clean up resources

This group is used in several of the how-to processes that are available in the **How-to guides** section of this documentation. However, if you'd rather not use this group, you can delete it and its assigned members using the following steps:

1. On the **Groups - All groups** page, search for the **MDM policy - West** group.
2. Select the **MDM policy - West** group.

The **MDM policy - West Overview** page appears.

3. Select **Delete**.

The group and its associated members are deleted.

Home > Contoso > Groups - All groups > MDM policy - West

MDM policy - West

Group

[Delete](#)

MDM policy - West

Manage

- Properties
- Members
- Owners
- Group memberships
- Applications
- Licenses
- Azure resources

Activity

- Access reviews
- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Membership type: Assigned
Type: Security
Source: Cloud
Object ID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

Members: 50 User(s) | 0 Group(s) | 50 Device(s) | 0 Other(s)

Group memberships: 0 | **Owners:** 2

IMPORTANT

This doesn't delete the user Alain Charon, just his membership in the deleted group.

Next steps

Advance to the next article to learn how to associate a subscription to your Azure AD directory.

[Associate an Azure subscription](#)

Manage app and resource access using Azure Active Directory groups

4/10/2022 • 3 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) lets you use groups to manage access to your cloud-based apps, on-premises apps, and your resources. Your resources can be part of the Azure AD organization, such as permissions to manage objects through roles in Azure AD, or external to the organization, such as for Software as a Service (SaaS) apps, Azure services, SharePoint sites, and on-premises resources.

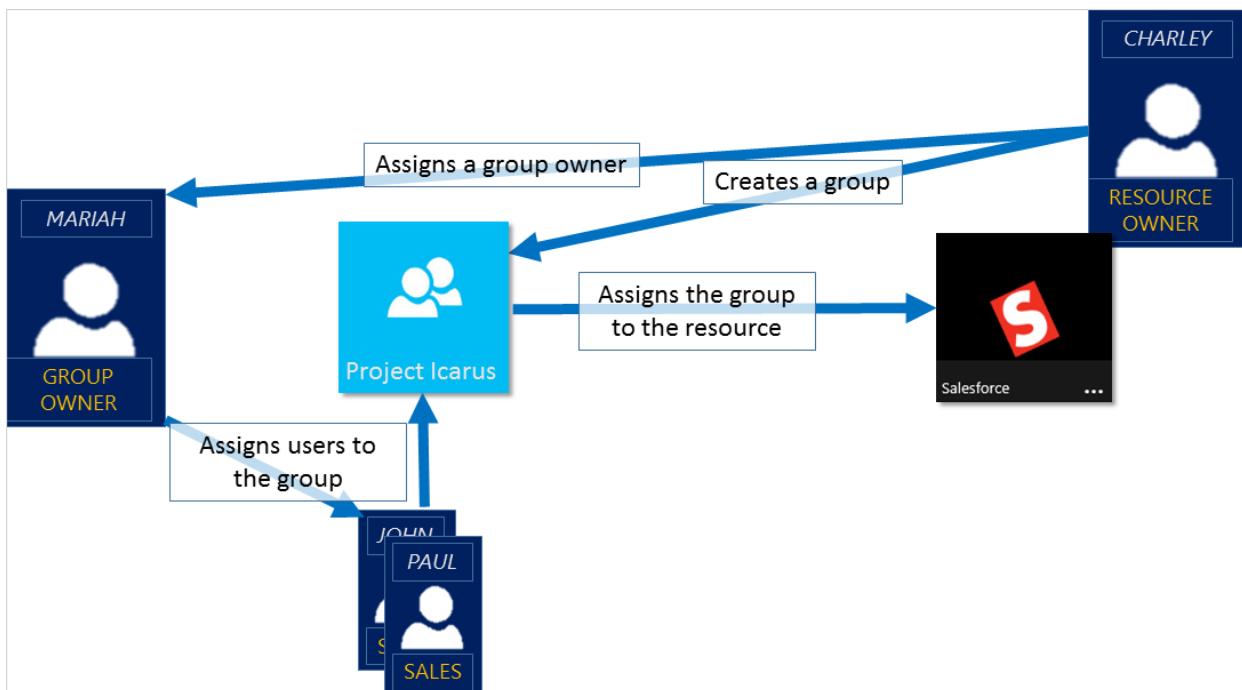
NOTE

In the Azure portal, you can see some groups whose membership and group details you can't manage in the portal:

- Groups synced from on-premises Active Directory can be managed only in on-premises Active Directory.
- Other group types such as distribution lists and mail-enabled security groups are managed only in Exchange admin center or Microsoft 365 admin center. You must sign in to Exchange admin center or Microsoft 365 admin center to manage these groups.

How access management in Azure AD works

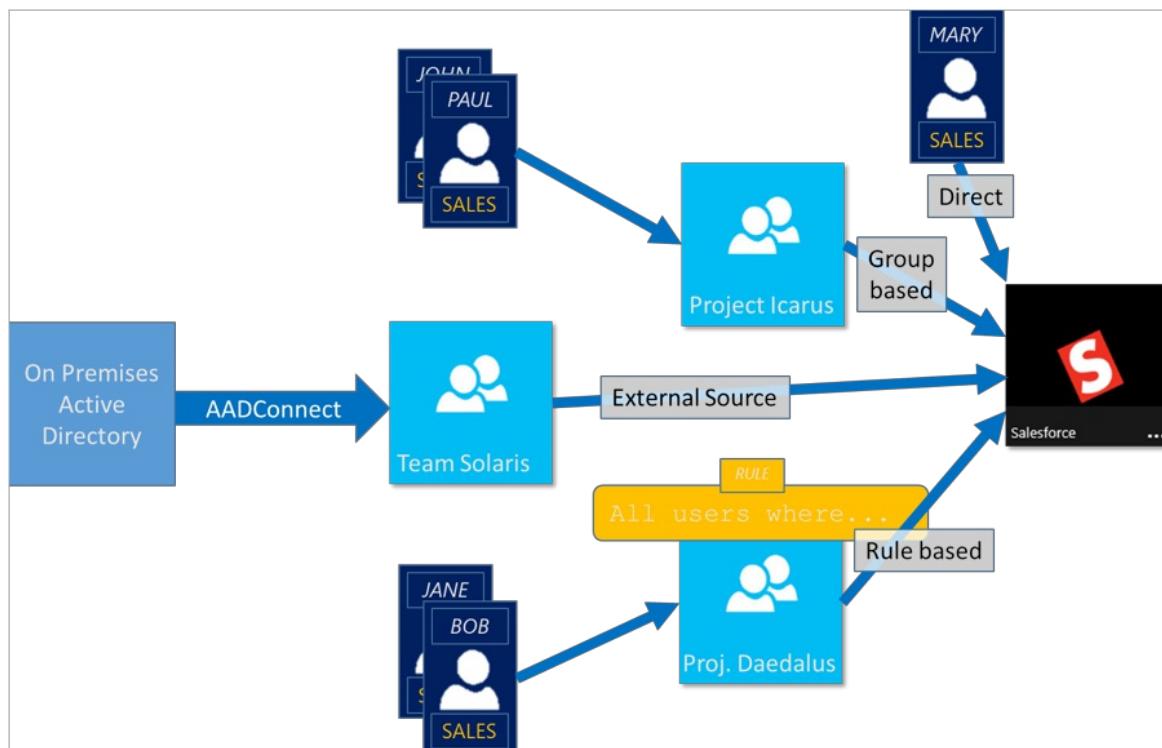
Azure AD helps you give access to your organization's resources by providing access rights to a single user or to an entire Azure AD group. Using groups lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one. The resource or directory owner can also give management rights for the member list to someone else, such as a department manager or a Helpdesk administrator, letting that person add and remove members, as needed. For more information about how to manage group owners, see [Manage group owners](#)



Ways to assign access rights

There are four ways to assign resource access rights to your users:

- **Direct assignment.** The resource owner directly assigns the user to the resource.
- **Group assignment.** The resource owner assigns an Azure AD group to the resource, which automatically gives all of the group members access to the resource. Group membership is managed by both the group owner and the resource owner, letting either owner add or remove members from the group. For more information about adding or removing group membership, see [How to: Add or remove a group from another group using the Azure Active Directory portal](#).
- **Rule-based assignment.** The resource owner creates a group and uses a rule to define which users are assigned to a specific resource. The rule is based on attributes that are assigned to individual users. The resource owner manages the rule, determining which attributes and values are required to allow access to the resource. For more information, see [Create a dynamic group and check status](#).
- **External authority assignment.** Access comes from an external source, such as an on-premises directory or a SaaS app. In this situation, the resource owner assigns a group to provide access to the resource and then the external source manages the group members.



Can users join groups without being assigned?

The group owner can let users find their own groups to join, instead of assigning them. The owner can also set up the group to automatically accept all users that join or to require approval.

After a user requests to join a group, the request is forwarded to the group owner. If it's required, the owner can approve the request and the user is notified of the group membership. However, if you have multiple owners and one of them disapproves, the user is notified, but isn't added to the group. For more information and instructions about how to let your users request to join groups, see [Set up Azure AD so users can request to join groups](#)

Next steps

Now that you have a bit of an introduction to access management using groups, you start to manage your resources and apps.

- [Create a new group using Azure Active Directory](#) or [Create and manage a new group using PowerShell cmdlets](#)

- Use groups to assign access to an integrated SaaS app
- Sync an on-premises group to Azure using Azure AD Connect

What is group-based licensing in Azure Active Directory?

4/10/2022 • 3 minutes to read • [Edit Online](#)

Microsoft paid cloud services, such as Microsoft 365, Enterprise Mobility + Security, Dynamics 365, and other similar products, require licenses. These licenses are assigned to each user who needs access to these services. To manage licenses, administrators use one of the management portals (Office or Azure) and PowerShell cmdlets. Azure Active Directory (Azure AD) is the underlying infrastructure that supports identity management for all Microsoft cloud services. Azure AD stores information about license assignment states for users.

Until now, licenses could only be assigned at the individual user level, which can make large-scale management difficult. For example, to add or remove user licenses based on organizational changes, such as users joining or leaving the organization or a department, an administrator often must write a complex PowerShell script. This script makes individual calls to the cloud service.

To address those challenges, Azure AD now includes group-based licensing. You can assign one or more product licenses to a group. Azure AD ensures that the licenses are assigned to all members of the group. Any new members who join the group are assigned the appropriate licenses. When they leave the group, those licenses are removed. This licensing management eliminates the need for automating license management via PowerShell to reflect changes in the organization and departmental structure on a per-user basis.

Licensing requirements

You must have one of the following licenses **for every user who benefits from** group-based licensing:

- Paid or trial subscription for Azure AD Premium P1 and above
- Paid or trial edition of Microsoft 365 Business Premium or Office 365 Enterprise E3 or Office 365 A3 or Office 365 GCC G3 or Office 365 E3 for GCCH or Office 365 E3 for DOD and above

Required number of licenses

For any groups assigned a license, you must also have a license for each unique member. While you don't have to assign each member of the group a license, you must have at least enough licenses to include all of the members. For example, if you have 1,000 unique members who are part of licensed groups in your tenant, you must have at least 1,000 licenses to meet the licensing agreement.

Features

Here are the main features of group-based licensing:

- Licenses can be assigned to any security group in Azure AD. Security groups can be synced from on-premises, by using Azure AD Connect. You can also create security groups directly in Azure AD (also called cloud-only groups), or automatically via the Azure AD dynamic group feature.
- When a product license is assigned to a group, the administrator can disable one or more service plans in the product. Typically, this assignment is done when the organization is not yet ready to start using a service included in a product. For example, the administrator might assign Microsoft 365 to a department, but temporarily disable the Yammer service.
- All Microsoft cloud services that require user-level licensing are supported. This support includes all Microsoft 365 products, Enterprise Mobility + Security, and Dynamics 365.

- Group-based licensing is currently available only through the [Azure portal](#). If you primarily use other management portals for user and group management, such as the [Microsoft 365 admin center](#), you can continue to do so. But you should use the Azure portal to manage licenses at group level.
- Azure AD automatically manages license modifications that result from group membership changes. Typically, license modifications are effective within minutes of a membership change.
- A user can be a member of multiple groups with license policies specified. A user can also have some licenses that were directly assigned, outside of any groups. The resulting user state is a combination of all assigned product and service licenses. If a user is assigned same license from multiple sources, the license will be consumed only once.
- In some cases, licenses cannot be assigned to a user. For example, there might not be enough available licenses in the tenant, or conflicting services might have been assigned at the same time. Administrators have access to information about users for whom Azure AD could not fully process group licenses. They can then take corrective action based on that information.

Your feedback is welcome!

If you have feedback or feature requests, share them with us using [the Azure AD admin forum](#).

Next steps

To learn more about other scenarios for license management through group-based licensing, see:

- [Assigning licenses to a group in Azure Active Directory](#)
- [Identifying and resolving license problems for a group in Azure Active Directory](#)
- [How to migrate individual licensed users to group-based licensing in Azure Active Directory](#)
- [How to migrate users between product licenses using group-based licensing in Azure Active Directory](#)
- [Azure Active Directory group-based licensing additional scenarios](#)
- [PowerShell examples for group-based licensing in Azure Active Directory](#)

What are the default user permissions in Azure Active Directory?

4/10/2022 • 10 minutes to read • [Edit Online](#)

In Azure Active Directory (Azure AD), all users are granted a set of default permissions. A user's access consists of the type of user, their [role assignments](#), and their ownership of individual objects.

This article describes those default permissions and compares the member and guest user defaults. The default user permissions can be changed only in user settings in Azure AD.

Member and guest users

The set of default permissions depends on whether the user is a native member of the tenant (member user) or whether the user is brought over from another directory as a business-to-business (B2B) collaboration guest (guest user). For more information about adding guest users, see [What is Azure AD B2B collaboration?](#). Here are the capabilities of the default permissions:

- *Member users* can register applications, manage their own profile photo and mobile phone number, change their own password, and invite B2B guests. These users can also read all directory information (with a few exceptions).
- *Guest users* have restricted directory permissions. They can manage their own profile, change their own password, and retrieve some information about other users, groups, and apps. However, they can't read all directory information.

For example, guest users can't enumerate the list of all users, groups, and other directory objects. Guests can be added to administrator roles, which grant them full read and write permissions. Guests can also invite other guests.

Compare member and guest default permissions

Area	Member User Permissions	Default Guest User Permissions	Restricted Guest User Permissions
Users and contacts	<ul style="list-style-type: none">• Enumerate the list of all users and contacts• Read all public properties of users and contacts• Invite guests• Change their own password• Manage their own mobile phone number• Manage their own photo• Invalidate their own refresh tokens	<ul style="list-style-type: none">• Read their own properties• Read display name, email, sign-in name, photo, user principal name, and user type properties of other users and contacts• Change their own password• Search for another user by object ID (if allowed)• Read manager and direct report information of other users	<ul style="list-style-type: none">• Read their own properties• Change their own password• Manage their own mobile phone number

Area	Member User Permissions	Default Guest User Permissions	Restricted Guest User Permissions
Groups	<ul style="list-style-type: none"> • Create security groups • Create Microsoft 365 groups • Enumerate the list of all groups • Read all properties of groups • Read non-hidden group memberships • Read hidden Microsoft 365 group memberships for joined groups • Manage properties, ownership, and membership of groups that the user owns • Add guests to owned groups • Manage dynamic membership settings • Delete owned groups • Restore owned Microsoft 365 groups 	<ul style="list-style-type: none"> • Read properties of non-hidden groups, including membership and ownership (even non-joined groups) • Read hidden Microsoft 365 group memberships for joined groups • Search for groups by display name or object ID (if allowed) 	<ul style="list-style-type: none"> • Read object ID for joined groups • Read membership and ownership of joined groups in some Microsoft 365 apps (if allowed)
Applications	<ul style="list-style-type: none"> • Register (create) new applications • Enumerate the list of all applications • Read properties of registered and enterprise applications • Manage application properties, assignments, and credentials for owned applications • Create or delete application passwords for users • Delete owned applications • Restore owned applications 	<ul style="list-style-type: none"> • Read properties of registered and enterprise applications 	<ul style="list-style-type: none"> • Read properties of registered and enterprise applications

Area	Member User Permissions	Default Guest User Permissions	Restricted Guest User Permissions
Devices	<ul style="list-style-type: none"> Enumerate the list of all devices Read all properties of devices Manage all properties of owned devices 	No permissions	No permissions
Directory	<ul style="list-style-type: none"> Read all company information Read all domains Read all partner contracts 	<ul style="list-style-type: none"> Read company display name Read all domains 	<ul style="list-style-type: none"> Read company display name Read all domains
Roles and scopes	<ul style="list-style-type: none"> Read all administrative roles and memberships Read all properties and membership of administrative units 	No permissions	No permissions
Subscriptions	<ul style="list-style-type: none"> Read all subscriptions Enable service plan memberships 	No permissions	No permissions
Policies	<ul style="list-style-type: none"> Read all properties of policies Manage all properties of owned policies 	No permissions	No permissions

Restrict member users' default permissions

It's possible to add restrictions to users' default permissions. You can use this feature if you don't want all users in the directory to have access to the Azure AD admin portal/directory.

For example, a university has many users in its directory. The admin might not want all of the students in the directory to be able to see the full directory and violate other students' privacy. The use of this feature is optional and at the discretion of the Azure AD administrator.

You can restrict default permissions for member users in the following ways:

Permission	Setting Explanation
Register applications	Setting this option to No prevents users from creating application registrations. You can grant the ability back to specific individuals by adding them to the application developer role.

PERMISSION	SETTING EXPLANATION
Allow users to connect work or school account with LinkedIn	Setting this option to No prevents users from connecting their work or school account with their LinkedIn account. For more information, see LinkedIn account connections data sharing and consent .
Create security groups	Setting this option to No prevents users from creating security groups. Global administrators and user administrators can still create security groups. To learn how, see Azure Active Directory cmdlets for configuring group settings .
Create Microsoft 365 groups	Setting this option to No prevents users from creating Microsoft 365 groups. Setting this option to Some allows a set of users to create Microsoft 365 groups. Global administrators and user administrators can still create Microsoft 365 groups. To learn how, see Azure Active Directory cmdlets for configuring group settings .
Access the Azure AD administration portal	<p>Setting this option to No lets non-administrators use the Azure AD administration portal to read and manage Azure AD resources. Yes restricts all non-administrators from accessing any Azure AD data in the administration portal.</p> <p>This setting does not restrict access to Azure AD data by using PowerShell or other clients such as Visual Studio. When you set this option to Yes to grant a specific non-admin user the ability to use the Azure AD administration portal, assign any administrative role such as the directory reader role.</p> <p>The directory reader role allows reading basic directory information. Member users have it by default. Guests and service principals don't.</p> <p>This setting blocks non-admin users who are owners of groups or applications from using the Azure portal to manage their owned resources. This setting does not restrict access as long as a user is assigned a custom role (or any role) and is not just a user.</p>
Read other users	<p>This setting is available in Microsoft Graph and PowerShell only. Setting this flag to <code>\$false</code> prevents all non-admins from reading user information from the directory. This flag does not prevent reading user information in other Microsoft services like Exchange Online.</p> <p>This setting is meant for special circumstances, so we don't recommend setting the flag to <code>\$false</code>.</p>

NOTE

It's assumed that the average user would only use the portal to access Azure AD, and not use PowerShell or the Azure CLI to access their resources. Currently, restricting access to users' default permissions occurs only when users try to access the directory within the Azure portal.

Restrict guest users' default permissions

You can restrict default permissions for guest users in the following ways.

NOTE

The **Guest user access restrictions** setting replaced the **Guest users permissions are limited** setting. For guidance on using this feature, see [Restrict guest access permissions in Azure Active Directory](#).

PERMISSION	SETTING EXPLANATION
Guest user access restrictions	<p>Setting this option to Guest users have the same access as members grants all member user permissions to guest users by default.</p> <p>Setting this option to Guest user access is restricted to properties and memberships of their own directory objects restricts guest access to only their own user profile by default. Access to other users is no longer allowed, even when they're searching by user principal name, object ID, or display name. Access to group information, including groups memberships, is also no longer allowed.</p> <p>This setting does not prevent access to joined groups in some Microsoft 365 services like Microsoft Teams. To learn more, see Microsoft Teams guest access.</p> <p>Guest users can still be added to administrator roles regardless of this permission setting.</p>
Guests can invite	<p>Setting this option to Yes allows guests to invite other guests. To learn more, see Configure external collaboration settings.</p>
Members can invite	<p>Setting this option to Yes allows non-admin members of your directory to invite guests. To learn more, see Configure external collaboration settings.</p>
Admins and users in the guest inviter role can invite	<p>Setting this option to Yes allows admins and users in the guest inviter role to invite guests. When you set this option to Yes, users in the guest inviter role will still be able to invite guests, regardless of the Members can invite setting. To learn more, see Configure external collaboration settings.</p>

Object ownership

Application registration owner permissions

When a user registers an application, they're automatically added as an owner for the application. As an owner, they can manage the metadata of the application, such as the name and permissions that the app requests. They can also manage the tenant-specific configuration of the application, such as the single sign-on (SSO) configuration and user assignments.

An owner can also add or remove other owners. Unlike global administrators, owners can manage only the applications that they own.

Enterprise application owner permissions

When a user adds a new enterprise application, they're automatically added as an owner. As an owner, they can manage the tenant-specific configuration of the application, such as the SSO configuration, provisioning, and

user assignments.

An owner can also add or remove other owners. Unlike global administrators, owners can manage only the applications that they own.

Group owner permissions

When a user creates a group, they're automatically added as an owner for that group. As an owner, they can manage properties of the group (such as the name) and manage group membership.

An owner can also add or remove other owners. Unlike global administrators and user administrators, owners can manage only the groups that they own.

To assign a group owner, see [Managing owners for a group](#).

Ownership permissions

The following tables describe the specific permissions in Azure AD that member users have over owned objects. Users have these permissions only on objects that they own.

Owned application registrations

Users can perform the following actions on owned application registrations:

ACTION	DESCRIPTION
microsoft.directory/applications/audience/update	Update the <code>applications.audience</code> property in Azure AD.
microsoft.directory/applications/authentication/update	Update the <code>applications.authentication</code> property in Azure AD.
microsoft.directory/applications/basic/update	Update basic properties on applications in Azure AD.
microsoft.directory/applications/credentials/update	Update the <code>applications.credentials</code> property in Azure AD.
microsoft.directory/applications/delete	Delete applications in Azure AD.
microsoft.directory/applications/owners/update	Update the <code>applications.owners</code> property in Azure AD.
microsoft.directory/applications/permissions/update	Update the <code>applications.permissions</code> property in Azure AD.
microsoft.directory/applications/policies/update	Update the <code>applications.policies</code> property in Azure AD.
microsoft.directory/applications restore	Restore applications in Azure AD.

Owned enterprise applications

Users can perform the following actions on owned enterprise applications. An enterprise application consists of a service principal, one or more application policies, and sometimes an application object in the same tenant as the service principal.

ACTION	DESCRIPTION
microsoft.directory/auditLogs/allProperties/read	Read all properties (including privileged properties) on audit logs in Azure AD.
microsoft.directory/policies/basic/update	Update basic properties on policies in Azure AD.

ACTION	DESCRIPTION
microsoft.directory/policies/delete	Delete policies in Azure AD.
microsoft.directory/policies/owners/update	Update the <code>policies.owners</code> property in Azure AD.
microsoft.directory/servicePrincipals/appRoleAssignedTo/update	Update the <code>servicePrincipals.appRoleAssignedTo</code> property in Azure AD.
microsoft.directory/servicePrincipals/appRoleAssignments/update	Update the <code>users.appRoleAssignments</code> property in Azure AD.
microsoft.directory/servicePrincipals/audience/update	Update the <code>servicePrincipals.audience</code> property in Azure AD.
microsoft.directory/servicePrincipals/authentication/update	Update the <code>servicePrincipals.authentication</code> property in Azure AD.
microsoft.directory/servicePrincipals/basic/update	Update basic properties on service principals in Azure AD.
microsoft.directory/servicePrincipals/credentials/update	Update the <code>servicePrincipals.credentials</code> property in Azure AD.
microsoft.directory/servicePrincipals/delete	Delete service principals in Azure AD.
microsoft.directory/servicePrincipals/owners/update	Update the <code>servicePrincipals.owners</code> property in Azure AD.
microsoft.directory/servicePrincipals/permissions/update	Update the <code>servicePrincipals.permissions</code> property in Azure AD.
microsoft.directory/servicePrincipals/policies/update	Update the <code>servicePrincipals.policies</code> property in Azure AD.
microsoft.directory/signInReports/allProperties/read	Read all properties (including privileged properties) on sign-in reports in Azure AD.

Owned devices

Users can perform the following actions on owned devices:

ACTION	DESCRIPTION
microsoft.directory/devices/bitLockerRecoveryKeys/read	Read the <code>devices.bitLockerRecoveryKeys</code> property in Azure AD.
microsoft.directory/devices/disable	Disable devices in Azure AD.

Owned groups

Users can perform the following actions on owned groups.

NOTE

Owners of dynamic groups must have a global administrator, group administrator, Intune administrator, or user administrator role to edit group membership rules. For more information, see [Create or update a dynamic group in Azure Active Directory](#).

ACTION	DESCRIPTION
<code>microsoft.directory/groups/appRoleAssignments/update</code>	Update the <code>groups.appRoleAssignments</code> property in Azure AD.
<code>microsoft.directory/groups/basic/update</code>	Update basic properties on groups in Azure AD.
<code>microsoft.directory/groups/delete</code>	Delete groups in Azure AD.
<code>microsoft.directory/groups/members/update</code>	Update the <code>groups.members</code> property in Azure AD.
<code>microsoft.directory/groups/owners/update</code>	Update the <code>groups.owners</code> property in Azure AD.
<code>microsoft.directory/groups/restore</code>	Restore groups in Azure AD.
<code>microsoft.directory/groups/settings/update</code>	Update the <code>groups.settings</code> property in Azure AD.

Next steps

- To learn more about the **Guest user access restrictions** setting, see [Restrict guest access permissions in Azure Active Directory](#).
- To learn more about how to assign Azure AD administrator roles, see [Assign a user to administrator roles in Azure Active Directory](#).
- To learn more about how resource access is controlled in Microsoft Azure, see [Understanding resource access in Azure](#).
- For more information on how Azure AD relates to your Azure subscription, see [How Azure subscriptions are associated with Azure Active Directory](#).
- [Manage users](#).

What are custom security attributes in Azure AD? (Preview)

4/10/2022 • 8 minutes to read • [Edit Online](#)

IMPORTANT

Custom security attributes are currently in PREVIEW. See the [Supplemental Terms of Use for Microsoft Azure Previews](#) for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Custom security attributes in Azure Active Directory (Azure AD) are business-specific attributes (key-value pairs) that you can define and assign to Azure AD objects. These attributes can be used to store information, categorize objects, or enforce fine-grained access control over specific Azure resources. Custom security attributes can be used with [Azure attribute-based access control \(Azure ABAC\)](#).

Why use custom security attributes?

- Extend user profiles, such as add Employee Hire Date and Hourly Salary to all my employees.
- Ensure only administrators can see the Hourly Salary attribute in my employees' profiles.
- Categorize hundreds or thousands of applications to easily create a filterable inventory for auditing.
- Grant users access to the Azure Storage blobs belonging to a project.

What can I do with custom security attributes?

- Define business-specific information (attributes) for your tenant.
- Add a set of custom security attributes on users, applications, Azure AD resources, or Azure resources.
- Manage Azure AD objects using custom security attributes with queries and filters.
- Provide attribute governance so attributes determine who can get access.

Features of custom security attributes

- Available tenant-wide
- Include a description
- Support different data types: Boolean, integer, string
- Support single value or multiple values
- Support user-defined free-form values or predefined values
- Assign custom security attributes to directory synced users from an on-premises Active Directory

The following example shows how you can specify custom security attribute values that are single, multiple, free-form, or predefined.

Attribute set	Attribute name	Attribute descrip...	Data type	Multi-valued	Assigned values
Engineering	Project	Active projects for ...	String	Yes	2 values
Marketing	Level	Deployment level	String	No	Public
Engineering	ProjectDate	Target completion ...	String	No	2021-12-01
Engineering	Certification	Indicates whether c...	Boolean	No	true
Engineering	CostCenter	Cost center codes	Integer	Yes	1 value

Objects that support custom security attributes

Currently, you can add custom security attributes for the following Azure AD objects:

- Azure AD users
- Azure AD enterprise applications (service principals)
- Managed identities for Azure resources

How do custom security attributes compare with directory schema extensions?

Here are some ways that custom security attributes compare with [directory schema extensions](#):

- Directory schema extensions cannot be used for authorization scenarios and attributes because the access control for the extension attributes is tied to the Azure AD object. Custom security attributes can be used for authorization and attributes needing access control because the custom security attributes can be managed and protected through separate permissions.
- Directory schema extensions are tied to an application and share the lifecycle of an application. Custom security attributes are tenant wide and not tied to an application.
- Directory schema extensions support assigning a single value to an attribute. Custom security attributes support assigning multiple values to an attribute.

Steps to use custom security attributes

1. Check permissions

Check that you are assigned the [Attribute Definition Administrator](#) or [Attribute Assignment Administrator](#) roles. If not, check with your administrator to assign you the appropriate role at tenant scope or attribute set scope. By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes. If necessary, a Global Administrator can assign these roles to themselves.



2. Add attribute sets

Add attribute sets to group and manage related custom security attributes. [Learn more](#)

Attribute set:
Engineering



Attribute set:
Marketing



3. Manage attribute sets

Specify who can read, define, or assign custom security attributes in an attribute set. [Learn more](#)

Attribute set:
Engineering



Alice
Attribute Definition
Administrator

Chandra
Attribute Assignment
Administrator

Attribute set:
Marketing



Bob
Attribute Definition Administrator
Attribute Assignment Administrator

4. Define attributes

Add your custom security attributes to your directory. You can specify the date type (Boolean, integer, or string) and whether values are predefined, free-form, single, or multiple. [Learn more](#)

Attribute set:
Engineering



Certification={true, false}
CostCenter={1001, 1002, 1003}
Project={Alpine, Baker, Cascade}
ProjectDate={}

Alice
Attribute Definition
Administrator

Chandra
Attribute Assignment
Administrator

Attribute set:
Marketing



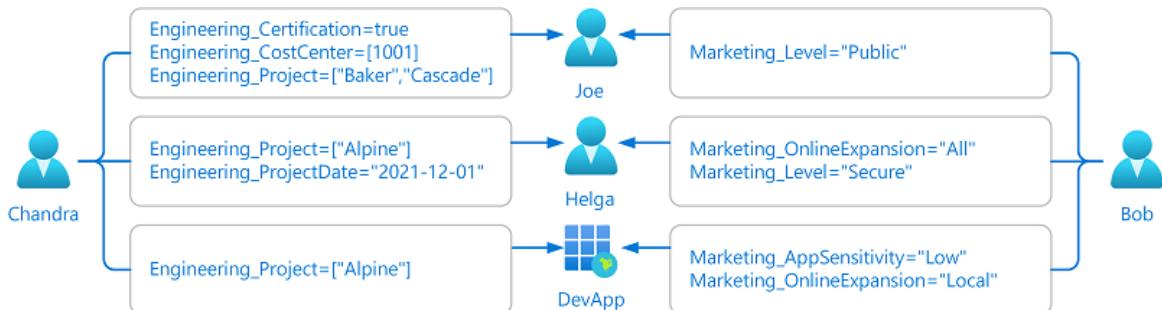
AppCountry={}
AppSensitivity={High, Medium, Low}
Level={Internal, Public, Secure}
OnlineExpansion={Global, Local, All}

Bob

Attribute Definition Administrator
Attribute Assignment Administrator

5. Assign attributes

Assign custom security attributes to Azure AD objects for your business scenarios. [Learn more](#)



6. Use attributes

Filter users and applications that use custom security attributes. [Learn more](#)

Add conditions that use custom security attributes to Azure role assignments for fine-grained access control. [Learn more](#)

Terminology

To better understand custom security attributes, you can refer back to the following list of terms.

TERM	DEFINITION
attribute definition	The schema of a custom security attribute or key-value pair. For example, the custom security attribute name, description, data type, and predefined values.
attribute set	A collection of related custom security attributes. Attribute sets can be delegated to other users for defining and assigning custom security attributes.
attribute name	A unique name of a custom security attribute within an attribute set. The combination of attribute set and attribute name forms a unique attribute for your tenant.
attribute assignment	The assignment of a custom security attribute to an Azure AD object, such as users, enterprise applications (service principals), and managed identities.
predefined value	A value that is allowed for a custom security attribute.

Custom security attribute properties

The following table lists the properties you can specify for attribute sets and custom security attributes. Some properties are immutable and cannot be changed later.

PROPERTY	REQUIRED	CAN BE CHANGED LATER	DESCRIPTION
Attribute set name	✓		Name of the attribute set. Must be unique within a tenant. Cannot include spaces or special characters.
Attribute set description		✓	Description of the attribute set.
Maximum number of attributes		✓	Maximum number of custom security attributes that can be defined in an attribute set. Default value is <code>null</code> . If not specified, the administrator can add up to the maximum of 500 active attributes per tenant.
Attribute set	✓		A collection of related custom security attributes. Every custom security attribute must be part of an attribute set.
Attribute name	✓		Name of the custom security attribute. Must be unique within an attribute set. Cannot include spaces or special characters.

PROPERTY	REQUIRED	CAN BE CHANGED LATER	DESCRIPTION
Attribute description		✓	Description of the custom security attribute.
Data type	✓		Data type for the custom security attribute values. Supported types are <code>Boolean</code> , <code>Integer</code> , and <code>String</code> .
Allow multiple values to be assigned	✓		Indicates whether multiple values can be assigned to the custom security attribute. If data type is set to <code>Boolean</code> , cannot be set to Yes.
Only allow predefined values to be assigned	✓		Indicates whether only predefined values can be assigned to the custom security attribute. If set to No, free-form values are allowed. Can later be changed from Yes to No, but cannot be changed from No to Yes. If data type is set to <code>Boolean</code> , cannot be set to Yes.
Predefined values			Predefined values for the custom security attribute of the selected data type. More predefined values can be added later. Values can include spaces, but some special characters are not allowed.
Predefined value is active		✓	Specifies whether the predefined value is active or deactivated. If set to false, the predefined value cannot be assigned to any additional supported directory objects.
Attribute is active		✓	Specifies whether the custom security attribute is active or deactivated.

Limits and constraints

Here are some of the limits and constraints for custom security attributes.

RESOURCE	LIMIT	NOTES

RESOURCE	LIMIT	NOTES
Attribute definitions per tenant	500	Applies only to active attributes in the tenant
Attribute sets per tenant	500	
Attribute set name length	32	Unicode characters and case insensitive
Attribute set description length	128	Unicode characters
Attribute name length	32	Unicode characters and case insensitive
Attribute description length	128	Unicode characters
Predefined values		Unicode characters and case sensitive
Predefined values per attribute definition	100	
Attribute value length	64	Unicode characters
Attribute values assigned per object	50	Values can be distributed across single and multi-valued attributes. Example: 5 attributes with 10 values each or 50 attributes with 1 value each
Characters not allowed for: Attribute set name Attribute name	<space> ` ~ ! @ # \$ % ^ & * () - + = { [}] \ \ : ; " ' < , > . ? /	Attribute set name and attribute name cannot start with a number
Characters not allowed for: Attribute values	# % & * + \ : " / < > ?	

Custom security attribute roles

Azure AD provides built-in roles to work with custom security attributes. The Attribute Definition Administrator role is the minimum role you need to manage custom security attributes. The Attribute Assignment Administrator role is the minimum role you need to assign custom security attribute values for Azure AD objects like users and applications. You can assign these roles at tenant scope or at attribute set scope.

ROLE	PERMISSIONS
Attribute Definition Reader	Read attribute sets Read custom security attribute definitions
Attribute Definition Administrator	Manage all aspects of attribute sets Manage all aspects of custom security attribute definitions
Attribute Assignment Reader	Read attribute sets Read custom security attribute definitions Read custom security attribute keys and values for users and service principals

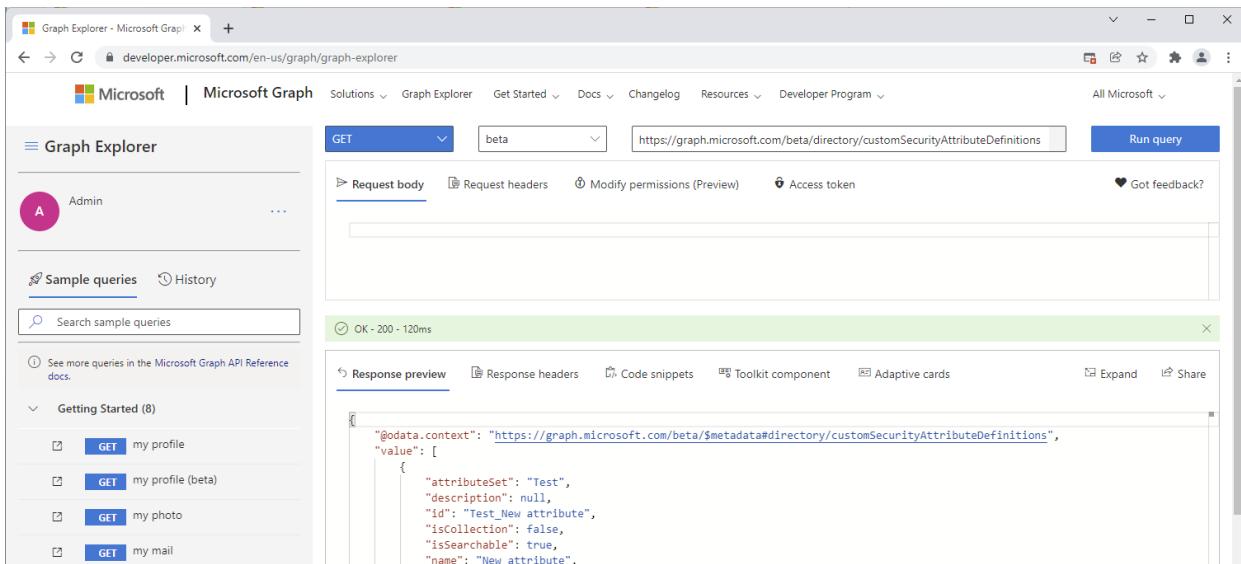
ROLE	PERMISSIONS
Attribute Assignment Administrator	Read attribute sets Read custom security attribute definitions Read and update custom security attribute keys and values for users and service principals

IMPORTANT

By default, **Global Administrator** and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Graph Explorer

If you use the Microsoft Graph API, you can use [Graph Explorer](#) to more easily try the Microsoft Graph APIs for custom security attributes. For more information, see [Overview of custom security attributes using the Microsoft Graph API](#).


 A screenshot of the Microsoft Graph Explorer web application. The top navigation bar shows 'Microsoft Graph' and various links like 'Solutions', 'Graph Explorer', 'Get Started', 'Docs', 'Changelog', 'Resources', and 'Developer Program'. Below the navigation is a search bar with 'beta' selected and the URL 'https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions'. The main area is titled 'Graph Explorer' and shows a user profile 'A Admin'. There are tabs for 'Request body', 'Request headers', 'Modify permissions (Preview)', 'Access token', and 'Run query'. Below these tabs is a large text input field. To the right of the input field is a button labeled 'OK - 200 - 120ms'. At the bottom of the main area is a 'Response preview' section with tabs for 'Response preview', 'Response headers', 'Code snippets', 'Toolkit component', 'Adaptive cards', 'Expand', and 'Share'. The 'Response preview' tab is selected and displays a JSON response structure.

Known issues

Here are some of the known issues with custom security attributes:

- Global Administrators can read audit logs for custom security attribute definitions and assignments.
- If you have an Azure AD Premium P2 license, you can't add eligible role assignments at attribute set scope.
- If you have an Azure AD Premium P2 license, the **Assigned roles** page for a user does not list permanent role assignments at attribute set scope. The role assignments exist, but aren't listed.

Depending on whether you have an Azure AD Premium P1 or P2 license, here are the role assignment tasks that are currently supported for custom security attribute roles:

ROLE ASSIGNMENT TASK	PREMIUM P1	PREMIUM P2
Permanent role assignments	✓	✓
Eligible role assignments	n/a	✓
Permanent role assignments at attribute set scope	✓	✓

ROLE ASSIGNMENT TASK	PREMIUM P1	PREMIUM P2
----------------------	------------	------------

Eligible role assignments at attribute set scope	n/a	✗
Assigned roles page lists permanent role assignments at attribute set scope	✓	⚠ Role assignments exist, but aren't listed

License requirements

Using this feature requires an Azure AD Premium P1 license. To find the right license for your requirements, see [Compare generally available features of Azure AD](#).

Next steps

- [Add or deactivate custom security attributes in Azure AD](#)
- [Manage access to custom security attributes in Azure AD](#)
- [Assign or remove custom security attributes for a user](#)

What is the Azure Active Directory architecture?

4/10/2022 • 6 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) enables you to securely manage access to Azure services and resources for your users. Included with Azure AD is a full suite of identity management capabilities. For information about Azure AD features, see [What is Azure Active Directory?](#)

With Azure AD, you can create and manage users and groups, and enable permissions to allow and deny access to enterprise resources. For information about identity management, see [The fundamentals of Azure identity management](#).

Azure AD architecture

Azure AD's geographically distributed architecture combines extensive monitoring, automated rerouting, failover, and recovery capabilities, which deliver company-wide availability and performance to customers.

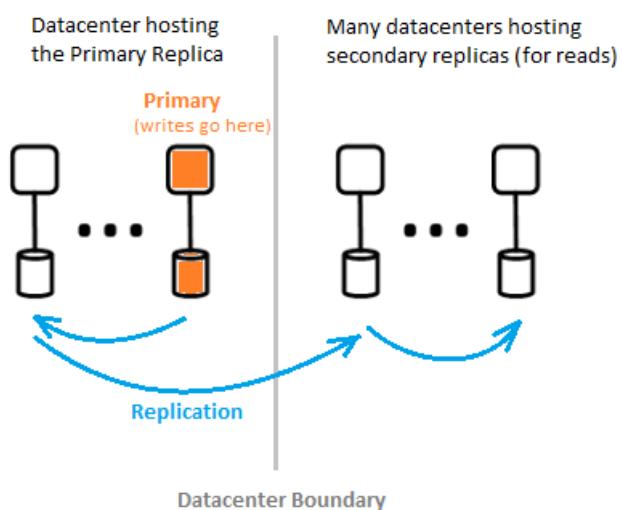
The following architecture elements are covered in this article:

- Service architecture design
- Scalability
- Continuous availability
- Datacenters

Service architecture design

The most common way to build an accessible and usable, data-rich system is through independent building blocks or scale units. For the Azure AD data tier, scale units are called *partitions*.

The data tier has several front-end services that provide read-write capability. The diagram below shows how the components of a single-directory partition are delivered throughout geographically distributed datacenters.



The components of Azure AD architecture include a primary replica and secondary replicas.

Primary replica

The *primary replica* receives all *writes* for the partition it belongs to. Any write operation is immediately replicated to a secondary replica in a different datacenter before returning success to the caller, thus ensuring geo-redundant durability of writes.

Secondary replicas

All directory *reads* are serviced from *secondary replicas*, which are at datacenters that are physically located across different geographies. There are many secondary replicas, as data is replicated asynchronously. Directory reads, such as authentication requests, are serviced from datacenters that are close to customers. The secondary replicas are responsible for read scalability.

Scalability

Scalability is the ability of a service to expand to meet increasing performance demands. Write scalability is achieved by partitioning the data. Read scalability is achieved by replicating data from one partition to multiple secondary replicas distributed throughout the world.

Requests from directory applications are routed to the datacenter that they are physically closest to. Writes are transparently redirected to the primary replica to provide read-write consistency. Secondary replicas significantly extend the scale of partitions because the directories are typically serving reads most of the time.

Directory applications connect to the nearest datacenters. This connection improves performance, and therefore scaling out is possible. Since a directory partition can have many secondary replicas, secondary replicas can be placed closer to the directory clients. Only internal directory service components that are write-intensive target the active primary replica directly.

Continuous availability

Availability (or uptime) defines the ability of a system to perform uninterrupted. The key to Azure AD's high-availability is that the services can quickly shift traffic across multiple geographically distributed datacenters. Each datacenter is independent, which enables de-correlated failure modes. Through this high availability design, Azure AD requires no downtime for maintenance activities.

Azure AD's partition design is simplified compared to the enterprise AD design, using a single-master design that includes a carefully orchestrated and deterministic primary replica failover process.

Fault tolerance

A system is more available if it is tolerant to hardware, network, and software failures. For each partition on the directory, a highly available master replica exists: The primary replica. Only writes to the partition are performed at this replica. This replica is being continuously and closely monitored, and writes can be immediately shifted to another replica (which becomes the new primary) if a failure is detected. During failover, there could be a loss of write availability typically of 1-2 minutes. Read availability is not affected during this time.

Read operations (which outnumber writes by many orders of magnitude) only go to secondary replicas. Since secondary replicas are idempotent, loss of any one replica in a given partition is easily compensated by directing the reads to another replica, usually in the same datacenter.

Data durability

A write is durably committed to at least two datacenters prior to it being acknowledged. This happens by first committing the write on the primary, and then immediately replicating the write to at least one other datacenter. This write action ensures that a potential catastrophic loss of the datacenter hosting the primary does not result in data loss.

Azure AD maintains a zero [Recovery Time Objective \(RTO\)](#) to not lose data on failovers. This includes:

- Token issuance and directory reads
- Allowing only about 5 minutes RTO for directory writes

Datacenters

Azure AD's replicas are stored in datacenters located throughout the world. For more information, see [Azure global infrastructure](#).

Azure AD operates across datacenters with the following characteristics:

- Authentication, Graph, and other AD services reside behind the Gateway service. The Gateway manages load balancing of these services. It will fail over automatically if any unhealthy servers are detected using transactional health probes. Based on these health probes, the Gateway dynamically routes traffic to healthy datacenters.
- For *reads*, the directory has secondary replicas and corresponding front-end services in an active-active configuration operating in multiple datacenters. In case of a failure of an entire datacenter, traffic will be automatically routed to a different datacenter. *For *writes*, the directory will fail over primary (master) replica across datacenters via planned (new primary is synchronized to old primary) or emergency failover procedures. Data durability is achieved by replicating any commit to at least two datacenters.

Data consistency

The directory model is one of eventual consistencies. One typical problem with distributed asynchronously replicating systems is that the data returned from a "particular" replica may not be up-to-date.

Azure AD provides read-write consistency for applications targeting a secondary replica by routing its writes to the primary replica, and synchronously pulling the writes back to the secondary replica.

Application writes using the Microsoft Graph API of Azure AD are abstracted from maintaining affinity to a directory replica for read-write consistency. The Microsoft Graph API service maintains a logical session, which has affinity to a secondary replica used for reads; affinity is captured in a "replica token" that the service caches using a distributed cache in the secondary replica datacenter. This token is then used for subsequent operations in the same logical session. To continue using the same logical session, subsequent requests must be routed to the same Azure AD datacenter. It is not possible to continue a logical session if the directory client requests are being routed to multiple Azure AD datacenters; if this happens then the client has multiple logical sessions which have independent read-write consistencies.

NOTE

Writes are immediately replicated to the secondary replica to which the logical session's reads were issued.

Service-level backup

Azure AD implements daily backup of directory data and can use these backups to restore data in case of any service-wide issue.

The directory also implements soft deletes instead of hard deletes for selected object types. The tenant administrator can undo any accidental deletions of these objects within 30 days. For more information, see the [API to restore deleted objects](#).

Metrics and monitors

Running a high availability service requires world-class metrics and monitoring capabilities. Azure AD continually analyzes and reports key service health metrics and success criteria for each of its services. There is also continuous development and tuning of metrics and monitoring and alerting for each scenario, within each Azure AD service and across all services.

If any Azure AD service is not working as expected, action is immediately taken to restore functionality as quickly as possible. The most important metric Azure AD tracks is how quickly live site issues can be detected and mitigated for customers. We invest heavily in monitoring and alerts to minimize time to detect (TTD Target: <5 minutes) and operational readiness to minimize time to mitigate (TTM Target: <30 minutes).

Secure operations

Using operational controls such as multi-factor authentication (MFA) for any operation, as well as auditing of all operations. In addition, using a just-in-time elevation system to grant necessary temporary access for any operational task-on-demand on an ongoing basis. For more information, see [The Trusted Cloud](#).

Next steps

Five steps for integrating all your apps with Azure AD

4/10/2022 • 7 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) is the Microsoft cloud-based identity and access management service. Azure AD provides secure authentication and authorization solutions so that customers, partners, and employees can access the applications they need. With Azure AD, [conditional access](#), [multi-factor authentication](#), [single-sign on](#), and [automatic user provisioning](#) make identity and access management easy and secure.

If your company has a Microsoft 365 subscription, you likely [already use](#) Azure AD. However, Azure AD can be used for all your applications, and by [centralizing your application management](#) you can use the same identity management features, tools, and policies across your entire app portfolio. Doing so will provide a unified solution that improves security, reduces costs, increases productivity, and enables you to ensure compliance. And you will get remote access to on-premises apps.

This guide explains how to integrate all your applications with Azure AD. In each step, we explain the value and provide links to resources that will explain the technical details. We present these steps in an order we recommend. However, you can jump to any part of the process to get started with whatever adds the most value for you.

Other resources on this topic, including in-depth business process whitepapers, that can be found on our [Resources for migrating applications to Azure Active Directory](#) page.

1. Use Azure AD for new applications

First, focus on newly acquired applications. When your business starts using a new application, [add it to your Azure AD tenant](#) right away. Set up a company policy so that adding new apps to Azure AD is the standard practice in your organization. This is minimally disruptive to existing business processes and allows you to investigate and prove the value you get from integrating apps without changing the way that people do business in your environment today.

Azure Active Directory (Azure AD) has a gallery that contains thousands of pre-integrated applications to make it easy to get started. You can [add a gallery app to your Azure AD organization](#) with step-by-step [tutorials](#) for integrating with popular apps like:

- [ServiceNow](#)
- [Workday](#)
- [Salesforce](#)
- [AWS](#)
- [Slack](#)

In addition you can [integrate applications not in the gallery](#), including any application that already exists in your organization, or any third-party application from a vendor who is not already part of the Azure AD gallery. You can also [add your app to the gallery](#) if it is not there.

Finally, you can also integrate the apps you develop in-house. This is covered in step five of this guide.

2. Determine existing application usage and prioritize work

Next, discover the applications employees are frequently using, and prioritize your work for integrating them with Azure AD.

You can start by using the Microsoft Defender for Cloud Apps [cloud discovery tools](#) to discover and manage "shadow" IT in your network (that is, apps not managed by the IT department). You can [use Microsoft Defender Advanced Threat Protection \(ATP\)](#) to simplify and extend the discovery process.

In addition, you can use the [AD FS application activity report](#) in the Azure portal to discover all the AD FS apps in your organization, the number of unique users that have signed in to them, and compatibility for integrating them with Azure AD.

Once you have discovered your existing landscape, you will want to [create a plan](#) and prioritize the highest priority apps to integrate. Some example questions you can ask to guide this process are:

- Which apps are the most used?
- Which are the riskiest?
- Which apps will be decommissioned in the future, making a move unnecessary?
- Which apps need to stay on-premises and cannot be moved to the cloud?

You will see the largest benefits and cost savings once all your apps are integrated and you no longer rely on multiple identity solutions. However, you will experience easier identity management and increased security as you move stepwise towards this goal. You want to use this time to prioritize your work and decide what makes sense for your situation.

3. Integrate apps that rely on other identity providers

During your discovery process, you may have found applications that are untracked by the IT department, which leave your data and resources vulnerable. You may also have applications that use alternative identity solutions, including Active Directory Federation Services (ADFS) or other identity providers. Consider how you can consolidate your identity and access management to save money and increase security. Reducing the number of identity solutions you have will:

- Save you money by eliminating the need for on-premises user provisioning and authentication as well as licensing fees paid to other cloud identity providers for the same service.
- Reduce the administrative overhead and enable tighter security with fewer redundancies in your identity and access management process.
- Enable employees to get secure single sign-on access to ALL the applications they need via the [MyApps portal](#).
- Improve the intelligence of Azure AD's [identity protection](#) related services like conditional access by increasing the amount of data it gets from your app usage, and extend its benefits to the newly added apps.

We have published guidance for managing the business process of integrating apps with Azure AD, including a [poster](#) and [presentation](#) you can use to make business and application owners aware and interested. You can modify those samples with your own branding and publish them to your organization through your company portal, newsletter, or other medium as you go about completing this process.

A good place to start is by evaluating your use of Active Directory Federation Services (ADFS). Many organizations use ADFS for authentication with SaaS apps, custom Line-of-Business apps, and Microsoft 365 and Azure AD-based apps:



You can upgrade this configuration by [replacing ADFS with Azure AD as the center](#) of your identity management solution. Doing so enables sign-on for every app your employees want to access, and makes it easy for employees to find any business application they need via the [MyApps portal](#), in addition to the other benefits mentioned above.

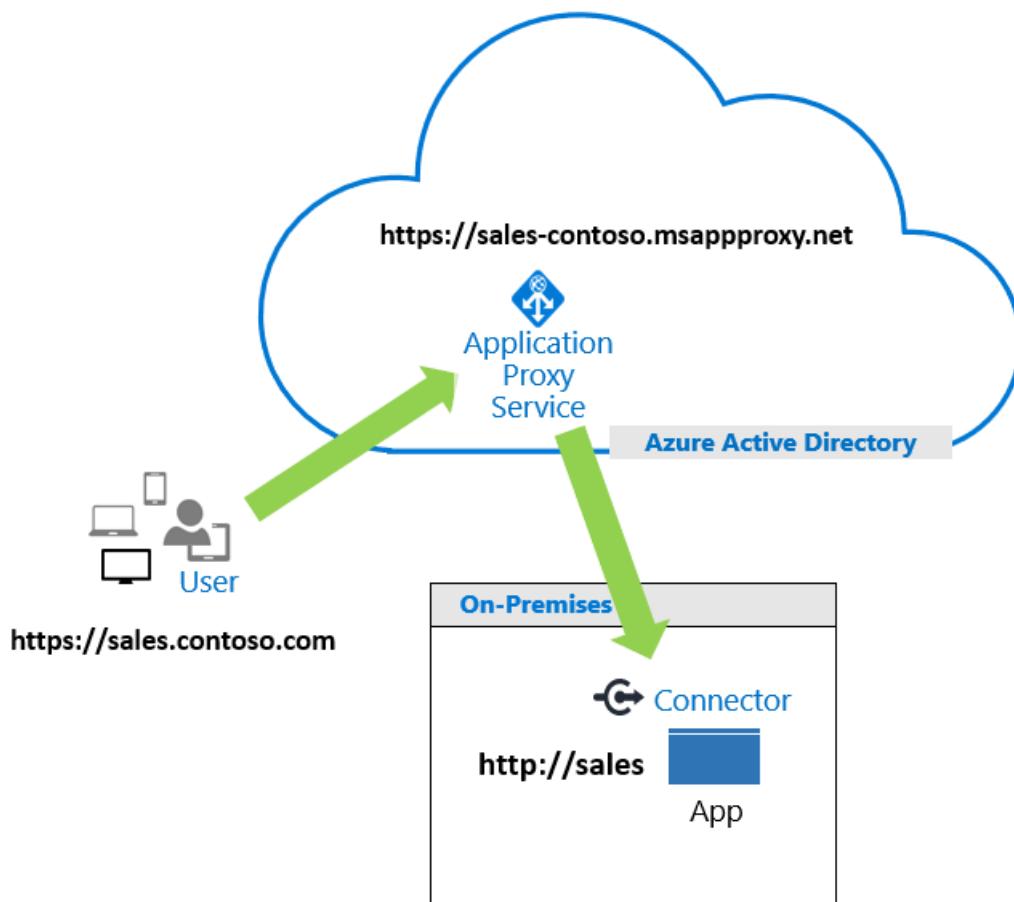


Once Azure AD becomes the central identity provider, you may be able to switch from ADFS completely, rather than using a federated solution. Apps that previously used ADFS for authentication can now use Azure AD alone.

You can also migrate apps that use a different cloud-based identity provider to Azure AD. Your organization may have multiple Identity Access Management (IAM) solutions in place. Migrating to one Azure AD infrastructure is an opportunity to reduce dependencies on IAM licenses (on-premises or in the cloud) and infrastructure costs. In cases where you may have already paid for Azure AD via M365 licenses, there is no reason to pay the added cost of another IAM solution.

4. Integrate on-premises applications

Traditionally, applications were kept secure by allowing access only while connected to the corporate network. However, in an increasingly connected world we want to allow access to apps for customers, partners, and/or employees, regardless of where they are in the world. [Azure AD Application Proxy](#) (AppProxy) is a feature of Azure AD that connects your existing on-premises apps to Azure AD and does not require that you maintain edge servers or other additional infrastructure to do so.



You can use [Tutorial: Add an on-premises application for remote access through Application Proxy in Azure Active Directory](#) to enable Application Proxy and add an on-premises application to your Azure AD tenant.

In addition, you can integrate application delivery controllers like F5 BIG-IP APM or Zscaler Private Access. By integrating these with Azure AD, you get the modern authentication and identity management of Azure AD alongside the traffic management and security features of the partner product. We call this solution [Secure Hybrid Access](#). If you use any of the following services today, we have tutorials that will step you through how to integrate them with Azure AD.

- [Akamai Enterprise Application Access \(EAA\)](#)

- [Citrix Application Deliver Controller \(ADC\)](#) (Formerly known as Citrix Netscaler)
- [F5 BIG-IP APM](#)
- [Zscaler Private Access \(ZPA\)](#)

5. Integrate apps your developers build

For apps that are built within your company, your developers can use the [Microsoft identity platform](#) to implement authentication and authorization. Applications integrated with the platform will be [registered with Azure AD](#) and managed just like any other app in your portfolio.

Developers can use the platform for both internal-use apps and customer facing apps, and there are other benefits that come with using the platform. [Microsoft Authentication Libraries \(MSAL\)](#), which is part of the platform, allows developers to enable modern experiences like multi-factor authentication and the use of security keys to access their apps without needing to implement it themselves. Additionally, apps integrated with the Microsoft identity platform can access [Microsoft Graph](#) - a unified API endpoint providing the Microsoft 365 data that describes the patterns of productivity, identity, and security in an organization. Developers can use this information to implement features that increase productivity for your users. For example, by identifying the people the user has been interacting with recently and surfacing them in the app's UI.

We have a [video series](#) that provides a comprehensive introduction to the platform as well as [many code samples](#) in supported languages and platforms.

Next steps

- [Resources for migrating applications to Azure Active Directory](#)

Parallel and combined identity infrastructure options

4/10/2022 • 15 minutes to read • [Edit Online](#)

Microsoft delivers a range of technologies and solutions to integrate between their different on-premises and cloud components of their identity infrastructure. Often customers are unclear on which technologies are most right and may incorrectly think "the most recent release covers all scenarios of earlier technology releases."

This article covers scenarios when your company is going through a complex scenario outlined below and looking to combine your identity information. Ideally, an organization with a single HR source, a single Active Directory forest, and a single Azure Active Directory (Azure AD) tenant, all integrated with the same people in each, will have the best identity experience for their Microsoft Online Services. However, in practice an enterprise customer may not always be in a situation where that is possible. For example, the customer may be going through a merger, or have a need for isolation for some users or applications. A customer who has multiple HR, multiple AD, or multiple Azure AD tenants must decide on whether to combine to fewer instances of each or keep them in parallel.

Based on our customer feedback, the following are some of the common scenarios and requirements.

Scenarios that come up for multi-cloud and multi-org identities

- Mergers and acquisitions (M&A) – refers to a situation where, usually Company A buys Company B.
- Rebranding – A company name or brand change and typically an e-mail domain name change.
- Azure AD or Office 365 tenant consolidation - Companies with more than one Office 365 tenant may want to combine because of compliance or historic requirements.
- Active Directory Domain or forest consolidation - Companies evaluating to perform Active Directory domain or forest consolidation.
- Divestitures – Where a division or business group of a company is sold or becomes independent.
- User information privacy – Where companies have requirements to keep certain data (attributes) from not being publicly visible and only right delegated groups or users can read, change, and update it.

Requirements that stem out from these scenarios

- Bring all users' and groups' data to a single place, including email and status availability for meeting scheduling by creating a central or **universal directory**.
- Maintain a **single username and credentials** while reducing the need to enter usernames and passwords across all applications by implementing Single Sign On.
- Streamline user on-boarding so it doesn't take weeks or months.
- Prepare the organization for future acquisitions and access management demands.
- Enable and improve cross-company collaboration and productivity.
- Reduce the likelihood of a security breach or data exfiltration with security policies deployed centrally and consistently!

Scenarios not covered in this article

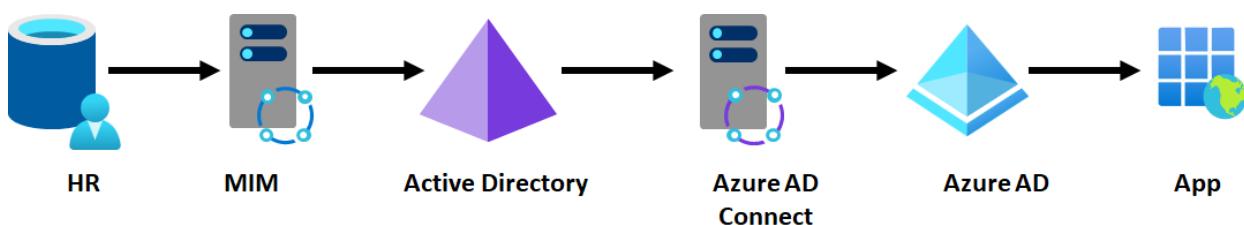
- Partial M&A. For example, an organization buys part of another organization.
- Divestiture or splitting organizations
- Renaming organizations.
- Joint ventures or temporary partners

This article outlines various multi-cloud or multi-org identity environments including M&A scenarios that Microsoft supports today and outline how an organization might select the right technologies depending upon how they approach consolidation.

Consolidation options for a hypothetical M&A scenario

The following sections cover four main scenarios for a hypothetical M&A scenario:

Suppose Contoso is an enterprise customer, and their IT has a single (on-premises) HR system, single Active Directory forest, single tenant Azure AD for their apps, running as expected. Users are brought in from their HR system into Active Directory and projected into Azure AD and from there into SaaS apps. This scenario is illustrated with the diagram below, with the arrows showing the flow of identity information. The same model is also applicable to customers with cloud HR system such as Workday or SuccessFactors provisioning Active Directory, not just customers using Microsoft Identity Manager (MIM).



Next, Contoso has begun to merge with Litware, which has previously been running their own IT independently. Contoso IT will handle the merger and expects that Contoso's IT will continue to have Contoso's apps remain unchanged, but they want to be able to have Litware's users receive access to them and collaborate within those apps. For Microsoft apps, third-party SaaS, and custom apps, the end state should be that Contoso and Litware users conceptually have access to the same data.

The first IT decision is how much they wish to combine infrastructure. They could choose to not rely upon any of Litware's identity infrastructure. Or they could consider using Litware's infrastructure and converging over time while minimizing disruption to Litware's environment. In some cases, the customer may wish to keep Litware's existing identity infrastructure independent and not converging it, while still using it to give Litware employee access to Contoso apps.

If the customer chooses to keep some or all Litware's identity infrastructure, then there are tradeoffs on how much of Litware's Active Directory Domain Services or Azure AD are used to give Litware users access to Contoso resources. This section looks at workable options, based on what Contoso would use for Litware's users:

- Scenario A - Don't use *any* of Litware's identity infrastructure.
- Scenario B - Use Litware's Active Directory forests, but not Litware's Azure AD (if they've one)
- Scenario C - Use Litware's Azure AD.
- Scenario D - Use Litware's non-Microsoft identity infrastructure (if Litware isn't using Active Directory/Azure AD)

The following table summarizes each option with the technologies for how the customer could achieve those outcomes, the constraints, and benefits of each.

			B3: ACTIVE DIRECT ORY FOREST TRUST, SINGLE AZURE AD CONNE CT	B4: AZURE AD CONNE CT THEIR ACTIVE DIRECT ORY TO THE SINGLE TENANT	B5: AZURE AD CONNE CT CLOUD SYNC THEIR ACTIVE DIRECT ORY	C6: PARALL EL PROVISI ON MULTIP LE TENANT S INTO APPS	C7: READ FROM THEIR TENANT AND INVITE THEIR USERS	C8: SINGLE IAM AND B2B USERS AS NEEDED	D9: DF WITH THEIR NON- AZURE AD IDP	
CONSIDERATIONS	A1: SINGLE HR, SINGLE IAM, AND TENANT	A2: SEPARATE HR, SINGLE IAM, AND TENANT								
Migration effort	High	Medium effort	Lower effort	Low effort	Low effort	None	None	None	None	
Deployment effort	Less effort	Medium effort	Medium effort	Medium effort	Low	Low	High	High	Very High	
End-user impact during migration	High	High	Medium	Medium	Medium	None	None	None	None	
Operating effort	Low cost	Low cost	Low cost	Low cost	Low cost	High	High	High	Very High	
Privacy and data capabilities (geo location /data boundaries)	None (Major roadblock for geo-location scenarios)	Limited isolation even though challenging	Limited isolation on-prem but not on the cloud	Limited isolation on-prem but not on the cloud	Limited isolation both on-prem and on the cloud	Good isolation both on-prem and on the cloud	Limited isolation both on-prem and cloud	Limited isolation both on-prem and cloud	Isolation both on-prem and on the cloud	
Isolation (separate delegation and setup different admin models) Note: as defined in source system (HR)	Not possible	Possible	Possible	Possible	Possible	Highly Possible	Highly possible	Highly possible	Possible	
Collaboration capabilities	Excellent	Excellent	Excellent	Excellent	Excellent	Poor	Average	Average	Poor	

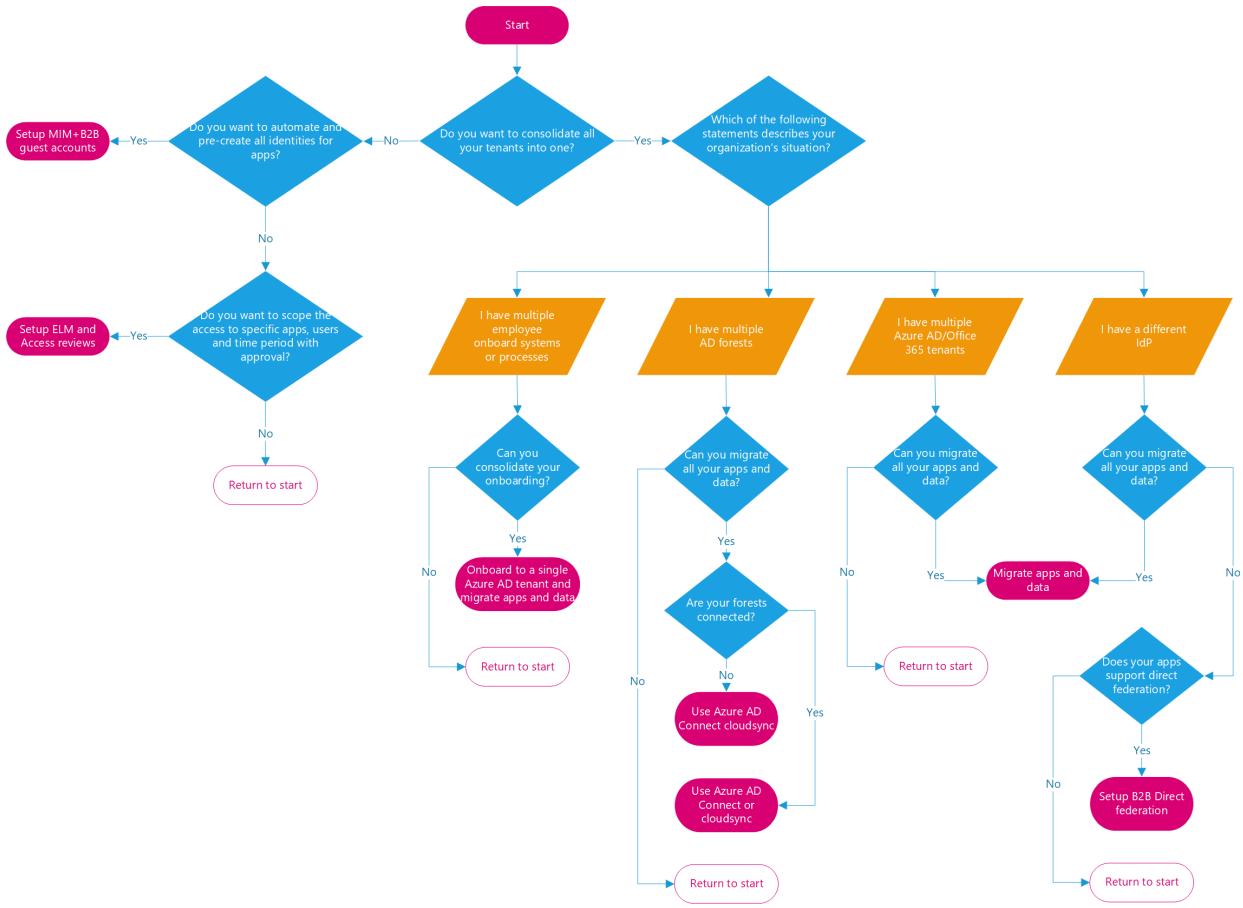
CONSIDERATIONS	A1: SINGLE HR, SINGLE IAM, AND TENANT	A2: SEPARATE HR, SINGLE IAM, AND TENANT	B3: ACTIVE DIRECTORY FOREST TRUST, SINGLE AZURE AD CONNECTION	B4: AZURE AD CONNECTION THEIR ACTIVE DIRECTORY TO THE SINGLE TENANT	B5: AZURE AD CONNECTION CLOUD SYNC THEIR ACTIVE DIRECTORY	C6: PARALLEL PROVISION MULTIPLE TENANTS INTO APPS	C7: READ FROM THEIR TENANT AND B2B INVITE THEIR USERS	C8: SINGLE IAM AND B2B USERS AS NEEDED	D9: DF WITH THEIR NON-AZURE AD IDP
IT admin model supported (centralized vs. separate d)	Centralized	Centralized	Centralized	Centralized	Centralized	Decentralized	Decentralized	Decentralized	Actively Decentralized
Limitations	No isolation	Limited isolation	Limited isolation	Limited isolation	Limited isolation . No writeback capabilities	Won't work for Microsoft Online Services apps. Highly dependent on app capability	Requires apps to be B2B aware	Requires apps to be B2B aware	Requires apps to be B2B aware. Uncertainty in how it all works together

Table details

- The employee effort tries to predict the required expertise and extra work required to implement the solution in an organization.
- Operating effort tries to predict the cost and effort it takes to keep the solution running.
- Privacy and data capabilities show if the solution allows support for geo location and data boundaries.
- Isolation shows if this solution supplies the ability to separate or delegate admin models.
- Collaboration capabilities show the level of collaboration the solution supports, more integrated solutions supply higher fidelity of teamwork.
- The IT admin model shows if the admin model requires to centralized or can be decentralized.
- Limitations: any issues of challenges worth listing.

Decision tree

Use the following decision tree to help you decide which scenario would work best for your organization.



The rest of this document will outline four scenarios A-D with various options supporting them.

Scenario A - If Contoso does not wish to rely upon Litware's existing identity infrastructure

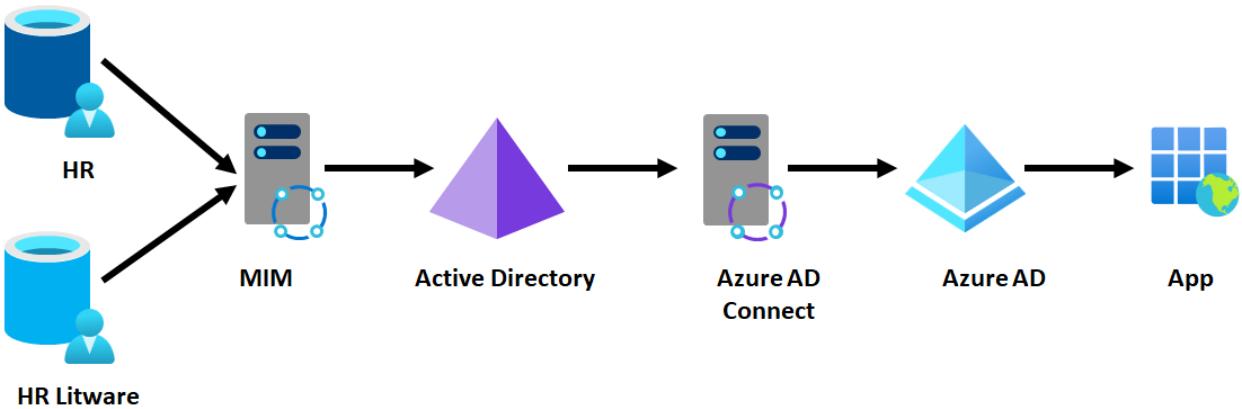
For this option, Litware may not have any identity systems (for example, a small business), or the customer may wish to turn off Litware's infrastructure. Or they wish to leave it untouched, for use by Litware employees to authenticate to Litware's apps but give Litware employees new identities as part of Contoso. For example, if Alice Smith was a Litware employee, she might have two identities – Alice@litware.com and ASmith123@contoso.com. Those identities would be entirely distinct from each other.

Option 1 - Combine into a single HR system

Typically, customers would bring the Litware employees into the Contoso HR system. This option would trigger those employees to receive accounts and the right access to Contoso's directories and apps. A Litware user would then have a new Contoso identity, which they could use to request access to the right Contoso apps.

Option 2 - Keep Litware HR system

Sometimes converging the HR systems may not be possible, at least not in the short term. Instead, the customer would connect their provisioning system, for example, MIM, to read from *both* HR systems. In this diagram, the top HR is the existing Contoso environment, and the second HR is Litware's addition to the overall infrastructure.



The same scenario would also be possible using Azure AD Workday or SuccessFactors inbound – Contoso could bring in users from Litware's Workday HR source alongside existing Contoso employees.

Outcomes of consolidating all identity infrastructure

- Reduced IT infrastructure, only one identity system to manage, no network connectivity requirements except for an HR system.
- Consistent end user and administrative experience

Constraints of consolidating all identity infrastructure

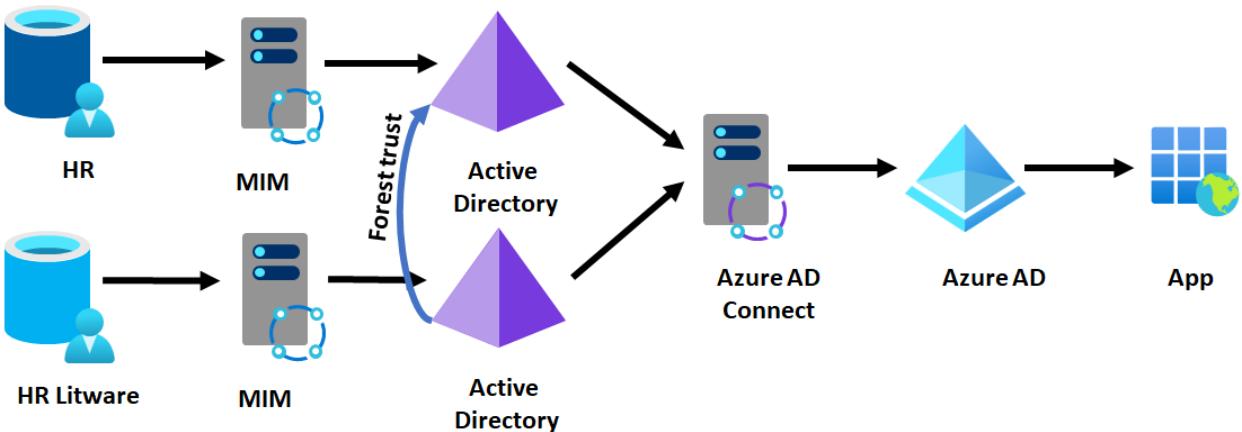
- Any data that is needed by Contoso employees that originated in Litware must be migrated to the Contoso environment.
- Any Active Directory or Azure AD-integrated apps from Litware that will be needed for Contoso must be reconfigured to the Contoso environment. This reconfiguration may require changes to the configuration, which groups it uses for access, or potentially to the apps themselves.

Scenario B - If Contoso wishes to keep Litware's Active Directory forests, but not use Litware's Azure AD

Litware may have many existing Active Directory-based apps that they rely on, and so Contoso may wish to continue to have Litware employees keep their own identities in their existing AD. A Litware employee would then use their existing identity for their authentication of their existing resources and authentication of Contoso resources. In this scenario, Litware doesn't have any cloud identities in Microsoft Online Services – either Litware wasn't an Azure AD customer, nothing of Litware's cloud assets were to be shared with Contoso, or Contoso migrated Litware's cloud assets to be part of Contoso's tenant.

Option 3 - Forest trust with the acquired forest

Using an [Active Directory forest trust](#), Contoso and Litware can connect their Active Directory domains. This trust enables Litware users to authenticate Contoso's Active Directory-integrated apps. Also [Azure AD Connect](#) can also read from Litware's Active Directory forest so that Litware users authenticate with Contoso's Azure AD integrated apps. This deployment topology requires a network route set up between the two domains, and TCP/IP network connectivity between any Litware user and Contoso Active Directory-integrated app. It's also straightforward to set up bidirectional trusts, so that Contoso users can access Litware AD-integrated apps (if any).



Outcome of setting up a forest trust

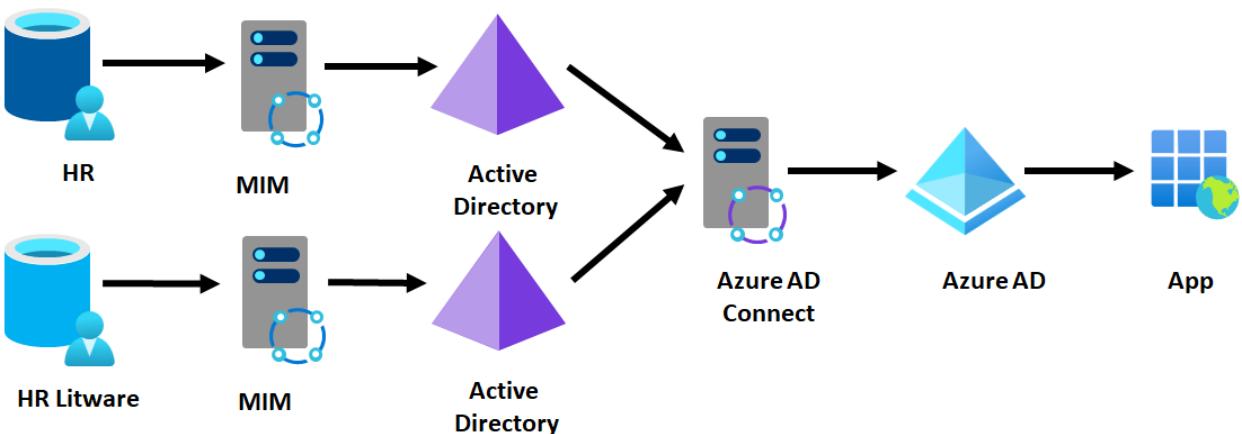
- All Litware employees can authenticate Contoso's Active Directory or Azure AD-integrated apps, and Contoso can use current AD-based tools to manage authorization.

Constraints of setting up a forest trust

- Requires TCP/IP connectivity between users who are domain joined to one forest and resources joined to the other forest.
- Requires the Active Directory-based apps in the Contoso forest to be multi-forest-aware

Option 4 - Configure Azure AD Connect to the acquired forest without forest trust

A customer can also configure Azure AD Connect to read from another forest. This configuration enables the Litware users to authenticate to Contoso's Azure AD integrated apps but doesn't supply access to Contoso's Active Directory integrated apps to the Litware user – those Contoso apps don't recognize Litware users. This deployment topology requires TCP/IP network connectivity between Azure AD Connect and Litware's domain controllers. For example, if Azure AD Connect is on a Contoso IaaS VM, they would need to establish a tunnel also to Litware's network as well.



Outcome of using Azure AD Connect to provision one tenant

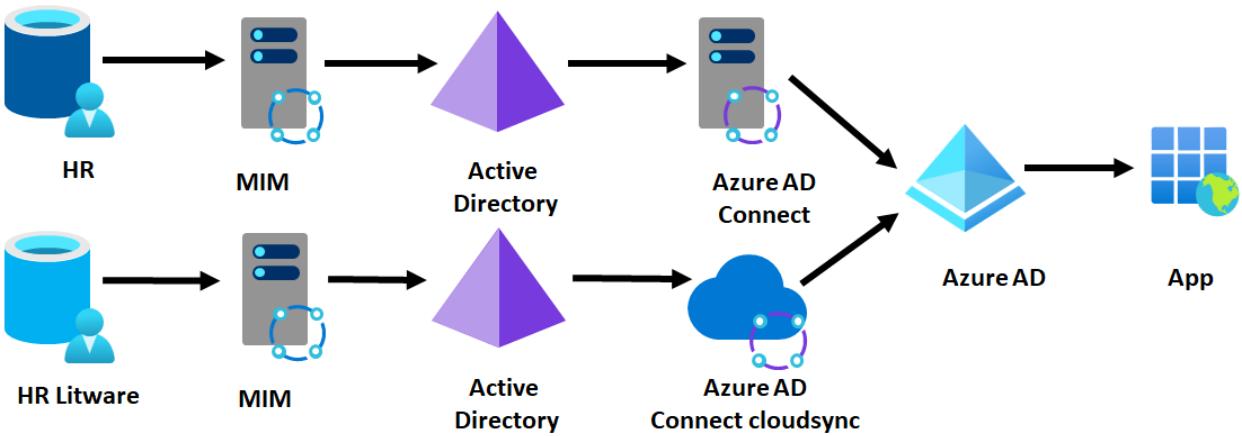
- All Litware employees can authenticate Contoso's Azure AD integrated apps.

Constraints of using Azure AD Connect to provision one tenant

- Requires TCP/IP connectivity between Contoso's Azure AD Connect and Litware's Active Directory domains.
- Doesn't permit Litware users to have access to Contoso's Active Directory based applications

Option 5 - Deploy Azure AD Connect cloud sync in the acquired forest

[Azure AD Connect cloud provisioning](#) removes the network connectivity requirement, but you can only have one Active Directory to Azure AD linking for a given user with cloud sync. Litware users can authenticate Contoso's Azure AD integrated apps, but not Contoso's Active Directory-integrated apps. This topology does not require any TCP/IP connectivity between Litware and Contoso's on-premises environments.



Outcome of deploying Azure AD Connect cloud sync in the acquired forest

- All Litware employees can authenticate Contoso's Azure AD-integrated apps.

Constraints of using Azure AD Connect cloud sync in the acquired forest

- Doesn't permit Litware users to have access to Contoso's AD-based applications

Scenario C - If Contoso wants to keep Litware's Azure AD

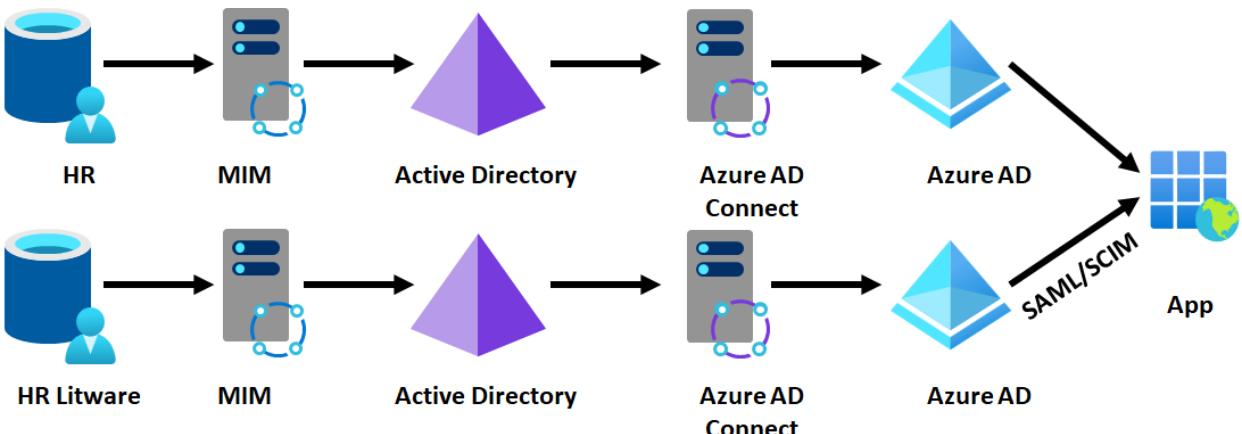
Litware may be a Microsoft Online Services or Azure customer or may have one or more Azure AD-based apps that they rely on. So, Contoso may want to continue to have Litware employees keep their own identities for access to those resources. A Litware employee would then use their existing identity for their authentication of their existing resources and authentication of Contoso resources.

This scenario is suitable in cases where:

- Litware has an extensive Azure or Microsoft Online Services investment including multiple Office 365 tenants that would be costly or time consuming to migrate to another tenant.
- Litware may be spun out in future or is a partnership that will run independently.
- Litware doesn't have on-premises infrastructure

Option 6 - Maintain parallel provisioning and SSO for apps in each Azure AD

One option is for each Azure AD to independently provide SSO and provision users from their directory into the target app. For example, if Contoso IT are using an app such as Salesforce, they would provide Litware with administrative rights to create users in the same Salesforce subscription.



Outcome of parallel provisioning

- Users can authenticate apps using their existing identity, without making changes to Contoso's infrastructure.

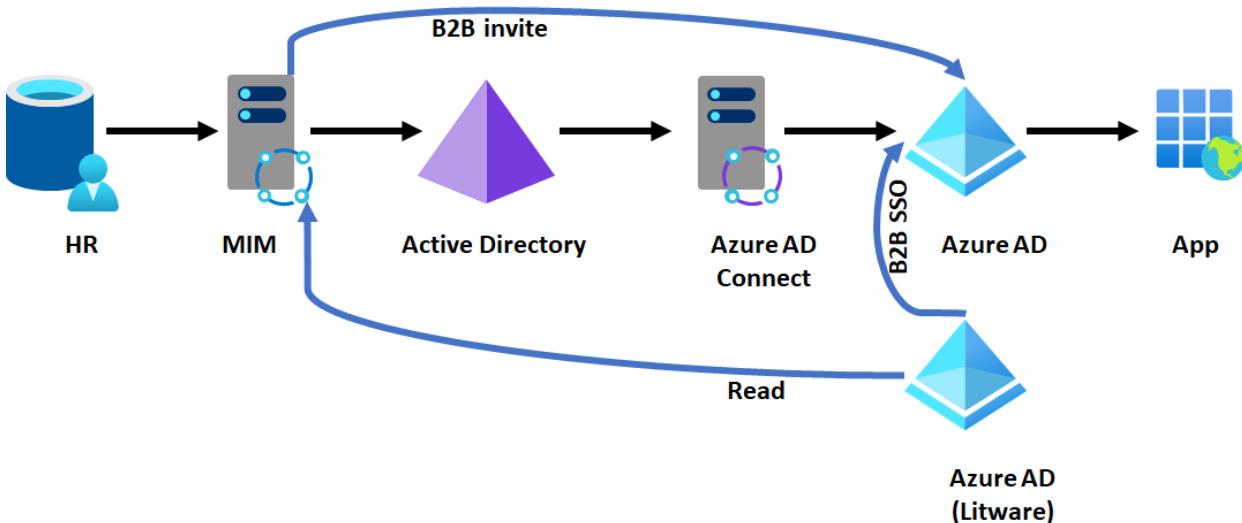
Constraints of parallel provisioning

- If using federation, it requires applications to support multiple federation providers for the same subscription.
- Not possible for Microsoft apps such as Office or Azure
- Contoso doesn't have visibility in their Azure AD of application access for Litware users

Option 7 - Configure B2B accounts for users from the acquired tenant

If Litware has been running its own tenant, then Contoso can read the users from that tenant, and through the B2B API, invite each of those users into the Contoso tenant. (This bulk invite process can be done through the [MIM graph connector](#), for example.) If Contoso also has AD-based apps that they wish to make available to Litware users, then MIM could also create users in Active Directory that would map to the UPNs of Azure AD users, so that the app proxy could perform KCD on behalf of a representation of a Litware user in Contoso's Active Directory.

Then when a Litware employee wishes to access a Contoso app, they can do so by authenticating to their own directory, with access assignment to the resource tenant.



Outcome of setting up B2B accounts for the other tenant

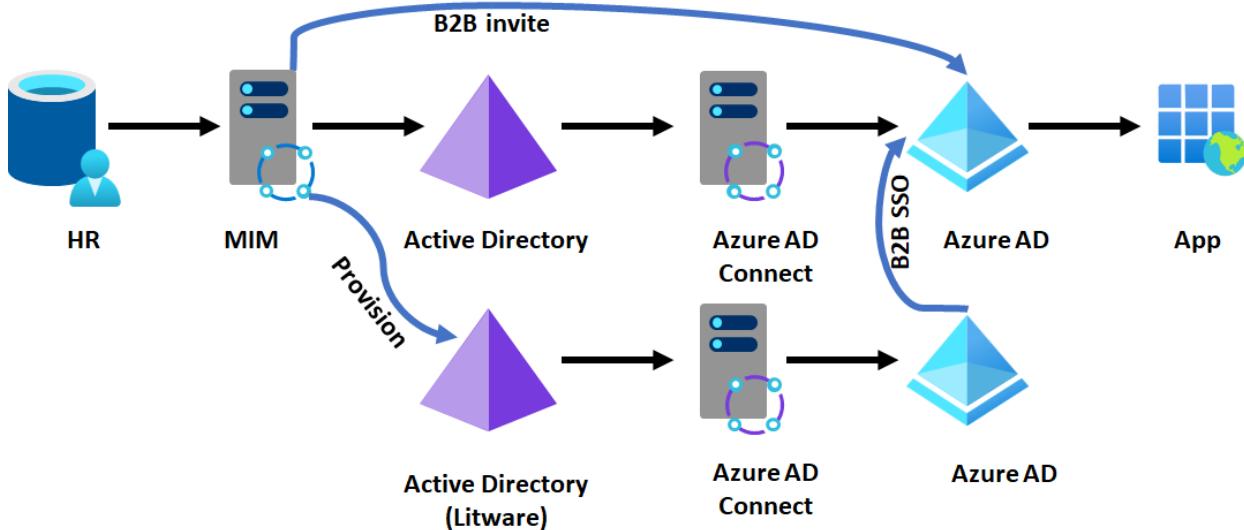
- Litware users can authenticate Contoso apps, and Contoso controls that access in their tenant.

Constraints of setting up B2B accounts for users from the other tenant

- It requires a duplicate account for each Litware user who requires access to Contoso resources.
- Requires the apps to be B2B capable for SSO.

Option 8 - Configure B2B but with a common HR feed for both directories

In some situations, after acquisition the organization may converge on a single HR platform, but still run existing identity management systems. In this scenario, MIM could provision users into multiple Active Directory systems, depending on which part of the organization the user is affiliated with. They could continue to use B2B so that users authenticate their existing directory, and have a unified GAL.



Outcome of setting up B2B guest users from a common HR system feed

- Litware users can authenticate to Contoso apps, and Contoso control that access in their tenant.
- Litware and Contoso have a unified GAL.
- No change to Litware's Active Directory or Azure AD

Constraints of setting up B2B guest users from a common HR system feed

- Requires changes to Contoso's provisioning to also send users to Litware's Active Directory, and connectivity between Litware's domains and Contoso's domains.
- Requires the apps to be B2B capable for SSO.

Scenario D - If Litware is using non-Active Directory infrastructure

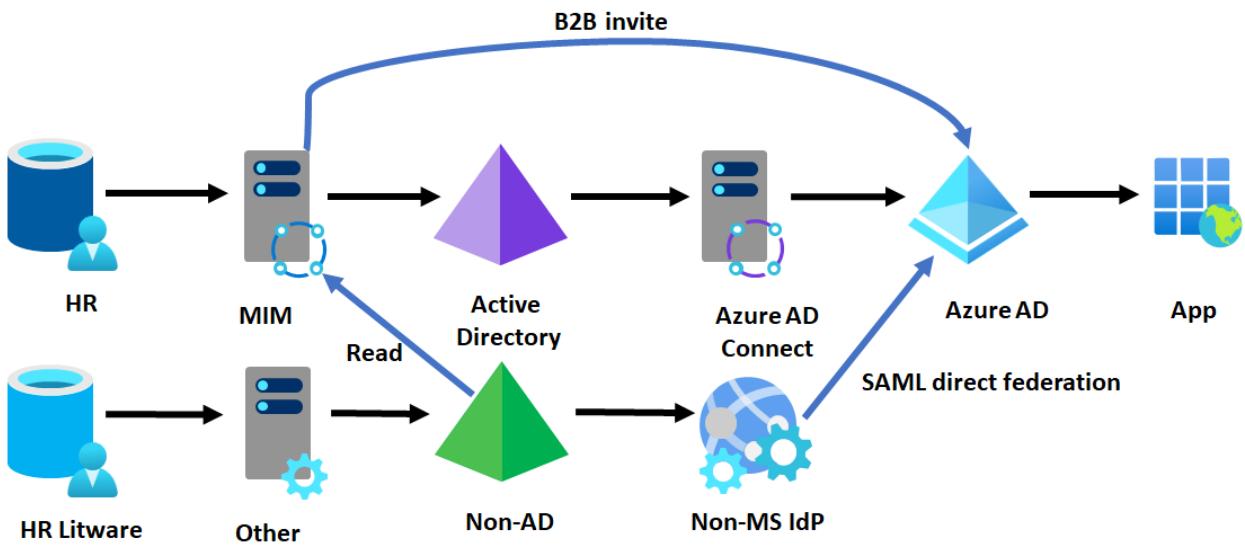
Finally, if Litware is using another directory service, either on-premises or in the cloud, then Contoso IT can still configure that Litware employees authenticate and can get access to Contoso's resources using their existing identity.

Option 9 - Use B2B direct federation (public preview)

In this scenario, Litware is assumed to have:

- Some existing directories, such as OpenLDAP or even a SQL database or flat file of users with their email addresses that they can regularly share with Contoso.
- An identity provider that supports SAML, such as PingFederate or OKTA.
- A publicly routed DNS domain such as Litware.com and users with email addresses in that domain

In this approach, Contoso would configure a [direct federation](#) relationship from their tenant for that domain to Litware's identity provider, and then regularly read updates to Litware users from their directory to invite the Litware users into Contoso's Azure AD. This update can be done with a MIM Graph connector. If Contoso also has Active Directory-based apps that they wish to make available to Litware users, then MIM could also create users in Active Directory that would map to the UPNs of Azure AD users, so that the app proxy could perform KCD on behalf of a representation of a Litware user in Contoso's Active Directory.



Outcome of using B2B direct federation

- Litware users authenticate to Contoso's Azure AD with their existing identity provider and access Contoso's cloud and on-premises web apps,

Constraints of using B2B direct federation

- Require the Contoso apps to be able to support B2B user SSO.

Next steps

- [What is Azure AD Connect cloud sync](#)
- [Setup Inbound provisioning for Azure AD](#)
- [Setup B2B direct federation](#)
- [Multi-tenant user management options](#)

Multi-tenant user management

4/10/2022 • 5 minutes to read • [Edit Online](#)

Provisioning users into a single Azure Active Directory (Azure AD) tenant provides a unified view of resources and a single set of policies and controls. This approach enables consistent user lifecycle management.

Microsoft recommends a single tenant when possible. However, immediate consolidation to a single Azure AD tenant isn't always possible. Multi-tenant organizations may span two or more Azure AD tenants. This can result in unique cross-tenant collaboration and management requirements.

Organizations may have identity and access management (IAM) requirements that are complicated by:

- mergers, acquisitions, and divestitures.
- collaboration across public, sovereign, and or regional clouds.
- political or organizational structures prohibiting consolidation to a single Azure AD tenant.

The guidance also provides guidance to help you achieve a consistent state of user lifecycle management. That is, provisioning, managing, and deprovisioning users across tenants using the tools available with Azure. Specifically, by using [Azure AD B2B collaboration](#).

Azure AD B2B collaboration

Azure AD collaboration enables you to securely share your company's applications and services with external guest users. The users can come from any organization. Using Azure AD B2B collaboration helps you maintain control over access to your IT environment and data. Azure AD B2B collaboration can also be used to provide guest access to internal users. Traditionally, B2B guest user access is used to authorize access to external users that aren't managed by your own organization. However, guest user access can also be used to manage access across multiple tenants managed by your organization. While not truly a B2B solution, Azure AD B2B collaboration can be used to manage internal users across your multi-tenant scenario.

The following links provide additional information you can visit to find out more about Azure AD B2B collaboration:

ARTICLE	DESCRIPTION
Conceptual articles	
B2B best practices	Recommendations for the smoothest experience for your users and administrators.
B2B and Office 365 external sharing	Explains the similarities and differences among sharing resources through B2B, office 365, and SharePoint/OneDrive.
Properties on an Azure AD B2B collaboration user	Describes the properties and states of the B2B guest user object in Azure Active Directory (Azure AD). The description provides details before and after invitation redemption.
B2B user tokens	Provides examples of the bearer tokens for B2B a B2B guest user.

ARTICLE	DESCRIPTION
Conditional access for B2B	Describes how conditional access and MFA work for guest users.
How-to articles	
Use PowerShell to bulk invite Azure AD B2B collaboration users	Learn how to use PowerShell to send bulk invitations to external users.
Enforce multifactor authentication for B2B guest users	Use conditional access and MFA policies to enforce tenant, app, or individual guest user authentication levels.
Email one-time passcode authentication	The Email one-time passcode feature authenticates B2B guest users when they can't be authenticated through other means like Azure AD, a Microsoft account (MSA), or Google federation.

Terminology

These terms are used throughout this content:

- **Resource tenant:** The Azure AD tenant containing the resources that users want to share with others.
- **Home tenant:** The Azure AD tenant containing users requiring access to the resources in the resource tenant.
- **User lifecycle management:** the process of provisioning, managing, and deprovisioning user access to resources.
- **Unified GAL:** Each user in each tenant can see users from each organization in their Global Address List (GAL).

Deciding how to meet your requirements

Your organization's unique requirements will determine your strategy for managing your users across tenants. To create an effective strategy, you must consider:

- Number of tenants
- Type of organization
- Current topologies
- Specific user synchronization needs

Common Requirements

Many organizations initially focus on requirements they want in place for immediate collaboration. Sometimes known as Day One requirements, these requirements focus on enabling end users to merge smoothly without interrupting their ability to generate value for the company. As you define your Day One and administrative requirements, consider including these goals:

REQUIREMENT CATEGORIES	COMMON NEEDS
Communications Requirements	

Requirement categories	Common needs
Unified global address list	Each user can see all other users in the GAL in their home tenant.
Free/Busy information	Enable users to discover each other's availability. You can do this with Organization relationships in Exchange Online .
Chat and presence	Enable users to determine others' presence and initiate instant messaging. This can be configured through external access in Microsoft Teams .
Book resources such as meeting rooms	Enable users to book conference rooms or other resources across the organization. Cross-tenant conference room booking isn't possible today.
Single email domain	Enable all users to send and receive mail from a single email domain, for example <i>users@contoso.com</i> . Sending requires a third party address rewrite solution today.
Access requirements	
Document access	Enable users to share documents from SharePoint, OneDrive, and Teams
Administration	Allow administrators to manage configuration of subscriptions and services deployed across multiple tenants
Application access	Allow end users to access applications across the organization
Single Sign-on	Enable users to access resources across the organization without the need to enter more credentials.

Patterns for account creation

There are several mechanisms available for creating and managing the lifecycle of your guest user accounts. Microsoft has distilled three common patterns. You can use the patterns to help define and implement your requirements. Choose which best aligns with your scenario and then focus on the details for that pattern.

Mechanism	Description	Best when
End-user-initiated	Resource tenant admins delegate the ability to invite guest users to the tenant, an app, or a resource to users within the resource tenant. Users from the home tenant are invited or sign up individually.	<ul style="list-style-type: none"> Users need improvised access to resources. No automatic synchronization of user attributes is necessary. Unified GAL is not needed.a
Scripted	Resource tenant administrators deploy a scripted "pull" process to automate discovery and provisioning of guest users to support sharing scenarios.	<ul style="list-style-type: none"> No more than two tenants. No automatic synchronization of user attributes is necessary. Users need pre-configured (not improvised) access to resources.

MECHANISM	DESCRIPTION	BEST WHEN
Automated	Resource tenant admins use an identity provisioning system to automate the provisioning and deprovisioning processes.	<ul style="list-style-type: none"> • Full identity lifecycle management with provisioning and deprovisioning must be automated. • Attribute syncing is required to populate the GAL details and support dynamic entitlement scenarios. • Users need pre-configured (not ad hoc) access to resources on "Day One".

Next steps

[Multi-tenant user management scenarios](#)

[Multi-tenant common considerations](#)

[Multi-tenant common solutions](#)

[Multi-tenant synchronization from Active Directory](#)

Multi-tenant user management scenarios

4/10/2022 • 11 minutes to read • [Edit Online](#)

End-user initiated scenario

For the end-user initiated scenario, resource tenant administrators delegate certain abilities to users in the tenant. Administrators enable end users to invite guest users to the tenant, an app, or a resource. Users from the home tenant are invited or sign up individually.

An example use case would be for a global professional services firm who works with subcontractors on a project. Subcontractor users require access to the firm's applications and documents. Admins at the firm can delegate to firm end users the ability to invite subcontractors or configure self-service for subcontractor resource access.

Provision accounts

There are many ways end users can get invited to access resource tenant resources. Here are five of the most widely used:

- [Application-based invitations](#). Microsoft applications may enable invitation of guest users. B2B invitation settings must be configured both in Azure AD B2B and in the relevant application or applications.
- [MyApps](#). Users invite and assign a guest user to an application using MyApps. The user account must have [application self-service sign up](#) approver permissions. They can invite guest users to a group if they're a group owner.
- [Entitlement Management](#): Enables admins or resource owners to tie resources, allowed external organizations, guest user expiration, and access policies together in access packages. Access packages can be published to enable self-service sign-up for resource access by guest users.
- [Azure portal](#) End users given the [Guest Inviter role](#) can sign in to the Azure portal and invite guest users from the Users menu in Azure Active Directory.
- [Programmatic \(PowerShell, Graph API\)](#) End users given the [Guest Inviter role](#) can invite guest users via PowerShell or Graph API.

Redeem invitations

As part of provisioning accounts to access a resource, email invitations are sent to the invited users email address. When an invited user receives an invitation, they can:

- Follow the link contained in the email to the redemption URL.
- Try to access the resource directly.

When the user tries to access the resource directly, it is named just-in-time (JIT) redemption. The following are the user experiences for each redemption method.

Redemption URL

By accessing the [redemption URL](#) in the email, the invited user can approve or deny the invitation (creating a guest user account if necessary).

Just-In-Time Redemption

The user can access the resource URL directly for just-in-time redemption if:

- The invited user already has an Azure AD or Microsoft account
-or-

- If [email one-time passcodes](#) is enabled

A few points during JIT redemption:

- If administrators have not suppressed accepting privacy terms, the user must accept the Privacy Terms agreement page before accessing the resource.
- PowerShell allows control over whether an email is sent when inviting [via PowerShell](#).
- You can allow or block invitations to guest users from specific organizations by using an [allowlist](#) or a [blocklist](#).

For more information, see [Azure Active Directory B2B collaboration invitation redemption](#).

Important – enable one-time passcode authentication

We strongly recommend enabling [email one time passcode authentication](#). This feature authenticates guest users when they can't be authenticated through other means, such as:

- Azure AD
- A Microsoft account (MSA)
- A Gmail account through Google federation
- An account from a SAML/WS-Fed IDP through Direct Federation

With one-time passcode authentication, there's no need to create a Microsoft account. When the guest user redeems an invitation or accesses a shared resource, they receive a temporary code. The code is sent to their email address and then they enter the code to continue signing in.

Without email one-time passcode authentication enabled, a Microsoft Account or a just-in-time "unmanaged" Azure AD tenant may be created.

Important: Microsoft is deprecating the creation of unmanaged tenants and their users as this feature becomes Generally Available (GA) in each cloud environment.

Manage accounts

The resource tenant administrator manages guest user accounts in the resource tenant. Guest users accounts aren't updated based on the updated values in the home tenant. In fact, the only visible attributes received include the email address and display name.

You can configure more attributes on guest user objects to facilitate scenarios. For example, you can include populating the address book with contact details, or in entitlement scenarios. For example, consider:

- HiddenFromAddressListsEnabled
- GivenName
- Surname
- Title
- Department
- TelephoneNumber

These attributes might be set to [add guests to the global address list](#). Other scenarios may require different attributes, such as for setting entitlements and permissions for Access Packages, Dynamic Group Membership, SAML Claims, etc.

Note: Invited guest users are hidden from the global address list (GAL) by default. Set guest user attributes to be

unhidden for them to be included in the unified GAL. For more information, see the [Microsoft Exchange Online documentation](#).

Deprovision accounts

End-user initiated scenarios decentralize access decisions. However, decentralizing access decisions creates the challenge of deciding when to remove a guest user and its associated access. [Entitlement Management](#) and [access reviews](#) provide a way to review and remove existing guest users and their access to resources.

Note: If users are invited outside of entitlement management, you must create a separate process to review and manage those guest users' access. For example, if the guest user is invited directly through SharePoint Online, it is not included in your entitlement management process.

Scripted scenario

For the scripted scenario, resource tenant administrators deploy a scripted pull process to automate discovery and provisioning of guest users. This approach is common for customers using a scripted mechanism.

An example use case would be a global shipping company that is acquired a competitor. Each company has a single Azure AD tenant. They want the following "day one" scenarios to work, without users having to perform any invitation or redemption steps. All users must be able to:

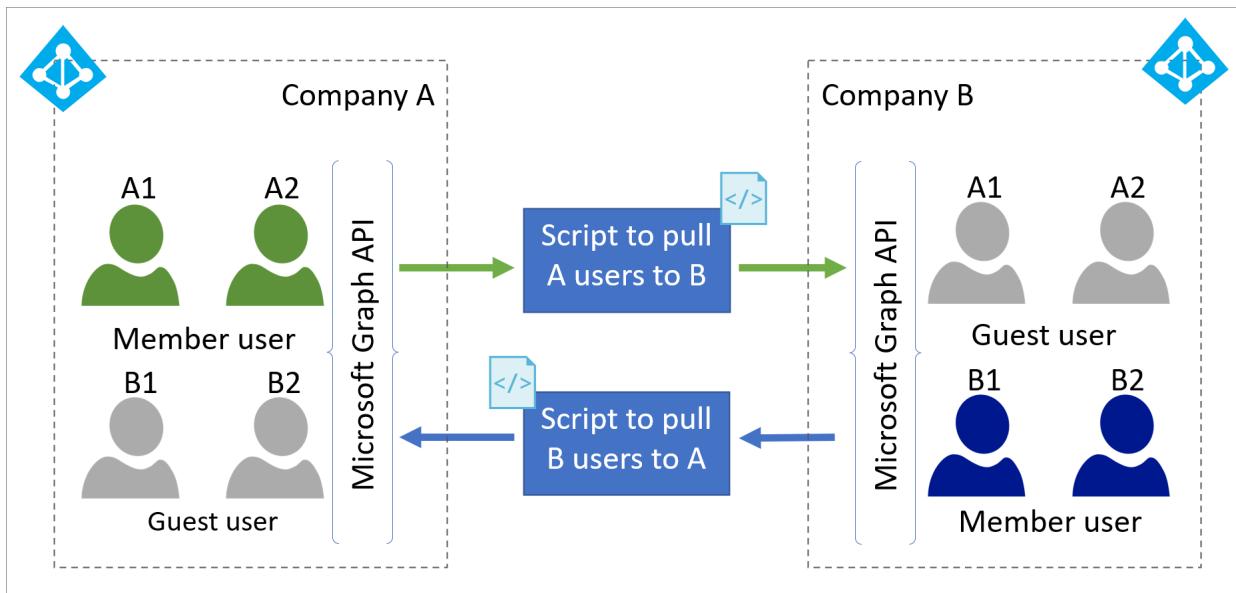
- Use single sign-on to all resources to which they are provisioned
- Find each other and also find other resources in a unified GAL
- Determine each other's presence and be able to initiate instant messages
- Access an application based on dynamic group membership

In this case, each organization's tenant is the home tenant for its existing employees, and the resource tenant for the other organization's employees.

Provision accounts

With [Delta Query](#), tenant admins can deploy a scripted pull process to automate discovery and provisioning of identities to support resource access. This process checks the home tenant for new users and uses the B2B Graph APIs to provision those users as invited users in the resource tenant. The following diagram shows the components.

Multi-tenant topology



- Administrators of each tenant pre-arrange credentials and consent to allow read of each tenant.

- Allows tenant administrators to automate enumeration and “pulling” scoped users to resource tenant.
- Use MS Graph API with consented permissions to read and provision users via the invitation API.
- Initial provisioning can read source attributes and apply them to the target user object.

Manage accounts

The resource organization may choose to augment profile data to support sharing scenarios by updating the user’s metadata attributes in the resource tenant. However, if ongoing synchronization is necessary, then a synchronized solution might be a better option.

Deprovision accounts

[Delta Query](#) can signal when a guest user needs to be deprovisioned. [Entitlement Management](#) and [access reviews](#) can also provide a way to review and remove existing guest users and their access to resources.

Note: If users are invited outside of entitlement management, you must create a separate process to review and manage those guest users’ access. For example, if the guest user is invited directly through SharePoint Online, it is not included in your entitlement management process.

Automated Scenario

By far, the most complex pattern is synchronized sharing across tenants. This pattern enables more automated management and deprovisioning scenarios than user-initiated or scripted. For automated scenarios, resource tenant admins use an identity provisioning system to automate the provisioning and deprovisioning processes.

An example use case would be a multinational conglomeration that has multiple subsidiaries. Each has their own Azure AD tenant, but need to work together. In addition to synchronizing new users among tenants, attribute updates must be automatically synchronized. Deprovisioning must be automated. For example, if an employee is no longer at a subsidiary, their account should be removed from all other tenants during the next synchronization.

Or, consider the following expanded scenario. A Defense Industrial Base (DIB) contractor has a defence-based and commercial-based subsidiary. These have competing regulation requirements:

- The US defense business resides in a US sovereign cloud tenant. For example, Microsoft 365 US Government GCC High.
- The commercial business resides in a separate Azure AD tenant in the public. For example, an Azure AD environment running on the global Azure cloud.

To act like a single company deployed into a “cross-sovereign cloud” architecture, all users are synchronized to both tenants. This enables a unified GAL available across both tenants. It may also ensure that users automatically synchronized to both tenants include entitlements and restrictions to applications and content. For example:

- US employees may have ubiquitous access to both tenants.
- Non-US employees show in the unified GAL of both tenants but does not have access to protected content in the GCC High tenant.

This will require automatic synchronization and identity management to configure users in both tenants while associating them with the proper entitlement and data protection policies.

Provision accounts

This advanced deployment uses [Microsoft Identity Manager](#) (MIM) as a synchronization engine. MIM calls the [MS Graph API](#) and [Exchange Online PowerShell](#). Alternative implementations can include the cloud hosted [Active Directory Synchronization Services](#) (ADSS) managed service offering from [Microsoft Consulting Services](#). There are also non-Microsoft offerings that can be created from scratch with other identity management

offerings.

These are complex scenarios and we recommend you work with your partners, Microsoft account team, and any other available resources throughout your planning and execution.

Note: There are considerations that are outside the scope of this document. For example, [integration of on-premises applications](#).

Choose the right topology

Most customers use one of two topologies in automated scenarios.

- A mesh topology enables sharing of all resources in all tenants. Users from other tenants are created in each resource tenant as guest users.
- A single resource tenant topology uses a single tenant (the resource tenant), in which users from other companies are external guest users.

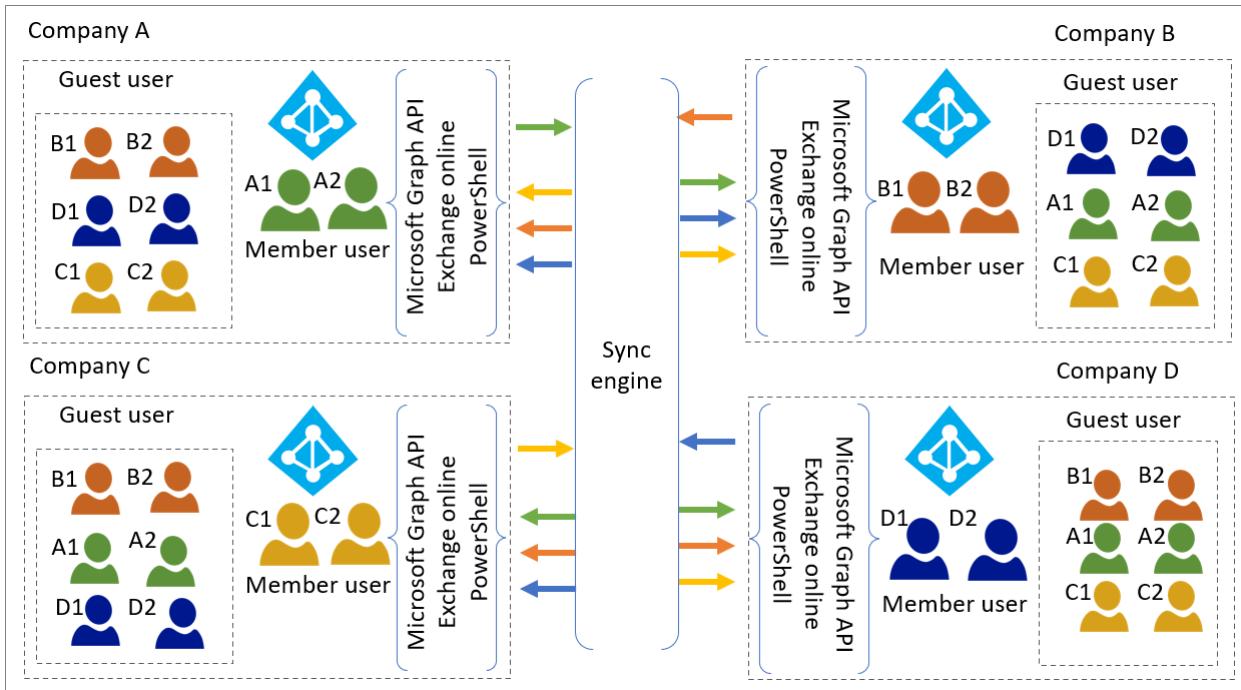
The following table can be used as a decision tree while you are designing your solution. We illustrate both topologies following the table. To help you determine which is right for your organization, consider the following.

Comparison of mesh versus single resource tenant topologies

CONSIDERATION	MESH TOPOLOGY	SINGLE RESOURCE TENANT
Each company has separate Azure AD tenant with users and resources	Yes	Yes
Resource location and collaboration		
Shared apps and other resources remain in their current home tenant	Yes	No - only resources in the resource tenant are shared.
All viewable in individual company's GALs (Unified GAL)	Yes	No
Resource access and administration		
ALL applications connected to Azure AD can be shared among all companies	Yes	No - only those in the resource tenant are shared. Those remaining in other tenants aren't.
Global resource administration	Continue at tenant level	Consolidated in the resource tenant
Licensing – Office 365 SharePoint Online, unified GAL, Teams access all support guests; however, other Exchange Online scenarios do not	Continues at tenant level	Continues at tenant level
Licensing – Azure AD (premium)	First 50 K Monthly Active Users are free (per tenant).	First 50 K Monthly Active Users are free.

CONSIDERATION	MESH TOPOLOGY	SINGLE RESOURCE TENANT
Licensing – SaaS apps	Remain in individual tenants, may require licenses per user per tenant	All shared resources reside in the single resource tenant. You can investigate consolidating licenses to the single tenant if appropriate.

Mesh topology



In a mesh topology, every user in each home tenant is synchronized to each of the other tenants, which become resource tenants.

- This enables any resource within a tenant to be shared with guest users.
- This enables each organization to see all users in the conglomerate. In the illustration above there are four unified GALs, each of which contains the home users and the guest users from the other three tenants.

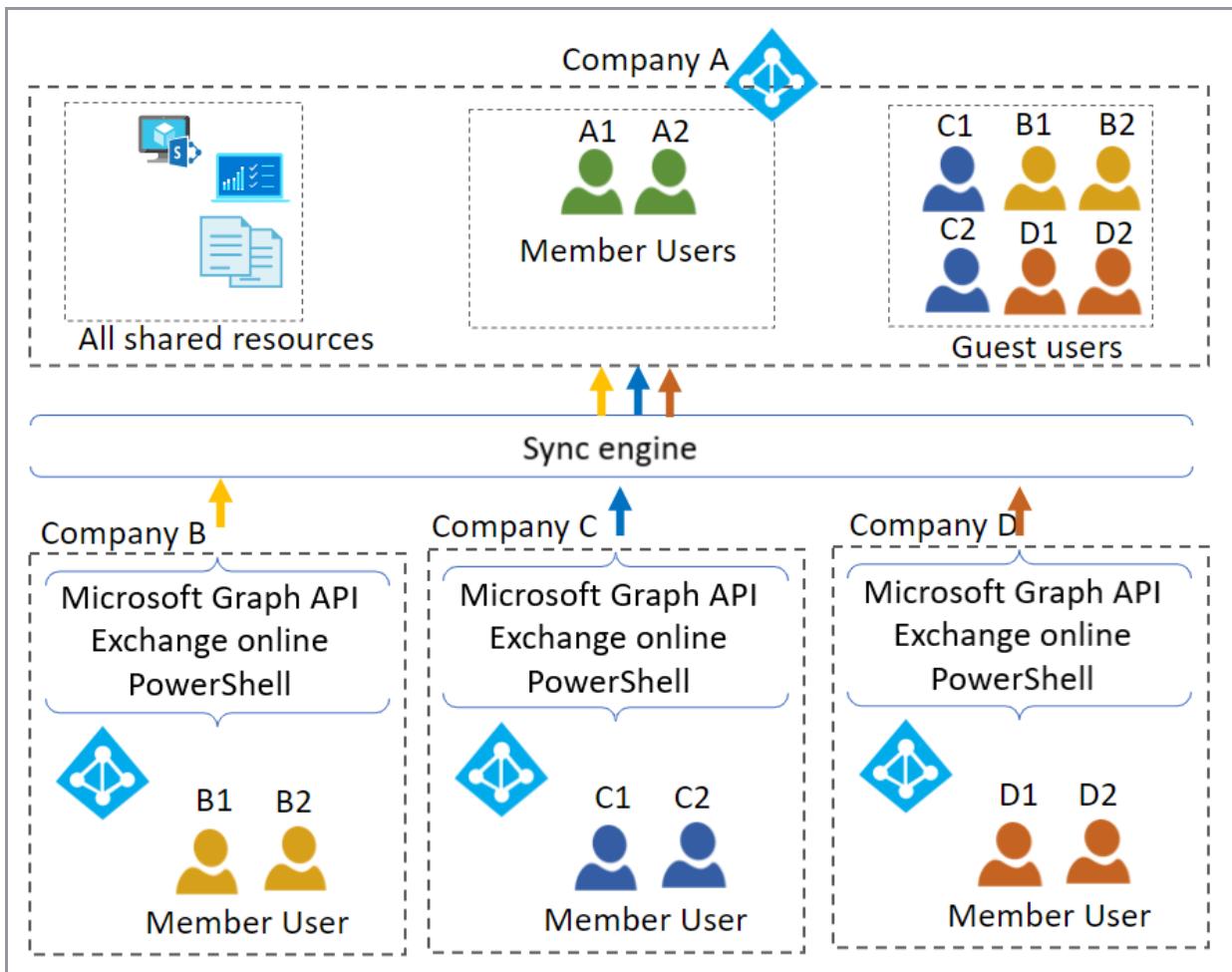
See the [common considerations](#) section of this document for additional information on provisioning, managing, and deprovisioning users in this scenario.

Mesh topology for cross-sovereign cloud

The mesh topology can be used in as few as two tenants, such as in the scenario for the DIB defense contractor straddling a cross-sovereign cloud solution. As with the mesh topology, every user in each home tenant is synchronized to the other tenant, that effectively becomes a resource tenant. In the illustration above, the public Commercial tenant member user is synchronized to the US sovereign GCC High tenant as a guest user account. At the same time, the GCC High member user is synchronized to Commercial as a guest user account.

Note: The illustration also describes where the data is stored. Data categorization and compliance is outside the scope of this whitepaper, but demonstrates that you can include entitlements and restrictions to applications and content. Content may include where a member user's 'personal data' resides. For example, data stored in their Exchange Online mailbox or OneDrive for Business. The content might only be in their home tenant, not in the resource tenant. Shared data might reside in either tenant. You can restrict access to the content through access control and conditional access policies.

Single resource tenant topology



In a single resource tenant topology, users and their attributes are synchronized to the resource tenant (Company A in the illustration above).

- All resources shared among the member organizations must reside in the single resource tenant.
 - If multiple subsidiaries have subscriptions to the same SaaS apps, this could be an opportunity to consolidate those subscriptions.
- Only the GAL in the resource tenant displays users from all companies.

Manage accounts

This solution detects and syncs attribute changes from source tenant users to resource tenant guest users. These attributes can be used to make authorization decisions. For example, when using dynamic groups.

Deprovision accounts

Automation detects deletion of the object in source environment and deletes the associated guest user object in the target environment.

See the [Common considerations](#) section of this document for additional information on provisioning, managing, and deprovisioning users in this scenario.

Next steps

[Multi-tenant user management introduction](#)

[Multi-tenant common considerations](#)

[Multi-tenant common solutions](#)

Common considerations for multi-tenant user management

4/10/2022 • 11 minutes to read • [Edit Online](#)

There are many considerations that are relevant to more than one collaboration pattern.

Directory object considerations

You can use the console to manually create an invitation for a guest user account. When you do, the user object is created with a user type of *Guest*. Using other techniques to create invitations enable you to set the user type to something other than a Guest account. For example, when using the API you can configure whether the account is a member account or a guest account.

- Some of the [limits on Guest functionality can be removed](#).
- [You can convert Guest accounts to a user type of Member](#).

IMPORTANT If you convert from a guest account to a user account, there might be issues with how Exchange Online handles B2B accounts. You can't mail-enable accounts invited as guest members. To get a guest member account mail-enabled, the best approach is to:

- Invite the cross-org users as guest accounts.
- Show the accounts in the GAL.
- Set the UserType to Member.

Using this approach, the accounts show up as MailUser in Exchange Online.

Issues with using mail-contact objects instead of external users or members

You can represent users from another tenant using a traditional GAL synchronization. If a GAL synchronization is done rather than using Azure AD B2B collaboration, a mail-contact object is created.

- A mail-contact object and a mail-enabled guest user (member or guest) can't coexist in the same tenant with the same email address at the same time.
- If a mail-contact object exists for the same mail address as the invited guest user, the guest user will be created but is NOT mail enabled.
- If the mail-enabled guest user exists with the same mail, an attempt to create a mail-contact object will throw an exception at creation time.

The following are the results of various mail-contact objects and guest user states.

EXISTING STATE	PROVISIONING SCENARIO	EFFECTIVE RESULT
None	Invite B2B Member	Non-mail enabled member user. See Important note above
None	Invite B2B Guest	Mail-enable guest user
Mail-contact object exists	Invite B2B Member	Error – Conflict of Proxy Addresses

EXISTING STATE	PROVISIONING SCENARIO	EFFECTIVE RESULT
Mail-contact object exists	Invite B2B Guest	Mail-contact and Non-Mail enabled guest user. See Important note above
Mail-enabled B2B Guest user	Create mail-contact object	Error
Mail-enabled B2B Member user exists	Create mail-contact	Error

Microsoft does not recommend traditional GAL synchronization. Instead, use Azure AD B2B collaboration to create:

- External guest users that you enable to show in the GAL
- Create external member users, which show in the GAL by default, but aren't mail-enabled.

Some organizations use the mail-contact object to show users in the GAL. This approach integrates a GAL without providing other permissions as mail-contacts are not security principals.

A better approach to achieve this goal is to:

- Invite guest users
- Unhide them from the GAL
- Disable them by [blocking them from sign in](#).

A mail-contact object cannot be converted to a user object. Therefore, any properties associated with a mail-contact object cannot be transferred. For example, group memberships and other resource access aren't transferred.

Using a mail-contact object to represent a user presents the following challenges.

- **Office 365 Groups** – Office 365 groups support policies governing the types of users allowed to be members of groups and interact with content associated with groups. For example, a group may not allow guest accounts to join. These policies can't govern mail-contact objects.
- **Azure AD Self-service group management (SSGM)** – Mail-contact objects aren't eligible to be members in groups using the SSGM feature. Additional tools may be needed to manage groups with recipients represented as contacts instead of user objects.
- **Azure AD Identity Governance - Access Reviews** – The access reviews feature can be used to review and attest to membership of Office 365 group. Access reviews are based on user objects. Members represented by mail-contact objects are out of scope of access reviews.
- **Azure AD Identity Governance - Entitlement Management (EM)** – When EM is used to enable self-service access requests for external users via the company's EM portal, a user object is created at the time of request. Mail-contact objects aren't supported.

Azure AD conditional access considerations

The state of the user, device, or network in the user's home tenant isn't conveyed to the resource tenant. Therefore, a guest user account might not satisfy conditional access (CA) policies that use the following controls.

- **Require multi-factor authentication** – Guest users will be required to register/respond to MFA in the resource tenant, even if MFA was satisfied in the home tenant, resulting in multiple MFA challenges. Also, if they need to reset their MFA proofs they might not be aware of the multiple MFA proof registrations across tenants. The lack of awareness might require the user to contact an administrator in the home tenant, resource tenant, or both.

- **Require device to be marked as compliant**– Device identity isn't registered in the resource tenant, so the guest user will be blocked from accessing resources that require this control.
- **Require Hybrid Azure AD Joined device** - Device identity isn't registered in the resource tenant (or on-premises Active Directory connected to resource tenant), so the guest user will be blocked from accessing resources that require this control.
- **Require approved client app or Require app protection policy** – External guest users can't apply resource tenant Intune Mobile App Management (MAM) policy because it also requires device registration. Resource tenant Conditional Access (CA) policy using this control doesn't allow home tenant MAM protection to satisfy the policy. External Guest users should be excluded from every MAM-based CA policy.

Additionally, while the following CA conditions can be used, be aware of the possible ramifications.

- **Sign-in risk and user risk** – The sign in risk and user risk are determined in part by user behavior in their home tenant. The data and risk score is stored in the home tenant.
If resource tenant policies block a guest user, a resource tenant admin might not be able to enable access.
For more information, see [Identity Protection and B2B users](#).
- **Locations** – The named location definitions that are defined in the resource tenant are used to determine the scope of the policy. Trusted locations managed in the home tenant aren't evaluated in the scope of the policy. In some scenarios, organizations might want to share trusted locations across tenants. To share trusted locations, the locations must be defined in each tenant where the resources and conditional access policies are defined.

Other access control considerations

Some additional considerations when configuring access control.

- Define [access control policies](#) to control access to resources.
- Design CA policies with guest users in mind.
- Create policies specifically for guest users.
- If your organization is using the [All Users] condition in your existing CA policy, this policy will affect guest users because [Guest] users are in scope of [All Users].
- Create dedicated CA policies for [Guest] accounts.

For information on hardening dynamic groups that utilize the [All Users] expression, see [Dynamic groups and Azure AD B2B collaboration](#).

Require User Assignment

If an application has the [User assignment required?] property set to [No], guest users can access the application. Application admins must understand access control impacts, especially if the application contains sensitive information. For more information, see [How to restrict your Azure AD app to a set of users](#).

Terms and Conditions

[Azure AD terms of use](#) provides a simple method that organizations can use to present information to end users. You can use terms of use to require guest users to approve terms of use before accessing your resources.

Licensing considerations for guest users with Azure AD Premium features

Azure AD External Identities (guest user) pricing is based on monthly active users (MAU). The active users is the count of unique users with authentication activity within a calendar month. MAU billing helps you reduce costs by offering a free tier and flexible, predictable pricing. In addition, the first 50,000 MAUs per month are free for both Premium P1 and Premium P2 features. Premium features include Conditional Access Policies and Azure MFA for guest users.

For more information, see [MAU billing model for Azure AD External Identities](#).

Office 365 considerations

The following information addresses Office 365 in the context of this paper's scenarios. Detailed information is available at [Office 365 inter-tenant collaboration](#).

Microsoft Exchange Online

Exchange online limits certain functionality for guest users. The limits may be lessened by creating external members instead of external guests. However, none of the following are supported for external users at this time.

- A guest user can be assigned an Exchange Online license. However, they are prevented from being issued a token for Exchange Online. The results are that they are not able to access the resource.
 - Guest users can't use shared or delegated Exchange Online mailboxes in the resource tenant.
 - A guest user can be assigned to a shared mailbox, but can't access it.
- Guest users need to be unhidden in order to be included in the GAL. By default, they are hidden.
 - Hidden guest users are created at invite time. The creation is independent of whether the user has redeemed their invitation. So, if all guest users are unhidden, the list includes user objects of guest users who haven't redeemed an invitation. Based on your scenario, you may or may not want the objects listed.
 - Guest users may be unhidden using [Exchange Online PowerShell](#) only. You may execute the [Set-MailUser](#) PowerShell cmdlet to set the HiddenFromAddressListsEnabled property to a value of \$false.

```
Set-MailUser [GuestUserUPN] -HiddenFromAddressListsEnabled:$false
```

Where [GuestUserUPN] is the calculated UserPrincipalName. Example:

```
Set-MailUser guestuser1_contoso.com#EXT#@fabricam.onmicrosoft.com -  
HiddenFromAddressListsEnabled:$false
```

- Updates to Exchange-specific properties, such as the PrimarySmtpAddress, ExternalEmailAddress, EmailAddresses, and MailTip, can only be set using [Exchange Online PowerShell](#). The Exchange Online Admin Center doesn't allow you to modify the attributes using the GUI.

As shown above, you can use the [Set-MailUser](#) PowerShell cmdlet for mail-specific properties. Many additional user properties you can modify with the [Set-User](#) PowerShell cmdlet. Most of the properties can also be modified using the Azure AD Graph APIs.

Microsoft SharePoint Online

SharePoint Online has its own service-specific permissions depending on if the user is a member of guest in the Azure Active Directory tenant.

For more information, see [Office 365 external sharing and Azure Active Directory B2B collaboration](#).

After enabling external sharing in SharePoint Online, the ability to search for guest users in the SharePoint Online people picker is OFF by default. This setting prohibits guest users from being discoverable when they're hidden from the Exchange Online GAL. You can enable guest users to become visible in two ways (not mutually exclusive):

- You can enable the ability to search for guest users in a few ways:
 - Modify the setting 'ShowPeoplePickerSuggestionsForGuestUsers' at the tenant and site collection

level.

- Set the feature using the [Set-SPOTenant](#) and [Set-SPOSite SharePoint Online PowerShell](#) cmdlets.
- Guest users that are visible in the Exchange Online GAL are also visible in the SharePoint Online people picker. The accounts are visible regardless of the setting for 'ShowPeoplePickerSuggestionsForGuestUsers'.

Microsoft Teams

Microsoft Teams has features to limit access and based on user type. Changes to user type might affect content access and features available.

- The "tenant switching" mechanism for Microsoft Teams might require users to manually switch the context of their Teams client when working in Teams outside their home tenant.
- You can enable Teams users from another entire external domain to find, call, chat, and set up meetings with your users with Teams Federation. For more information, see [Manage external access in Microsoft Teams](#).

Licensing considerations for guest users in Teams

When using Azure B2B with Office 365 workloads,, there are some key considerations. There are instances in which guest accounts do not have the same experience as a member account.

Microsoft groups. See [Adding guests to office 365 Groups](#) to better understand the guest account experience in Microsoft Groups.

Microsoft Teams. See [Team owner, member, and guest capabilities in Teams](#) to better understand the guest account experience in Microsoft Teams.

You can enable a full fidelity experience in Teams by using B2B External Members. Office 365 recently clarified its licensing policy for Multi-tenant organizations.

- Users that are licensed in their home tenant may access resources in another tenant within the same legal entity. The access is granted using **External Members** setting with no additional licensing fees. The setting applies for SharePoint, OneDrive for Business, Teams, and Groups.
 - Engineering work is underway to automatically check the license status of a user in their home tenant and enable them to participate as a Member with no extra license assignment or configuration. However, for customers who wish to use External Members now, there is a licensing workaround that requires the Account Executive to work with the Microsoft Business Desk.
 - From now until the engineered licensing solution is enabled, customers can utilize a *Teams Trial license*. The license can be assigned to each user in their foreign tenant. The license has a one-year duration and enables all of the workloads listed above.
 - For customers that wish to convert B2B Guests into B2B Members there are several known issues with Microsoft Teams such as the inability to create new channels and the ability to add applications to an existing Team.
- **Identity Governance** features (Entitlement Management, Access Reviews) may require other licenses for guest users or external members. Work with the Account Team or Business Desk to get right answer for your organization.

Other products (like Dynamics CRM) may require licensing in every tenant in which a user is represented. Work with your account team to get the right answer for your organization.

Next steps

[Multi-tenant user management introduction](#)

[Multi-tenant end user management scenarios](#)

[Multi-tenant common solutions](#)

Common solutions for multi-tenant user management

4/10/2022 • 2 minutes to read • [Edit Online](#)

There are two specific challenges our customers have solved using current tools. Their solutions are detailed below. Microsoft recommends a single tenant wherever possible and is working on tools to resolve these challenges more easily. If single tenancy does not work for your scenario, these solutions have worked for customers today.

Automatic User Lifecycle Management and resource allocation across tenants

A customer acquires a competitor they previously had close business relationships with. The organizations will maintain their corporate identities.

Current state

Currently, the organizations are synchronizing each other's users as contact-mail objects so that they show in each other's directories.

- Each resource tenant has a mail-contact object enabled for all users in the other tenant.
- No access to applications is possible across tenants.

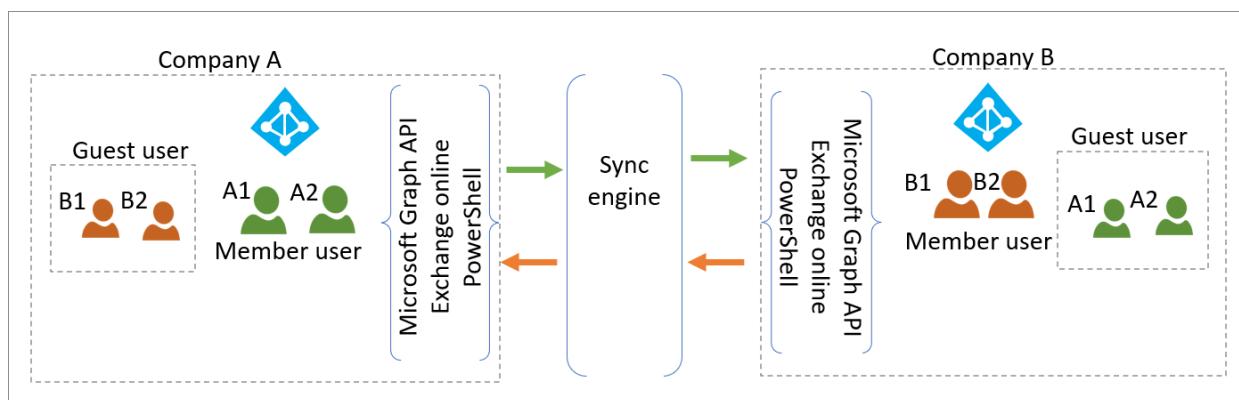
Goals

This customer had the following goals:

- Every user continues to be shown in each organization's GAL.
 - User account lifecycle changes in the home tenant automatically reflected in the resource tenant GAL.
 - Attribute changes in home tenants (such as department, name, SMTP address) automatically reflected in resource tenant GAL and the home GAL.
- Users can access applications and resources in the resource tenant.
- Users can self-serve access requests to resources.

Solution architecture

The organizations will use a point-to-point architecture with a synchronization engine such as MIM.



Each tenant admin does the following to create the user objects:

1. Ensure that their database of users is up to date.
2. Deploy and configure MIM.
 - a. Address existing contact objects.
 - b. Create B2B External Member objects for the other tenant's members.
 - c. Synchronize user object attributes.
3. Deploy and configure [Entitlement Management](#) access packages.
 - a. Resources to be shared
 - b. Expiration and access review policies

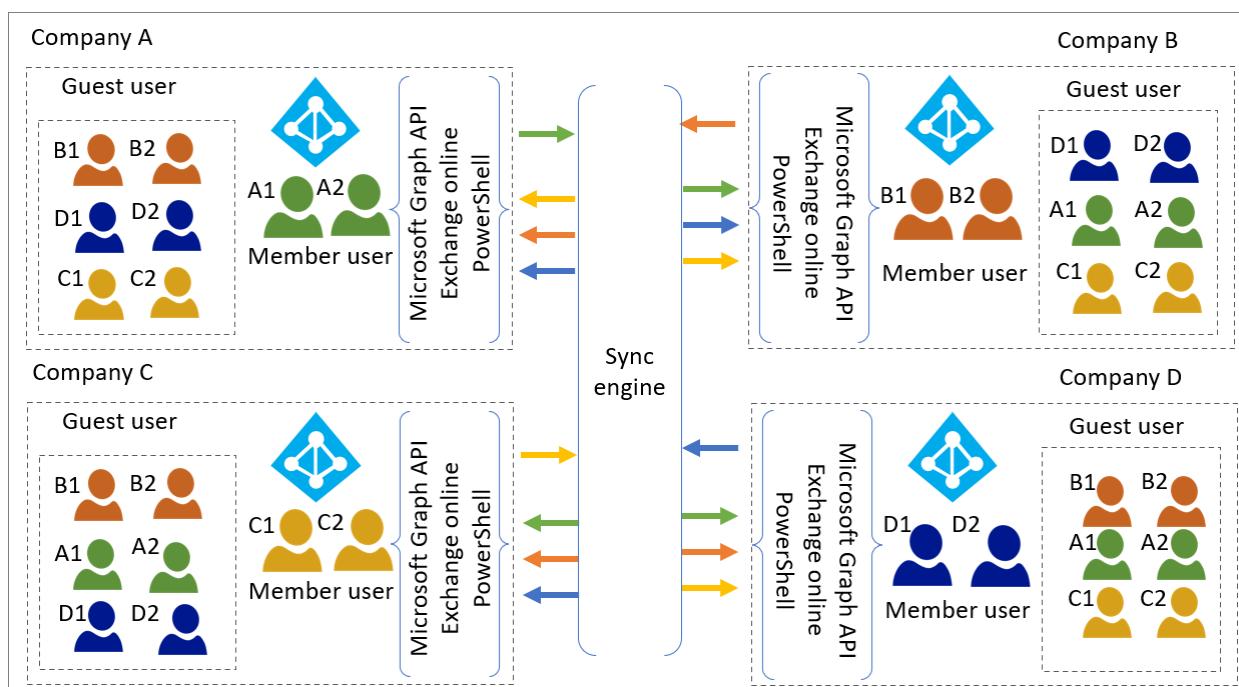
Sharing on-premises apps across tenants

This customer, with multiple peer organizations, has a need to share on-premises applications from one of the tenants.

Current state

Multiple peer organizations are synchronizing B2B Guest users in a mesh topology, enabling resource allocation to their cloud applications across tenants. They currently

- Share applications in Azure AD.
- Ensure user Lifecycle Management in resource tenant is automated based on home tenant. That is, add, modify, delete is reflected.
- Only member users in Company A access Company A's on-premises apps.



Goals

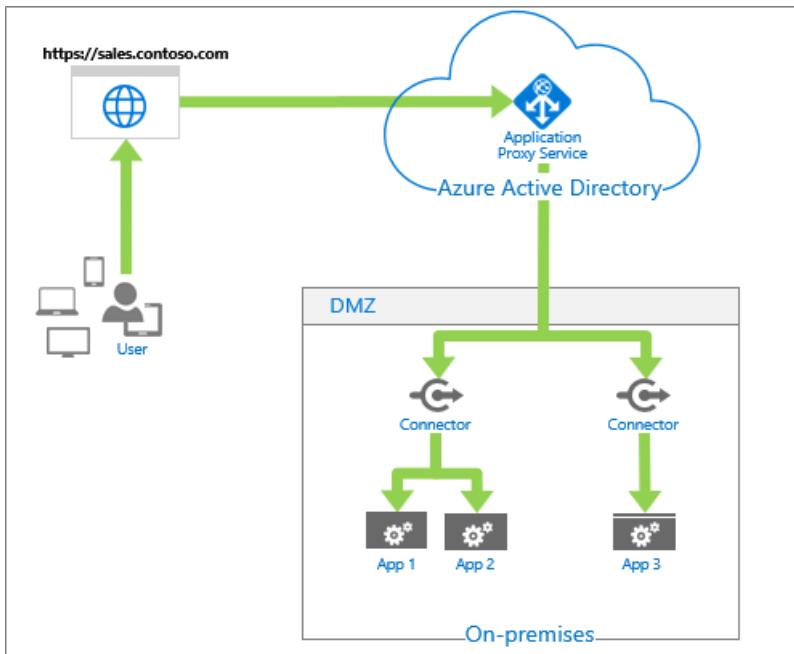
Along with the current functionality, they would like to

- Provide access to Company A's on-premises resources for the external guest users.
- Apps with SAML authentication

- Apps with Integrated Windows Authentication and Kerberos

Solution architecture

Company A is currently providing SSO to on-premises apps for its own members via Azure Application Proxy.



To enable their guest users to access the same on-premises applications Admins in tenet A will:

1. [Configure access to SAML apps.](#)
2. [Configure access to other applications.](#)
3. Create on-premises guest users through [MIM](#) or [PowerShell](#).

For more information about B2B collaboration, see

[Grant B2B users in Azure AD access to your on-premises resources](#)

[Azure Active Directory B2B collaboration for hybrid organizations](#)

Next steps

[Multi-tenant user management introduction](#)

[Multi-tenant end user management scenarios](#)

[Multi-tenant common considerations](#)

Azure Active Directory integrations with authentication and synchronization protocols

4/10/2022 • 2 minutes to read • [Edit Online](#)

Microsoft Azure Active Directory (Azure AD) enables integration with many authentication and synchronization protocols. The authentication integrations enable you to use Azure AD and its security and management features with little or no changes to your applications that use legacy authentication methods. The synchronization integrations enable you to sync user and group data to Azure AD, and then use Azure AD management capabilities. Some sync patterns also enable automated provisioning.

Legacy authentication protocols

The following table presents authentication Azure AD integration with legacy authentication protocols and their capabilities. Select the name of an authentication protocol to see

- A detailed description
- When to use it
- Architectural diagram
- Explanation of system components
- Links for how to implement the integration

AUTHENTICATION PROTOCOL	AUTHENTICATION	AUTHORIZATION	MULTI-FACTOR AUTHENTICATION	CONDITIONAL ACCESS
Header-based authentication	✓	✓	✓	✓
LDAP authentication	✓			
OAuth 2.0 authentication	✓	✓	✓	✓
OIDC authentication	✓	✓	✓	✓
Password based SSO authentication	✓	✓	✓	✓
RADIUS authentication	✓		✓	✓
Remote Desktop Gateway services	✓	✓	✓	✓
Secure Shell (SSH)	✓		✓	✓
SAML authentication	✓	✓	✓	✓

AUTHENTICATION PROTOCOL	AUTHENTICATION	AUTHORIZATION	MULTI-FACTOR AUTHENTICATION	CONDITIONAL ACCESS
Windows Authentication - Kerberos Constrained Delegation	✓	✓	✓	✓

Synchronization patterns

The following table presents Azure AD integration with synchronization patterns and their capabilities. Select the name of a pattern to see

- A detailed description
- When to use it
- Architectural diagram
- Explanation of system components
- Links for how to implement the integration

SYNCHRONIZATION PATTERN	DIRECTORY SYNCHRONIZATION	USER PROVISIONING
Directory synchronization	✓	
LDAP Synchronization	✓	
SCIM synchronization	✓	✓

Header-based authentication with Azure Active Directory

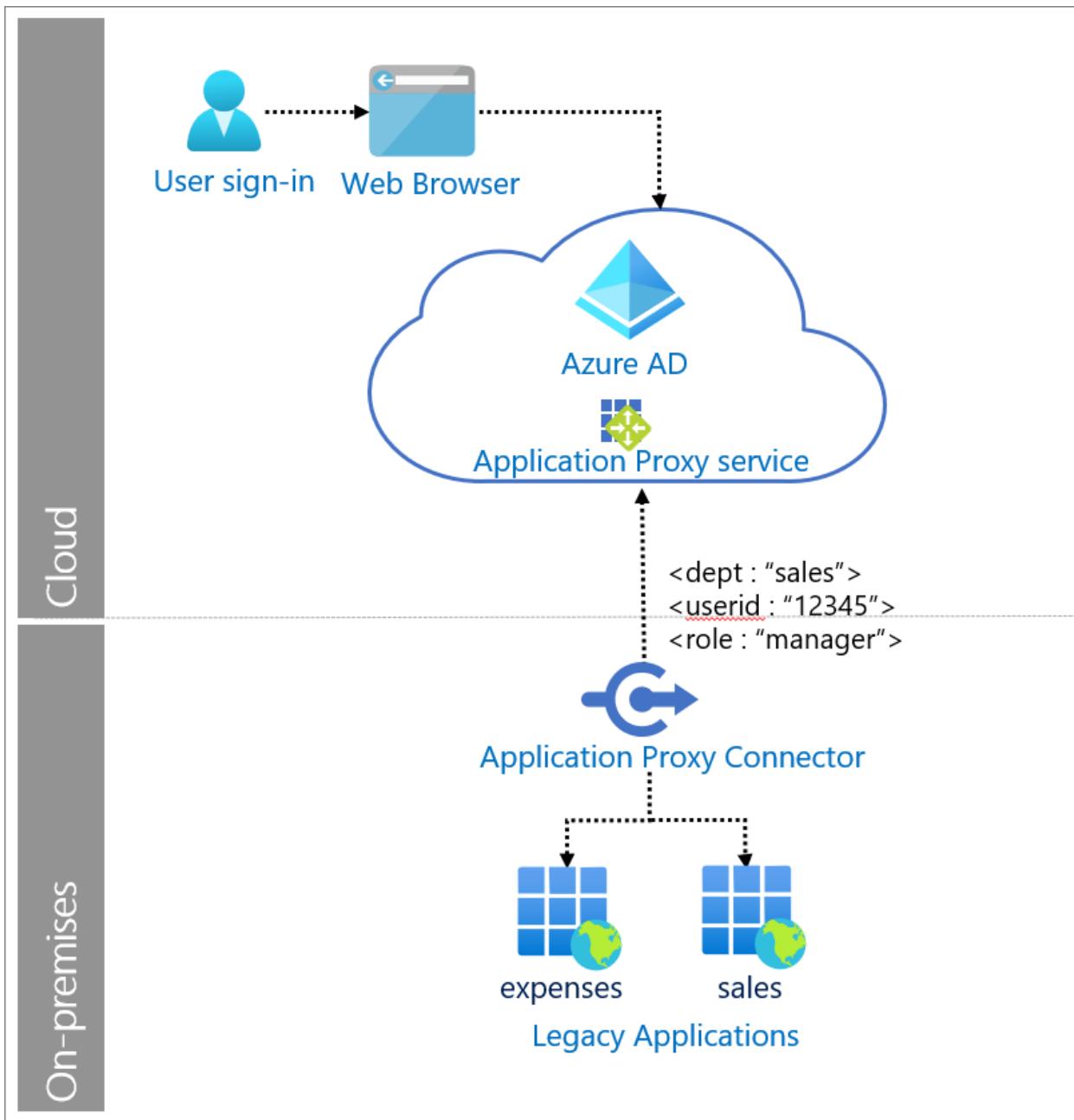
4/10/2022 • 2 minutes to read • [Edit Online](#)

Legacy applications commonly use Header-based authentication. In this scenario, a user (or message originator) authenticates to an intermediary identity solution. The intermediary solution authenticates the user and propagates the required Hypertext Transfer Protocol (HTTP) headers to the destination web service. Azure Active Directory (AD) supports this pattern via its Application Proxy service, and integrations with other network controller solutions.

In our solution, Application Proxy provides remote access to the application, authenticates the user, and passes headers required by the application.

Use when

Remote users need to securely single sign-on (SSO) into on-premises applications that require header-based authentication.



Components of system

- **User:** Accesses legacy applications served by Application Proxy.
- **Web browser:** The component that the user interacts with to access the external URL of the application.
- **Azure AD:** Authenticates the user.
- **Application Proxy service:** Acts as reverse proxy to send request from the user to the on-premises application. It resides in Azure AD and can also enforce any conditional access policies.
- **Application Proxy connector:** Installed on-premises on Windows servers to provide connectivity to the applications. It only uses outbound connections. Returns the response to Azure AD.
- **Legacy applications:** Applications that receive user requests from Application Proxy. The legacy application receives the required HTTP headers to set up a session and return a response.

Implement header-based authentication with Azure AD

- Add an on-premises application for remote access through Application Proxy in Azure AD

- Header-based authentication for single sign-on with Application Proxy and PingAccess
- Secure legacy apps with app delivery controllers and networks

LDAP authentication with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

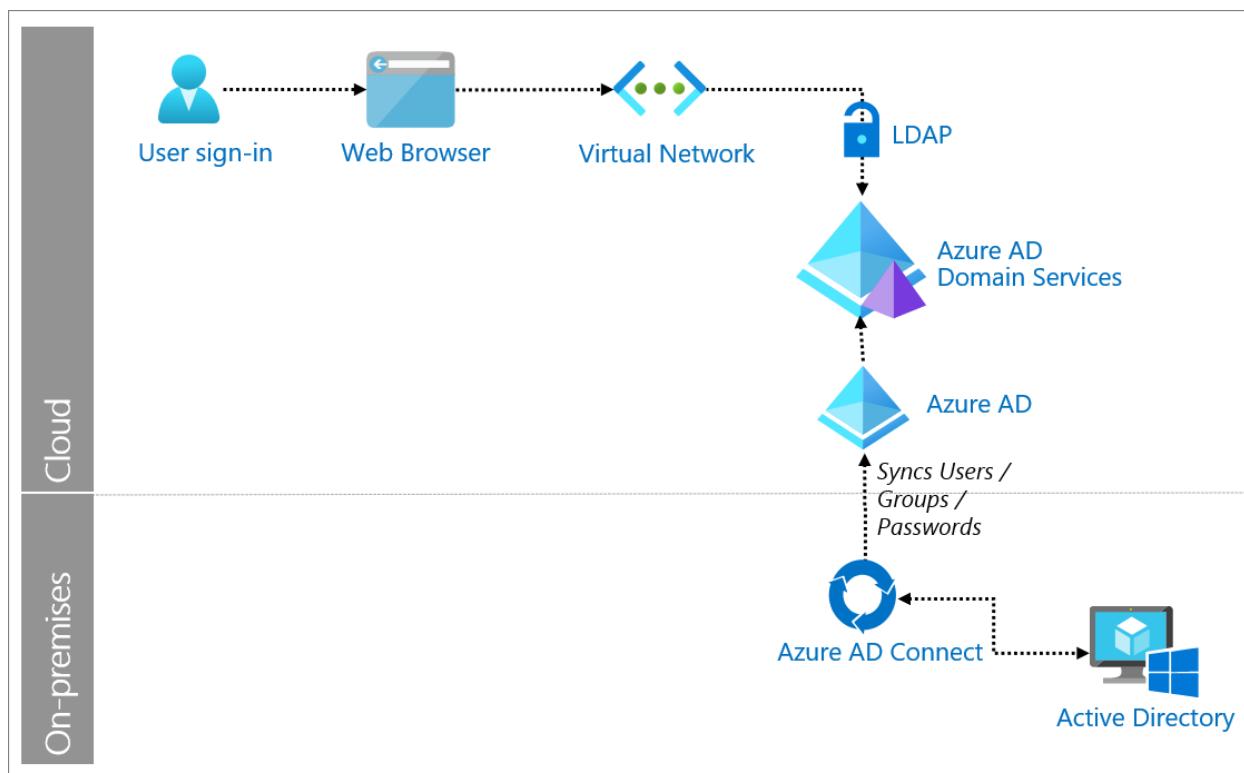
Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services. Directory services, such as Active Directory, [store user and account information](#), and security information like passwords. The service then allows the information to be shared with other devices on the network. Enterprise applications such as email, customer relationship managers (CRMs), and Human Resources (HR) software can use LDAP to authenticate, access, and find information.

Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud-first strategy to modernize their environment by moving off their on-premises LDAP resources to the cloud. The immediate benefits will be:

- Integrated with Azure AD. Additions of users and groups, or attribute changes to their objects are automatically synchronized from your Azure AD tenant to AD DS. Changes to objects in on-premises Active Directory are synchronized to Azure AD, and then to AD DS.
- Simplify operations. Reduces the need to manually keep and patch on-premises infrastructures.
- Reliable. You get managed, highly available services

Use when

There is a need to for an application or service to use LDAP authentication.



Components of system

- **User:** Accesses LDAP-dependent applications via a browser.
- **Web Browser:** The interface that the user interacts with to access the external URL of the application.

- **Virtual Network:** A private network in Azure through which the legacy application can consume LDAP services.
- **Legacy applications:** Applications or server workloads that require LDAP deployed either in a virtual network in Azure, or which have visibility to AD DS instance IPs via networking routes.
- **Azure AD:** Synchronizes identity information from organization's on-premises directory via Azure AD Connect.
- **Azure AD Domain Services (AD DS):** Performs a one-way synchronization from Azure AD to provide access to a central set of users, groups, and credentials. The AD DS instance is assigned to a virtual network. Applications, services, and VMs in Azure that connect to the virtual network assigned to AD DS can use common AD DS features such as LDAP, domain join, group policy, Kerberos, and NTLM authentication.

NOTE

In environments where the organization cannot synchronize password hashes, or users sign-in using smart cards, we recommend that you use a resource forest in AD DS.

- **Azure AD Connect:** A tool for synchronizing on premises identity information to Microsoft Azure AD. The deployment wizard and guided experiences help you configure prerequisites and components required for the connection, including sync and sign on from Active Directory to Azure AD.
- **Active Directory:** Directory service that stores [on-premises identity information such as user and account information](#), and security information like passwords.

Implement LDAP authentication with Azure AD

- [Create and configure an Azure AD DS instance](#)
- [Configure virtual networking for an Azure AD DS instance](#)
- [Configure Secure LDAP for an Azure AD DS managed domain](#)
- [Create an outbound forest trust to an on-premises domain in Azure AD DS](#)

OAuth 2.0 authentication with Azure Active Directory

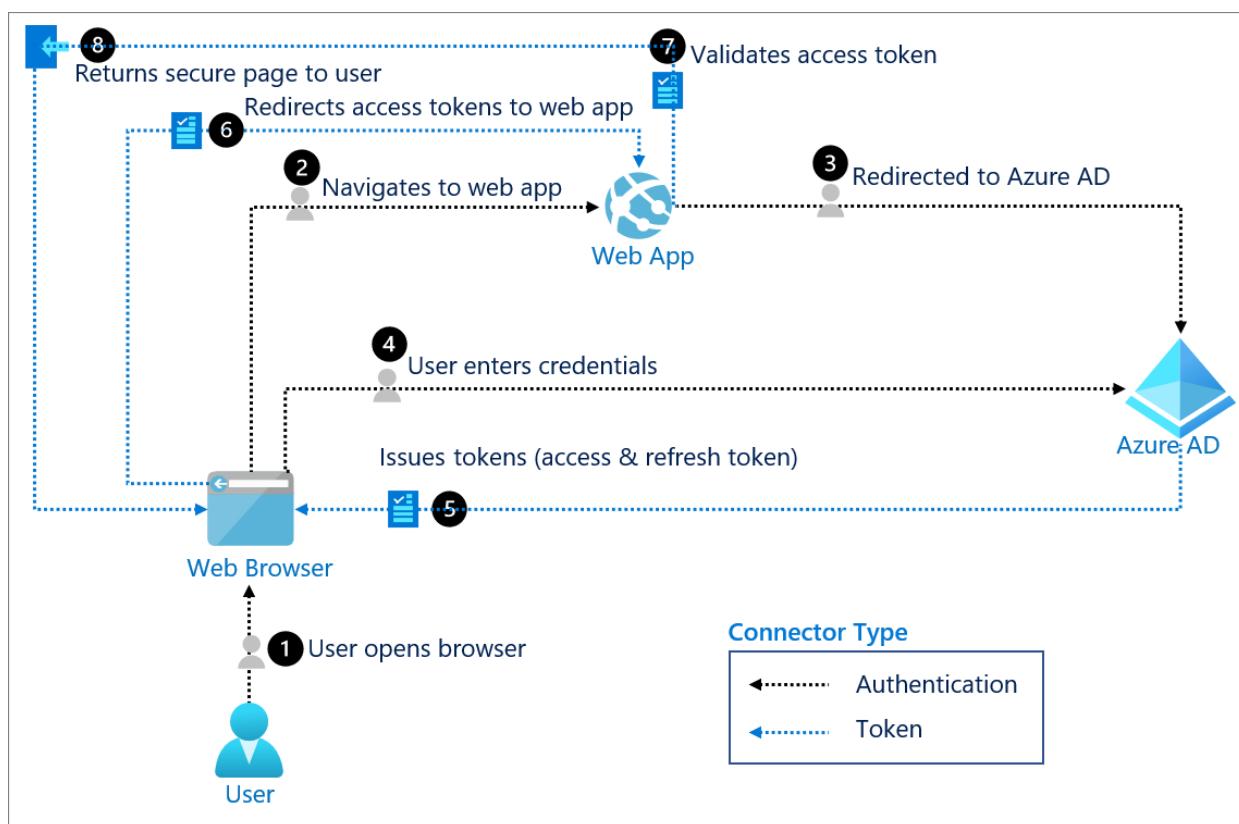
4/10/2022 • 2 minutes to read • [Edit Online](#)

The OAuth 2.0 is the industry protocol for authorization. It allows a user to grant limited access to its protected resources. Designed to work specifically with Hypertext Transfer Protocol (HTTP), OAuth separates the role of the client from the resource owner. The client requests access to the resources controlled by the resource owner and hosted by the resource server. The resource server issues access tokens with the approval of the resource owner. The client uses the access tokens to access the protected resources hosted by the resource server.

OAuth 2.0 is directly related to OpenID Connect (OIDC). Since OIDC is an authentication and authorization layer built on top of OAuth 2.0, it isn't backwards compatible with OAuth 1.0. Azure Active Directory (Azure AD) supports all OAuth 2.0 flows.

Use for:

Rich client and modern app scenarios and RESTful web API access.



Components of system

- **User:** Requests a service from the web application (app). The user is typically the resource owner who owns the data and has the power to allow clients to access the data or resource.
- **Web browser:** The web browser that the user interacts with is the OAuth client.
- **Web app:** The web app, or resource server, is where the resource or data resides. It trusts the authorization server to securely authenticate and authorize the OAuth client.

- **Azure AD:** Azure AD is the authorization server, also known as the Identity Provider (IdP). It securely handles anything to do with the user's information, their access, and the trust relationship. It's responsible for issuing the tokens that grant and revoke access to resources.

Implement OAuth 2.0 with Azure AD

- [Integrating applications with Azure AD](#)
- [OAuth 2.0 and OpenID Connect protocols on the Microsoft Identity Platform](#)
- [Application types and OAuth2](#)

OpenID Connect authentication with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

OpenID Connect (OIDC) is an authentication protocol based on the OAuth2 protocol (which is used for authorization). OIDC uses the standardized message flows from OAuth2 to provide identity services.

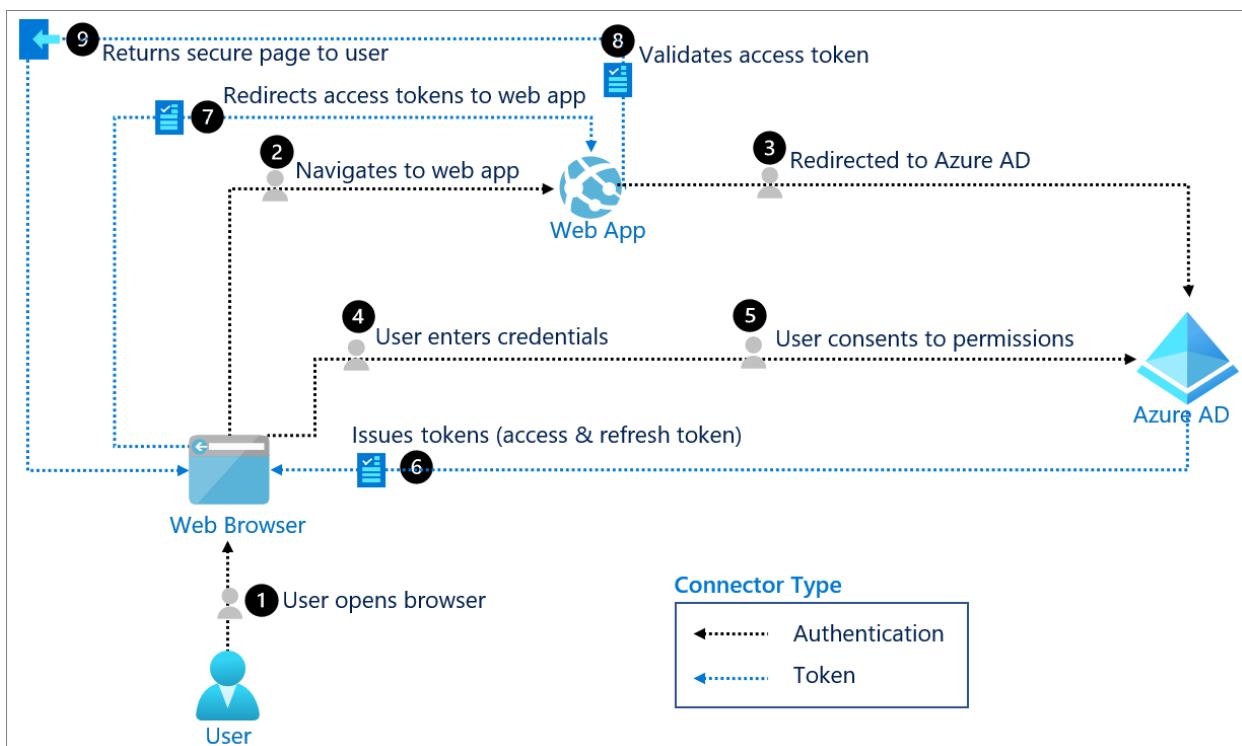
The design goal of OIDC is "making simple things simple and complicated things possible". OIDC lets developers authenticate their users across websites and apps without having to own and manage password files. This provides the app builder with a secure way to verify the identity of the person currently using the browser or native app that is connected to the application.

The authentication of the user must take place at an identity provider where the user's session or credentials will be checked. To do that, you need a trusted agent. Native apps usually launch the system browser for that purpose. Embedded views are considered not trusted since there's nothing to prevent the app from snooping on the user password.

In addition to authentication, the user can be asked for consent. Consent is the user's explicit permission to allow an application to access protected resources. Consent is different from authentication because consent only needs to be provided once for a resource. Consent remains valid until the user or admin manually revokes the grant.

Use when

There is a need for user consent and for web sign in.



Components of system

- User: Requests a service from the application.

- **Trusted agent:** The component that the user interacts with. This trusted agent is usually a web browser.
- **Application:** The application, or Resource Server, is where the resource or data resides. It trusts the identity provider to securely authenticate and authorize the trusted agent.
- **Azure AD:** The OIDC provider, also known as the identity provider, securely manages anything to do with the user's information, their access, and the trust relationships between parties in a flow. It authenticates the identity of the user, grants and revokes access to resources, and issues tokens.

Implement OIDC with Azure AD

- [Integrating applications with Azure AD](#)
- [OAuth 2.0 and OpenID Connect protocols on the Microsoft Identity Platform](#)
- [Microsoft identity platform and OpenID Connect protocol](#)
- [Web sign-in with OpenID Connect in Azure Active Directory B2C](#)
- [Secure your application by using OpenID Connect and Azure AD](#)

Password-based authentication with Azure Active Directory

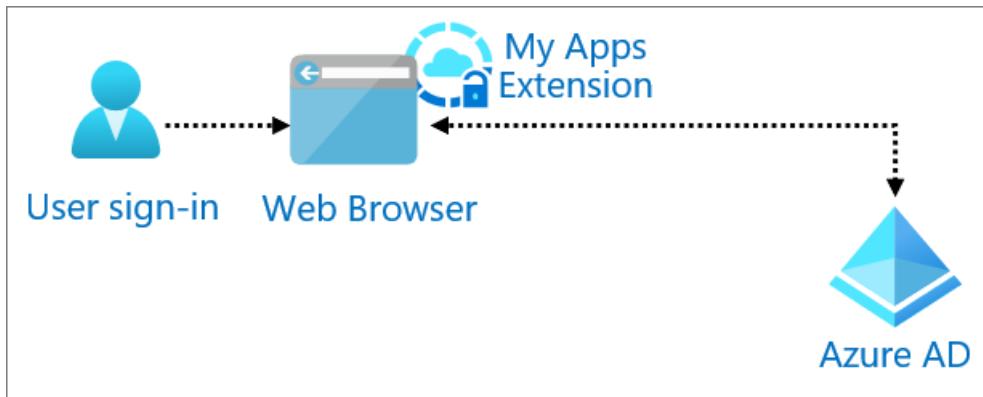
4/10/2022 • 2 minutes to read • [Edit Online](#)

Password based Single Sign-On (SSO) uses the existing authentication process for the application. When you enable password-based SSO, Azure Active Directory (Azure AD) collects, encrypts, and securely stores user credentials in the directory. Azure AD supplies the username and password to the application when the user attempts to sign in.

Choose password-based SSO when an application authenticates with a username and password instead of access tokens and headers. Password-based SSO supports any cloud-based application that has an HTML-based sign in page.

Use when

You need to protect with pre-authentication and provide SSO through password vaulting to web apps.



Components of system

- **User:** Accesses form-based application from either My Apps or by directly visiting the site.
- **Web browser:** The component that the user interacts with to access the external URL of the application. The user accesses the form-based application via the MyApps extension.
- **MyApps extension:** Identifies the configured password-based SSO application and supplies the credentials to the sign in form. The MyApps extension is installed on the web browser.
- **Azure AD:** Authenticates the user.

Implement password-based SSO with Azure AD

- [What is password based SSO](#)
- [Configure password based SSO for cloud applications](#)
- [Configure password-based SSO for on-premises applications with Application Proxy](#)

RADIUS authentication with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Remote Authentication Dial-In User Service (RADIUS) is a network protocol that secures a network by enabling centralized authentication and authorization of dial-in users. Many applications still rely on the RADIUS protocol to authenticate users.

Microsoft Windows Server has a role called the Network Policy Server (NPS), which can act as a RADIUS server and support RADIUS authentication.

Azure Active Directory (Azure AD) enables Multi-factor authentication with RADIUS-based systems. If a customer wants to apply Azure AD Multi-Factor Authentication to any of the previously mentioned RADIUS workloads, they can install the Azure AD Multi-Factor Authentication NPS extension on their Windows NPS server.

The Windows NPS server authenticates a user's credentials against Active Directory, and then sends the Multi-Factor Authentication request to Azure. The user then receives a challenge on their mobile authenticator. Once successful, the client application is allowed to connect to the service.

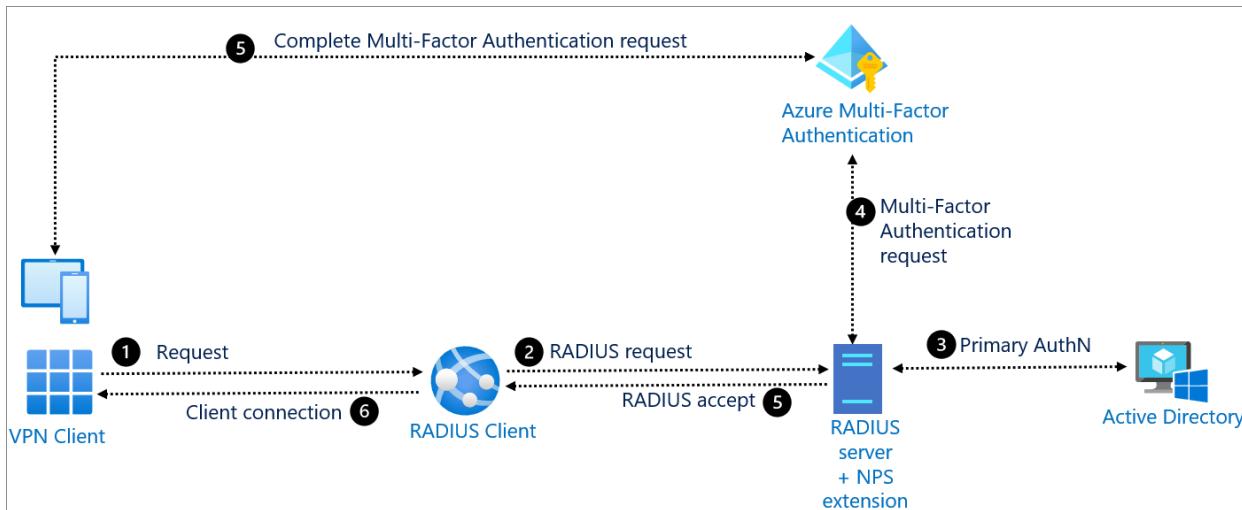
Use when:

You need to add Multi-Factor Authentication to applications like

- a Virtual Private Network (VPN)
- WiFi access
- Remote Desktop Gateway (RDG)
- Virtual Desktop Infrastructure (VDI)
- Any others that depend on the RADIUS protocol to authenticate users into the service.

NOTE

Rather than relying on RADIUS and the Azure AD Multi-Factor Authentication NPS extension to apply Azure AD Multi-Factor Authentication to VPN workloads, we recommend that you upgrade your VPN's to SAML and directly federate your VPN with Azure AD. This gives your VPN the full breadth of Azure AD protection, including Conditional Access, Multi-Factor Authentication, device compliance, and Identity Protection.



Components of the system

- **Client application (VPN client)**: Sends authentication request to the RADIUS client.
- **RADIUS client**: Converts requests from client application and sends them to RADIUS server that has the NPS extension installed.
- **RADIUS server**: Connects with Active Directory to perform the primary authentication for the RADIUS request. Upon success, passes the request to Azure AD Multi-Factor Authentication NPS extension.
- **NPS extension**: Triggers a request to Azure AD Multi-Factor Authentication for a secondary authentication. If successful, NPS extension completes the authentication request by providing the RADIUS server with security tokens that include Multi-Factor Authentication claim, issued by Azure's Security Token Service.
- **Azure AD Multi-Factor Authentication**: Communicates with Azure AD to retrieve the user's details and performs a secondary authentication using a verification method configured by the user.

Implement RADIUS with Azure AD

- [Provide Azure AD Multi-Factor Authentication capabilities using NPS](#)
- [Configure the Azure AD Multi-Factor Authentication NPS extension](#)
- [VPN with Azure AD Multi-Factor Authentication using the NPS extension](#)

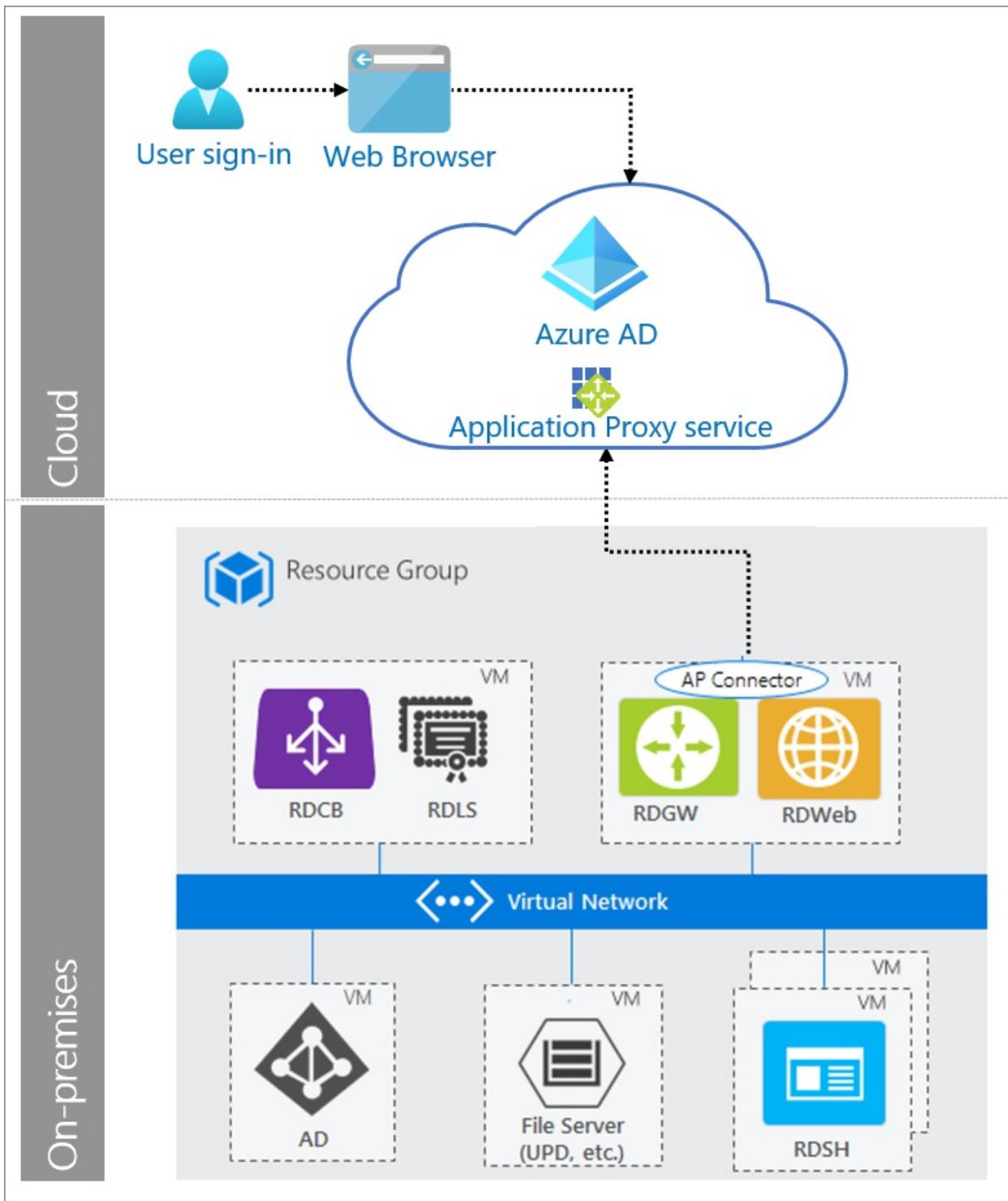
Remote Desktop Gateway Services

4/10/2022 • 2 minutes to read • [Edit Online](#)

A standard Remote Desktop Services (RDS) deployment includes various [Remote Desktop role services](#) running on Windows Server. The RDS deployment with Azure Active Directory (Azure AD) Application Proxy has a permanent outbound connection from the server running the connector service. Other deployments leave open inbound connections through a load balancer. This authentication pattern allows you to offer more types of applications by publishing on-premises applications through Remote Desktop Services. It also reduces the attack surface of their deployment by using Azure AD Application Proxy.

Use when

You need to provide remote access and protect your Remote Desktop Services deployment with pre-authentication.



Components of system

- **User:** Accesses RDS served by Application Proxy.
- **Web browser:** The component that the user interacts with to access the external URL of the application.
- **Azure AD:** Authenticates the user.
- **Application Proxy service:** Acts as reverse proxy to forward request from the user to RDS. Application Proxy can also enforce any Conditional Access policies.
- **Remote Desktop Services:** Acts as a platform for individual virtualized applications, providing secure mobile and remote desktop access, and providing end users the ability to run their applications and desktops from the cloud.

Implement Remote Desktop Gateway services with Azure AD

- [Publish remote desktop with Azure AD Application Proxy](#)
- [Add an on-premises application for remote access through Application Proxy in Azure AD](#)

SAML authentication with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between an identity provider and a service provider. SAML is an XML-based markup language for security assertions, which are statements that service providers use to make access-control decisions.

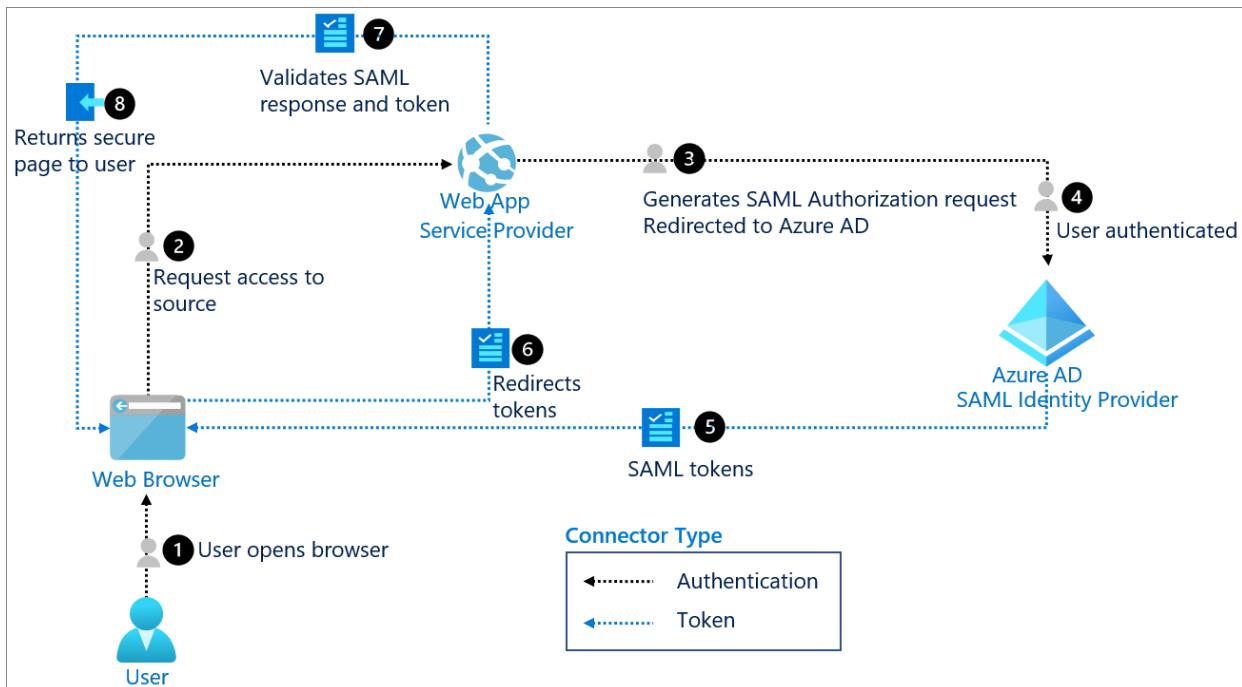
The SAML specification defines three roles:

- The principal, generally a user
- The identity provider (IdP)
- The service provider (SP)

Use when

There's a need to provide a single sign-on (SSO) experience for an enterprise SAML application.

While one of most important use cases that SAML addresses is SSO, especially by extending SSO across security domains, there are other use cases (called profiles) as well.



Components of system

- **User:** Requests a service from the application.
- **Web browser:** The component that the user interacts with.
- **Web app:** Enterprise application that supports SAML and uses Azure AD as IdP.
- **Token:** A SAML assertion (also known as SAML tokens) that carries sets of claims made by the IdP about the principle (user). It contains authentication information, attributes, and authorization decision statements.
- **Azure AD:** Enterprise cloud IdP that provides SSO and Multi-factor authentication for SAML apps. It

synchronizes, maintains, and manages identity information for users while providing authentication services to relying applications.

Implement SAML authentication with Azure AD

- [Tutorials for integrating SaaS applications using Azure Active Directory](#)
- [Configuring SAML based single sign-on for non-gallery applications](#)
- [How Azure AD uses the SAML protocol](#)

SSH

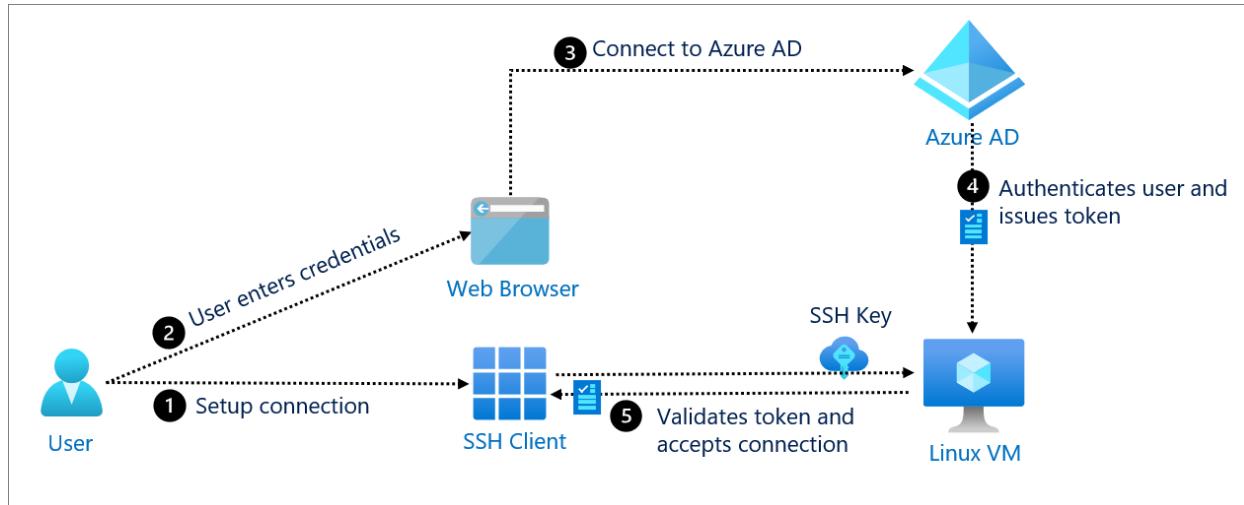
4/10/2022 • 2 minutes to read • [Edit Online](#)

Secure Shell (SSH) is a network protocol that provides encryption for operating network services securely over an unsecured network. SSH also provides a command-line sign in, executes remote commands, and securely transfer files. It is commonly used in Unix-based systems such as Linux®. SSH replaces the Telnet protocol, which does not provide encryption in an unsecured network.

Azure Active Directory (Azure AD) provides a Virtual Machine (VM) extension for Linux® -based systems running on Azure.

Use when

- Working with Linux® -based VMs that require remote sign in
- Executing remote commands in Linux® -based systems
- Securely transfer files in an unsecured network



SSH with Azure AD

Components of system

- **User:** Starts SSH client to set up a connection with the Linux® VMs and provides credentials for authentication.
- **Web browser:** The component that the user interacts with. It communicates with the Identity Provider (Azure AD) to securely authenticate and authorize the user.
- **SSH Client:** Drives the connection setup process.
- **Azure AD:** Authenticates the identity of the user using device flow, and issues token to the Linux VMs.
- **Linux VM:** Accepts token and provides successful connection.

Implement SSH with Azure AD

- [Log in to a Linux® VM with Azure Active Directory credentials - Azure Virtual Machines](#)

- OAuth 2.0 device code flow - Microsoft identity platform
- Integrate with Azure Active Directory (akamai.com)

Windows authentication - Kerberos constrained delegation with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

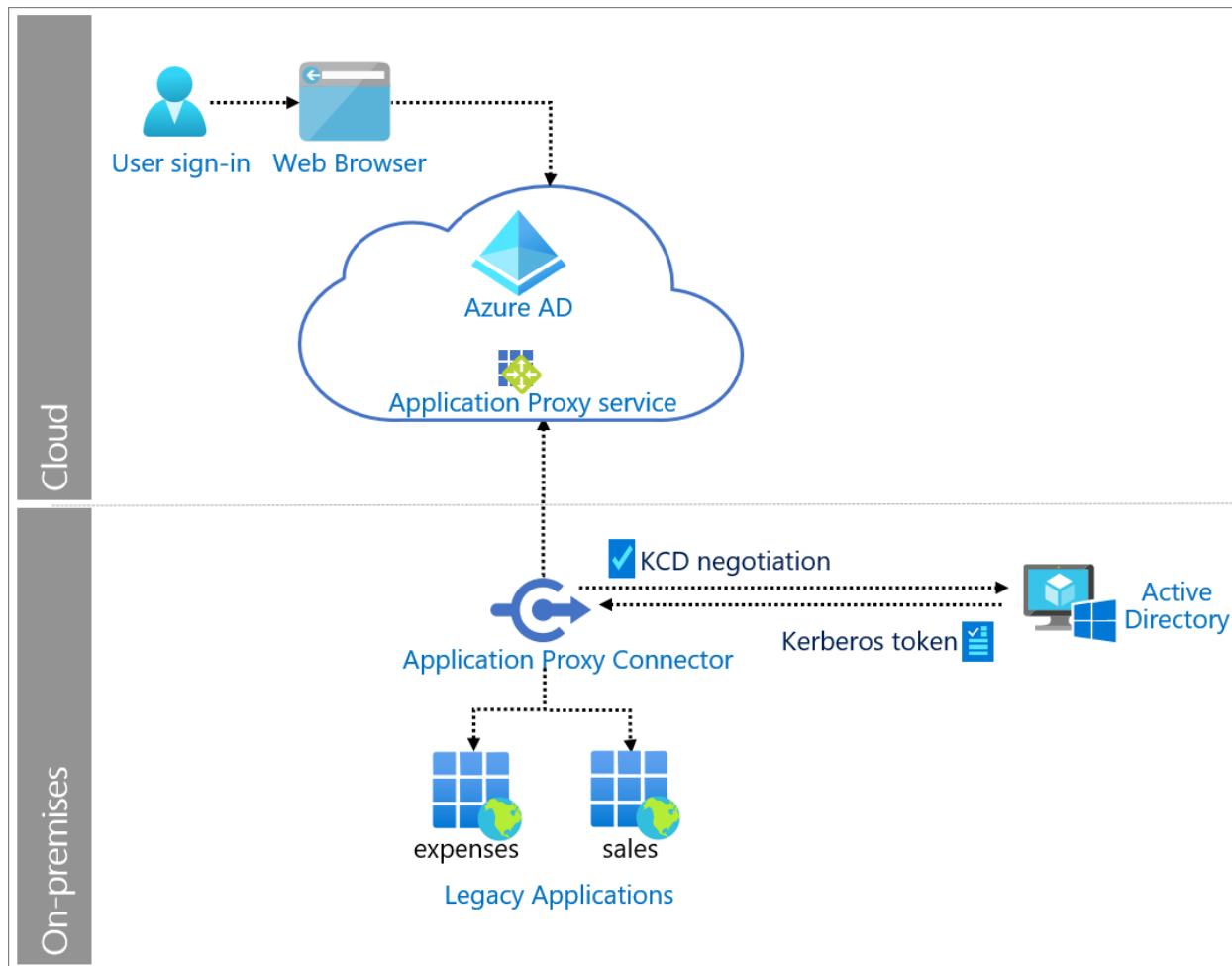
Kerberos Constrained Delegation (KCD) provides constrained delegation between resources and is based on Service Principle Names. It requires domain administrators to create the delegations and is limited to a single domain. Resource-based KCD is often used as a way of providing Kerberos authentication for a web application that has users in multiple domains within an Active Directory forest.

Azure Active Directory Application Proxy can provide single sign-on (SSO) and remote access to KCD-based applications that require a Kerberos ticket for access and Kerberos Constrained Delegation (KCD).

You enable SSO to your on-premises KCD applications that use integrated Windows authentication (IWA) by giving Application Proxy connectors permission to impersonate users in Active Directory. The Application Proxy connector uses this permission to send and receive tokens on the users' behalf.

Use when

There is a need to provide remote access, protect with pre-authentication, and provide SSO to on-premises IWA applications.



Components of system

- **User:** Accesses legacy application served by Application Proxy.

- **Web browser:** The component that the user interacts with to access the external URL of the application.
- **Azure AD:** Authenticates the user.
- **Application Proxy service:** Acts as reverse proxy to send request from the user to the on-premises application. It sits in Azure AD. Application Proxy can also enforce any conditional access policies.
- **Application Proxy connector:** Installed on-premises on Windows servers to provide connectivity to the application. Returns the response to Azure AD. Performs KCD negotiation with Active Directory, impersonating the user to get a Kerberos token to the application.
- **Active Directory:** Sends the Kerberos token for the application to the Application Proxy connector.
- **Legacy applications:** Applications that receive user requests from Application Proxy. The legacy applications return the response to the Application Proxy connector.

Implement Windows authentication (KCD) with Azure AD

- [Kerberos Constrained Delegation for single sign-on to your apps with Application Proxy](#)
- [Add an on-premises application for remote access through Application Proxy in Azure Active Directory](#)

Directory synchronization

4/10/2022 • 2 minutes to read • [Edit Online](#)

Many organizations have a hybrid infrastructure encompassing both on-premises and cloud components. Synchronizing users' identities between local and cloud directories lets users access resources with a single set of credentials.

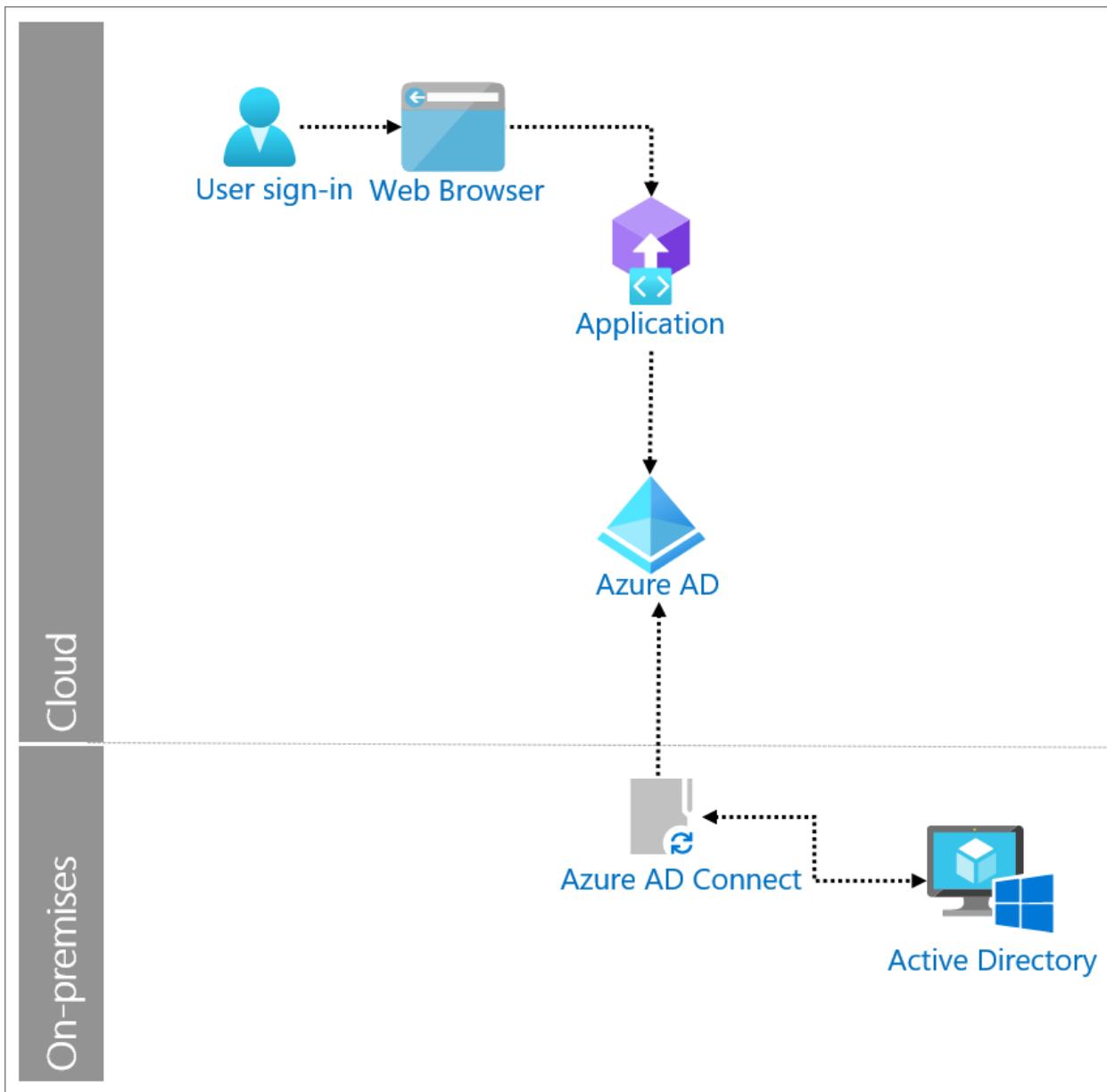
Synchronization is the process of

- creating an object based on certain conditions
- keeping the object updated
- removing the object when conditions are no longer met.

On-premises provisioning involves provisioning from on-premises sources (like Active Directory) to Azure Active Directory (Azure AD).

Use when

You need to synchronize identity data from your on-premises Active Directory environments to Azure AD.



Components of system

- **User:** Accesses an application using Azure AD.
- **Web browser:** The component that the user interacts with to access the external URL of the application.
- **Application:** Web app that relies on the use of Azure AD for authentication and authorization purposes.
- **Azure AD:** Synchronizes identity information from organization's on-premises directory via Azure AD Connect.
- **Azure AD Connect:** A tool for connecting on-premises identity infrastructures to Microsoft Azure AD. The wizard and guided experiences help you deploy and configure pre-requisites and components required for the connection, including sync and sign on from Active Directories to Azure AD.
- **Active Directory:** Active Directory is a directory service included in most Windows Server operating systems. Servers running Active Directory Domain Services (AD DS) are called domain controllers. They authenticate and authorize all users and computers in the domain.

Implement directory synchronization with Azure AD

- [What is identity provisioning?](#)

- Hybrid identity directory integration tools
- Azure AD Connect installation roadmap

LDAP synchronization with Azure Active Directory

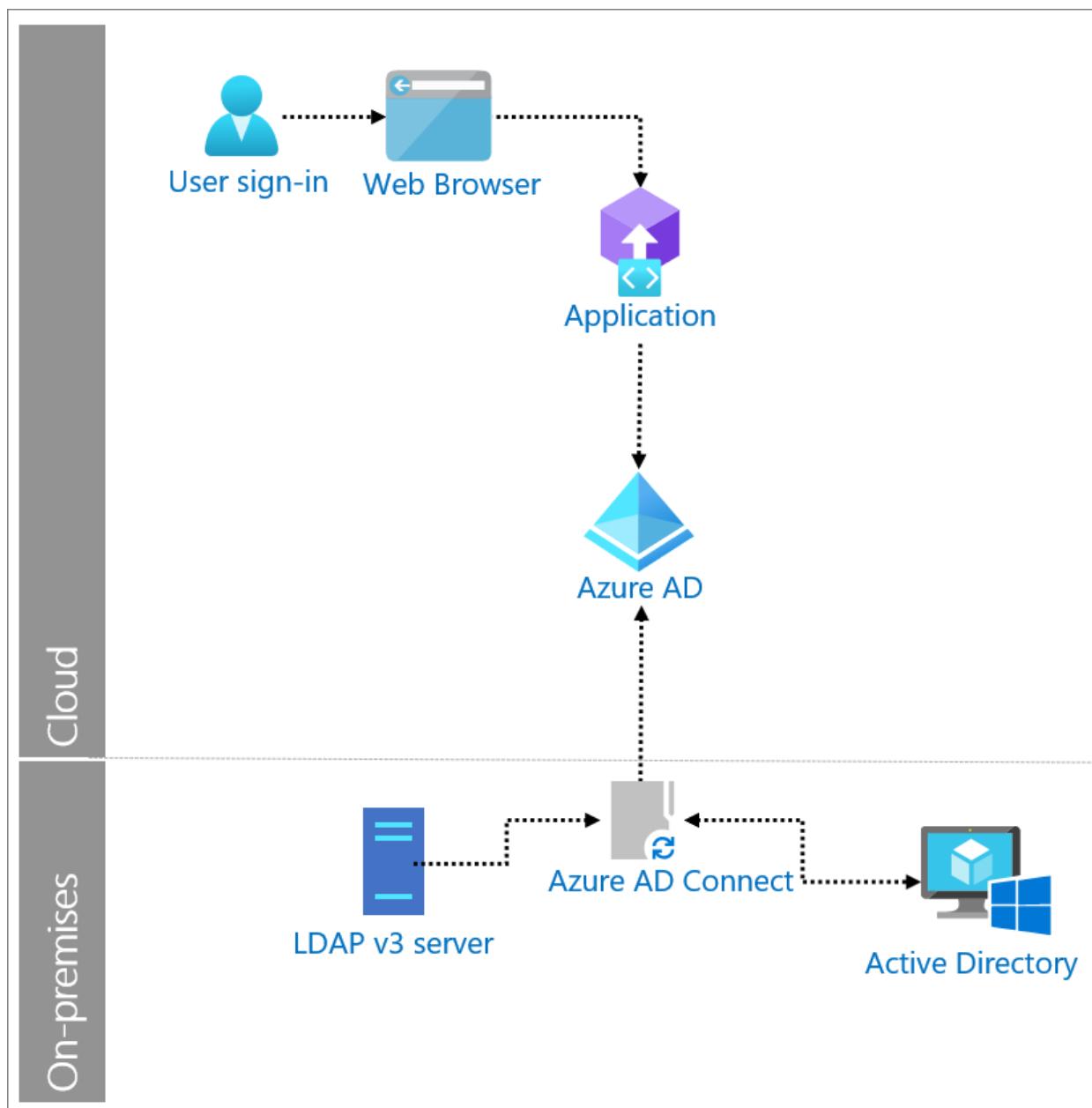
4/10/2022 • 2 minutes to read • [Edit Online](#)

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on the TCP/IP stack. It provides a mechanism used to connect to, search, and modify internet directories. The LDAP directory service is based on a client-server model and its function is to enable access to an existing directory. Many companies depend on on-premises LDAP servers to store users and groups for their critical business apps.

Azure Active Directory (Azure AD) can replace LDAP synchronization with Azure AD Connect. The Azure AD Connect synchronization service performs all the operations related to synchronizing identity data between your on-premises environments and Azure AD.

Use when

You need to synchronize identity data between your on-premises LDAP v3 directories and Azure AD.



Components of system

- **User:** Accesses an application that relies on the use of a LDAP v3 directory for sorting users and passwords.
- **Web browser:** The component that the user interacts with to access the external URL of the application
- **Web app:** Application with dependencies on LDAP v3 directories.
- **Azure AD:** Azure AD synchronizes identity information (users, groups) from organization's on-premises LDAP directories via Azure AD Connect.
- **Azure AD Connect:** is a tool for connecting on premises identity infrastructures to Microsoft Azure AD. The wizard and guided experiences help to deploy and configure pre-requisites and components required for the connection.
- **Custom Connector:** A Generic LDAP Connector enables you to integrate the Azure AD Connect synchronization service with an LDAP v3 server. It sits on Azure AD Connect.
- **Active Directory:** Active Directory is a directory service included in most Windows Server operating systems. Servers running Active Directory Directory Services are called domain controllers and they authenticate and authorize all users and computers in a Windows domain.
- **LDAP v3 server:** LDAP protocol-compliant directory storing corporate users and passwords used for directory services authentication.

Implement LDAP synchronization with Azure AD

- [Hybrid Identity directory integration tools](#)
- [Azure AD Connect installation roadmap](#)
- [Overview and creation a LDAP Connector](#)

NOTE

Deploying the LDAP Connector requires an advanced configuration and this connector is provided under limited support. Configuring this connector requires familiarity with Microsoft Identity Manager and the specific LDAP directory.

Customers who require to deploy this configuration in a production environment are recommended to work with a partner such as Microsoft Consulting Services for help, guidance and support for this configuration.

SCIM synchronization with Azure Active Directory

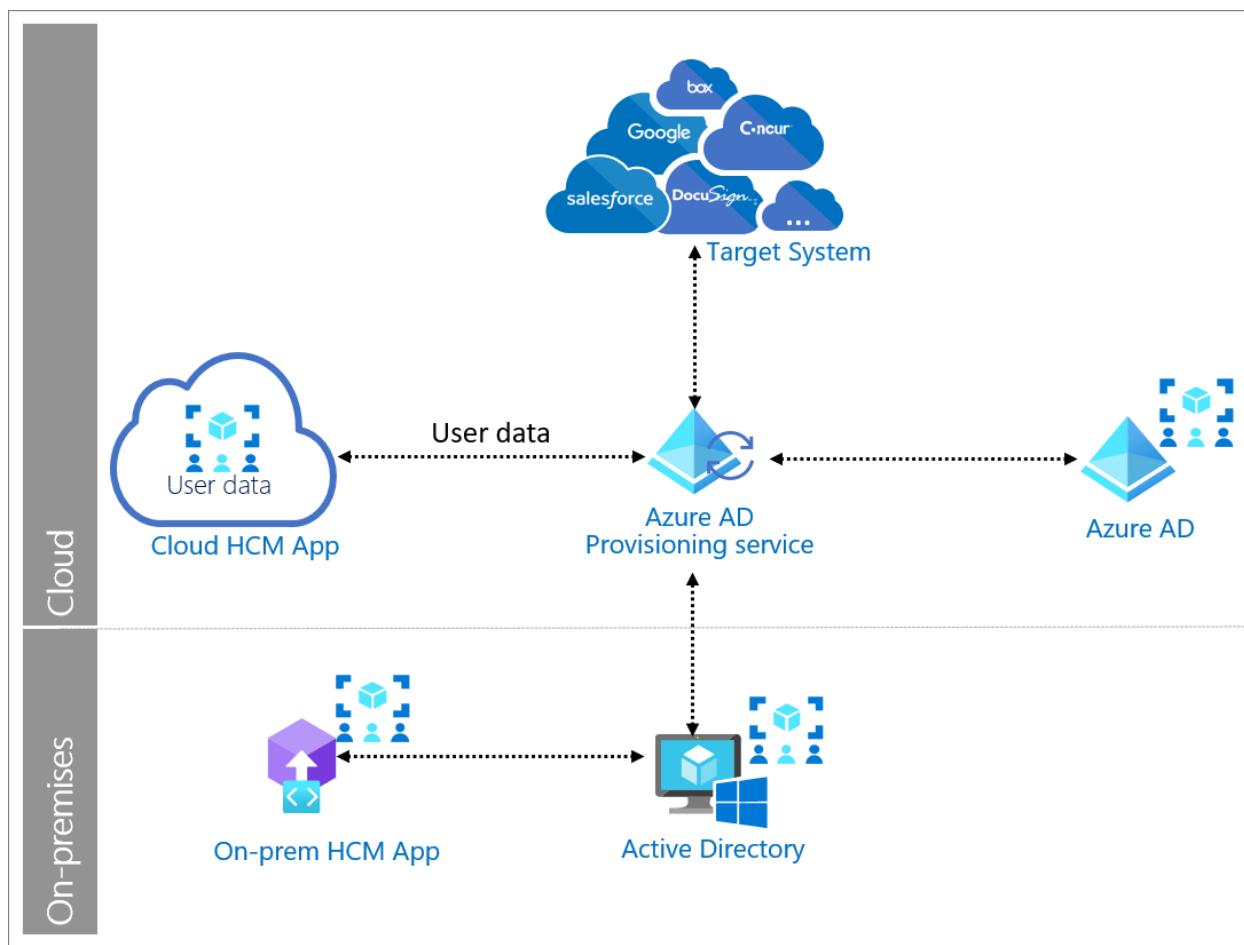
4/10/2022 • 2 minutes to read • [Edit Online](#)

System for Cross-Domain Identity Management (SCIM) is an open standard protocol for automating the exchange of user identity information between identity domains and IT systems. SCIM ensures that employees added to the Human Capital Management (HCM) system automatically have accounts created in Azure Active Directory (Azure AD) or Windows Server Active Directory. User attributes and profiles are synchronized between the two systems, updating removing users based on the user status or role change.

SCIM is a standardized definition of two endpoints: a /Users' endpoint and a /Groups endpoint. It uses common REST verbs to create, update, and delete objects. It also uses a pre-defined schema for common attributes like group name, username, first name, last name, and email. Applications that offer a SCIM 2.0 REST API can reduce or eliminate the pain of working with proprietary user management APIs or products. For example, any SCIM-compliant client can make an HTTP POST of a JSON object to the /Users endpoint to create a new user entry. Instead of needing a slightly different API for the same basic actions, apps that conform to the SCIM standard can instantly take advantage of pre-existing clients, tools, and code.

Use when:

You want to automatically provision user information from an HCM system to Azure AD and Windows Server Active Directory, and then to target systems if necessary.



Components of system

- **HCM system:** Applications and technologies that enable Human Capital Management process and

practices that support and automate HR processes throughout the employee lifecycle.

- **Azure AD Provisioning Service:** Uses the SCIM 2.0 protocol for automatic provisioning. The service connects to the SCIM endpoint for the application, and uses the SCIM user object schema and REST APIs to automate provisioning and de-provisioning of users and groups.
- **Azure AD:** User repository used to manage the lifecycle of identities and their entitlements.
- **Target system:** Application or system that has SCIM endpoint and works with the Azure AD provisioning to enable automatic provisioning of users and groups.

Implement SCIM with Azure AD

- [How provisioning works in Azure AD](#)
- [Managing user account provisioning for enterprise apps in the Azure portal](#)
- [Build a SCIM endpoint and configure user provisioning with Azure AD](#)
- [SCIM 2.0 protocol compliance of the Azure AD Provisioning Service](#)

Building resilience into identity and access management with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Identity and access management (IAM) is a framework of processes, policies, and technologies that facilitate the management of identities and what they access. It includes the many components supporting the authentication and authorization of user and other accounts in your system.

IAM resilience is the ability to endure disruption to system components and recover with minimal impact to your business, users, customers, and operations. Reducing dependencies, complexity, and single-points-of-failure, while ensuring comprehensive error handling will increase your resilience.

Disruption can come from any component of your IAM systems. To build a resilient IAM system, assume disruptions will occur and plan for it.

When planning the resilience of your IAM solution, consider the following elements:

- Your applications that rely on your IAM system.
- The public infrastructures your authentication calls use, including telecom companies, Internet service providers, and public key providers.
- Your cloud and on-premises identity providers.
- Other services that rely on your IAM, and the APIs that connect them.
- Any other on-premises components in your system.

Whatever the source, recognizing and planning for the contingencies is important. However, adding additional identity systems, and their resultant dependencies and complexity, may reduce your resilience rather than increase it.

To build more resilience in your systems, review the following articles:

- [Build resilience in your IAM infrastructure](#)
- [Build IAM resilience in your applications](#)
- [Build resilience in your Customer Identity and Access Management \(CIAM\) systems](#)

Build resilience in your identity and access management infrastructure

4/10/2022 • 2 minutes to read • [Edit Online](#)

Azure Active Directory is a global cloud identity and access management system that provides critical services such as authentication and authorization to your organization's resources. This document provides you with guidance to understand, contain, and mitigate the risk of disruption of authentication or authorization services for resources that rely on Azure Active Directory (Azure AD).

The document set is designed for

- Identity Architects
- Identity Service Owners
- Identity Operations teams

Please also see the documentation for [application developers](#) and for [Azure AD B2C systems](#).

What is resilience?

In the context of your identity infrastructure, resilience is the ability to endure disruption to services like authentication and authorization, or failure of other components, with minimal or no impact to your business, users, and operations. The impact of disruption can be severe, and resilience requires diligent planning.

Why worry about disruption?

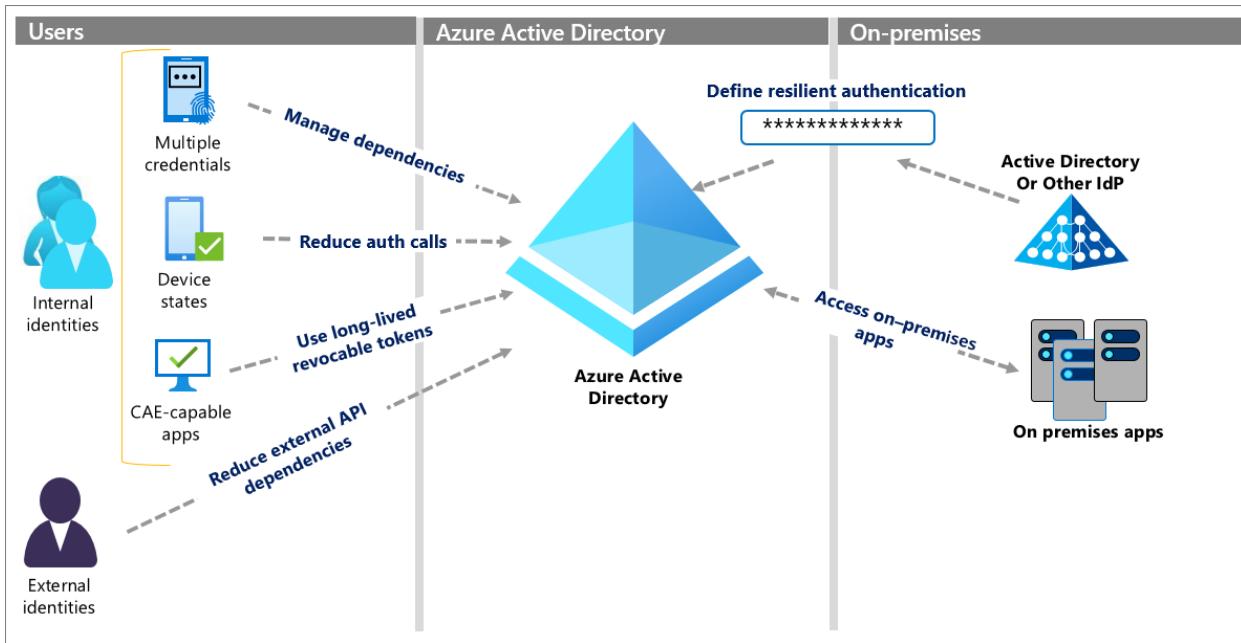
Every call to the authentication system is subject to disruption if any component of the call fails. When authentication gets disrupted, because of the underlying component failures, your users will not access their applications. Therefore, reducing the number of authentication calls and number of dependencies in those calls is important to your resilience. Application developers can assert some control over how often tokens are requested. For example, work with your developers to ensure they're using Azure AD Managed Identities for their applications wherever possible.

In a token-based authentication system like Azure AD, a user's application (client) must acquire a security token from the identity system before it can access an application or other resource. During the validity period, a client can present the same token multiple times to access the application.

When the token presented to the application expires, the application rejects the token, and the client must acquire a new token from Azure AD. Acquiring a new token potentially requires user interaction such as credential prompts or meeting other requirements of the authentication system. Reducing the frequency of authentication calls with longer-lived tokens decreases unnecessary interactions. However, you must balance token life with the risk created by fewer policy evaluations. For more information on managing token lifetimes, see this article on [optimizing reauthentication prompts](#).

Ways to increase resilience

The following diagram shows six concrete ways you can increase resilience. Each method is explained in detail in the articles linked in the Next steps portion of this article.



Next steps

Resilience resources for administrators and architects

- Build resilience with credential management
- Build resilience with device states
- Build resilience by using Continuous Access Evaluation (CAE)
- Build resilience in external user authentication
- Build resilience in your hybrid authentication
- Build resilience in application access with Application Proxy

Resilience resources for developers

- Build IAM resilience in your applications
- Build resilience in your CIAM systems

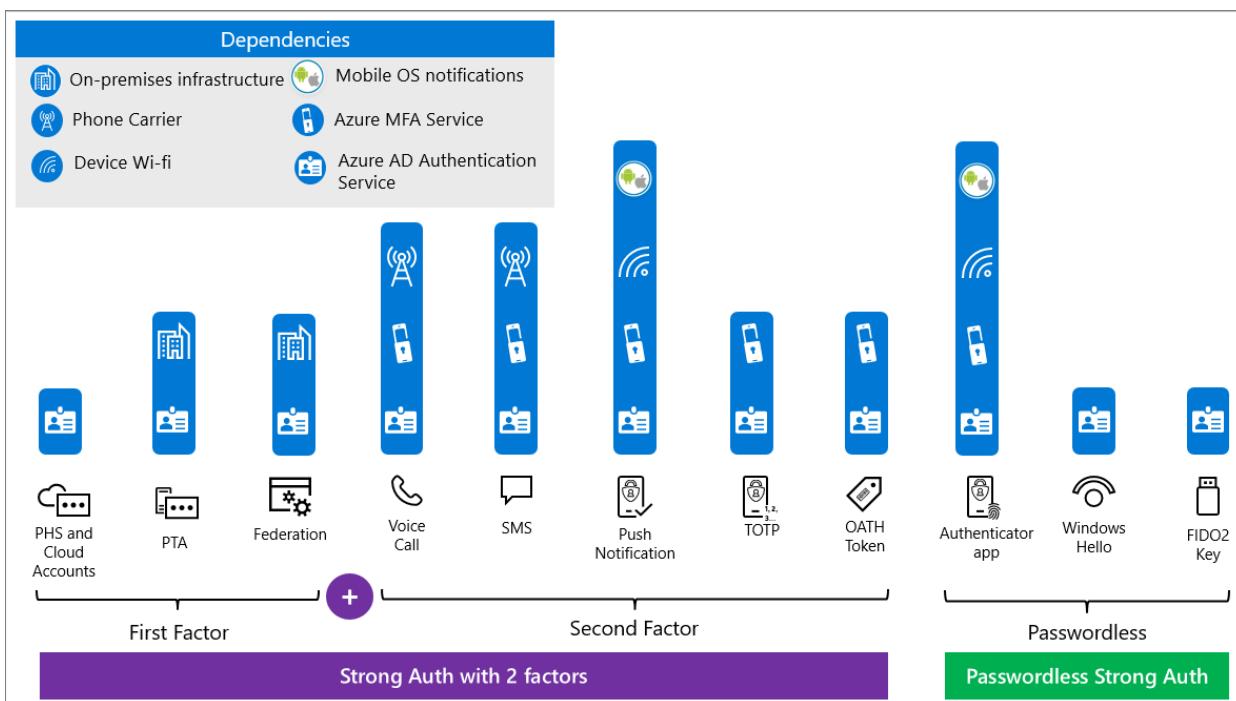
Build resilience with credential management

4/10/2022 • 2 minutes to read • [Edit Online](#)

When a credential is presented to Azure AD in a token request, there are multiple dependencies that must be available for validation. The first authentication factor relies on Azure AD authentication, and in some cases on on-premises infrastructure. For more information on hybrid authentication architectures, see [Build resilience in your hybrid infrastructure](#).

If you implement a second factor, the dependencies for the second factor are added to the dependencies for the first. For example, if your first factor is via PTA, and your second factor is SMS, your dependencies are:

- Azure AD authentication services
- Azure MFA service
- On-premises infrastructure
- Phone carrier
- The user's device (not pictured)



Your credential strategy should consider the dependencies of each authentication type, and provision methods that avoid a single point of failure.

Because authentication methods have different dependencies, it's a good idea to enable users to register for as many second-factor options as possible. Be sure to include second factors with different dependencies if possible. For example, Voice call and SMS as second factors share the same dependencies, so having them as the only options does not mitigate risk.

The most resilient credential strategy is to use passwordless authentication. Windows Hello for Business and FIDO 2.0 security keys have fewer dependencies than strong authentication with two separate factors. The Microsoft Authenticator app, Windows Hello for Business and Fido 2.0 security keys are the most secure.

For second factors, the Microsoft Authenticator app or other authenticator apps using time-based one time

passcode (TOTP) or OATH hardware tokens have the fewest dependencies, and are therefore more resilient.

How do multiple credentials help resilience?

Provisioning multiple credential types gives users options that accommodate their preferences and environmental constraints. As a result, interactive authentication where users are prompted for Multi-factor authentication will be more resilient to specific dependencies being unavailable at the time of the request. You can [optimize reauthentication prompts for Multi-factor authentication](#).

In addition to individual user resiliency described above, enterprises should plan contingencies for large-scale disruptions such as operational errors that introduce a misconfiguration, a natural disaster, or an enterprise-wide resource outage to an on-premises federation service (especially when used for Multi-factor authentication).

How do I implement resilient credentials?

- Deploy [Passwordless credentials](#) such as Windows Hello for Business, Phone Authentication, and FIDO2 security keys to reduce dependencies.
- Deploy the [Microsoft Authenticator App](#) as a second factor.
- Turn on [password hash synchronization](#) for hybrid accounts that are synchronized from Windows Server Active Directory. This option can be enabled alongside federation services such as AD FS and provides a fall back in case the federation service fails.
- [Analyze usage of Multi-factor authentication methods](#) to improve users' experience.
- [Implement a resilient access control strategy](#)

Next steps

Resilience resources for administrators and architects

- [Build resilience with device states](#)
- [Build resilience by using Continuous Access Evaluation \(CAE\)](#)
- [Build resilience in external user authentication](#)
- [Build resilience in your hybrid authentication](#)
- [Build resilience in application access with Application Proxy](#)

Resilience resources for developers

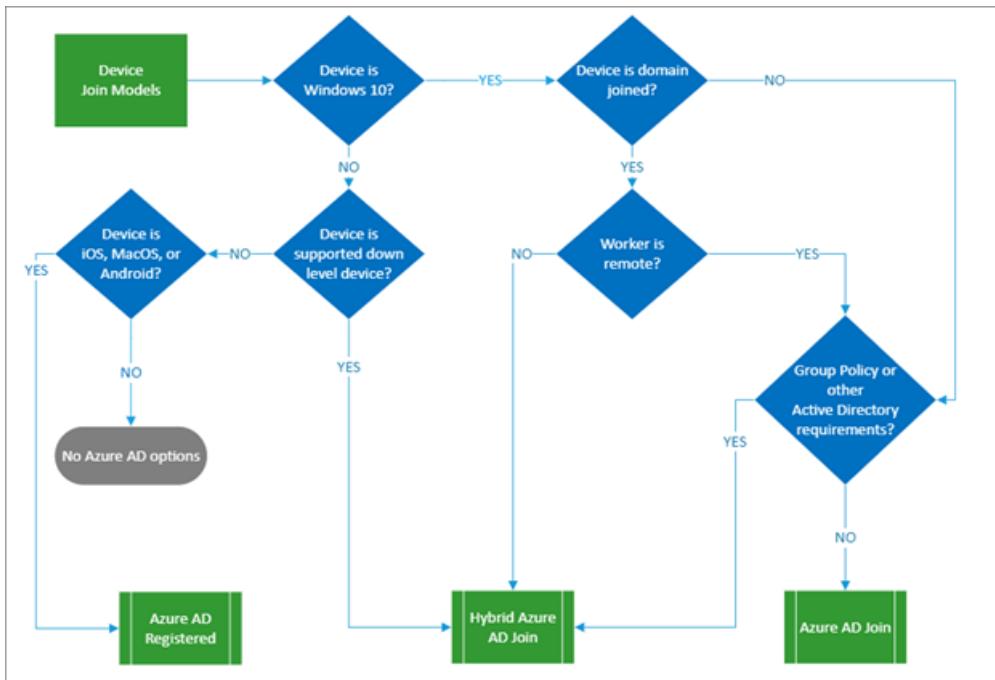
- [Build IAM resilience in your applications](#)
- [Build resilience in your CIAM systems](#)

Build resilience with device states

4/10/2022 • 2 minutes to read • [Edit Online](#)

By enabling [device states](#) with Azure AD, administrators can author [Conditional Access policies](#) that control access to applications based on device state. The added benefit of devices is that it satisfies strong authentication requirements for access to resources thus reducing additional MFA authentication requests and improving resiliency.

The following flow chart presents the different ways to onboard devices in Azure AD that enable device states. You can use more than one in your organization.



When you use [device states](#), users will in most cases experience single sign-on to resources through a [Primary Refresh Token](#) (PRT). The PRT contains claims about the user and the device and can be used to get authentication tokens to access applications from the device. The PRT is valid for 14 days and is continuously renewed as long as the user actively uses the device, providing users a resilient experience. A PRT can also get a multi-factor authentication claim in several ways. For more information, see [When does a PRT get an MFA claim](#).

How do device states help?

When a PRT is used to request access to an application, its device, session, and MFA claims are trusted by Azure AD. When administrators create policies that require either a device-based control or a Multi-factor authentication control, then the policy requirement can be met through its device state without attempting Multi-factor authentication. Users will not see additional Multi-factor authentication prompts on the same device. This increases resilience to a disruption of the Azure MFA service, or its dependencies like local telecom providers.

How do I implement device states?

- Enable [hybrid Azure AD Joined](#) and [Azure AD Join](#) for company owned Windows devices, and require they be joined if possible. If not possible, require they be registered.

If there are older versions of Windows in your organization, upgrade those devices to use Windows 10.

- Standardize user browser access to use either [Microsoft Edge](#) or Google Chrome with [supported extensions](#) that enabled seamless SSO to web applications using the PRT.
- For personal or company owned iOS and Android devices deploy the [Microsoft Authenticator App](#). In addition to the Multi-factor authentication and password-less sign in capabilities, the Microsoft Authenticator app will enable single sign across native application through [brokered authentication](#) with fewer authentication prompts for end users.
- For personal or company owned iOS and Android devices use [mobile application management](#) to securely access company resources with fewer authentication requests.
- [Use the Microsoft Enterprise SSO plug-in for Apple devices \(preview\)](#). This registers the device and provides SSO across browser and native Azure AD applications.

Next steps

Resilience resources for administrators and architects

- [Build resilience with credential management](#)
- [Build resilience by using Continuous Access Evaluation \(CAE\)](#)
- [Build resilience in external user authentication](#)
- [Build resilience in your hybrid authentication](#)
- [Build resilience in application access with Application Proxy](#)

Resilience resources for developers

- [Build IAM resilience in your applications](#)
- [Build resilience in your CIAM systems](#)

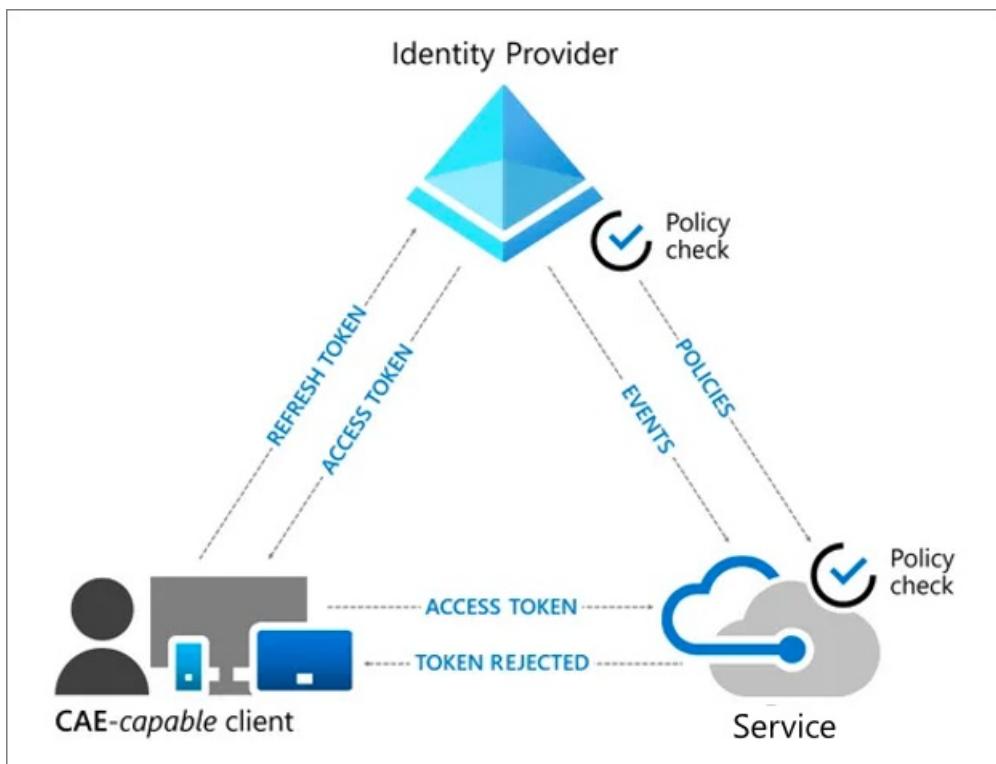
Build resilience by using Continuous Access Evaluation

4/10/2022 • 2 minutes to read • [Edit Online](#)

Continuous Access Evaluation (CAE) allows Azure AD applications to subscribe to critical events that can then be evaluated and enforced. This includes evaluation of the following events:

- The user account being deleted or disabled
- Password for a user is changed
- MFA is enabled for the user.
- Administrator explicitly revokes a token.
- Elevated user risk is detected.

As a result, applications can reject unexpired tokens based on the events signaled by Azure AD, as depicted in the following diagram.



How does CAE help?

This mechanism allows Azure AD to issue longer-lived tokens, while enabling applications a way to revoke access and force re-authentication only when needed. The net result of this pattern is fewer calls to acquire tokens, which means that the end-to-end flow is more resilient.

To use CAE, both the service and the client must be CAE-capable. Microsoft 365 services such as Exchange Online, Teams, and SharePoint Online support CAE. On the client side, browser-based experiences that use these Office 365 services (e.g. Outlook Web App) and specific versions of Office 365 native clients are CAE-capable. More Microsoft cloud services will become CAE-capable.

Microsoft is working with the industry to build standards that will allow third party applications to use this capability. You can also develop applications that are CAE-capable. See How to build resilience in your application for more information.

How do I implement CAE?

- [Update your code to use CAE-enabled APIs.](#)
- [Enable CAE in the Azure AD Security Configuration.](#)
- Ensure that your organization is using [compatible versions](#) of Microsoft Office native applications.
- [Optimize your reauthentication prompts.](#)

Next steps

Resilience resources for administrators and architects

- [Build resilience with credential management](#)
- [Build resilience with device states](#)
- [Build resilience in external user authentication](#)
- [Build resilience in your hybrid authentication](#)
- [Build resilience in application access with Application Proxy](#)

Resilience resources for developers

- [Build IAM resilience in your applications](#)
- [Build resilience in your CIAM systems](#)

Build resilience in external user authentication

4/10/2022 • 2 minutes to read • [Edit Online](#)

[Azure Active Directory B2B collaboration](#) (Azure AD B2B) is a feature of [External Identities](#) that enables collaboration with other organizations and individuals. It enables the secure onboarding of guest users into your Azure AD tenant without having to manage their credentials. External users bring their identity and credentials with them from an external identity provider (IdP), so they don't have to remember a new credential.

Ways to authenticate external users

You can choose the methods of external user authentication to your directory. You can use Microsoft IdPs or other IdPs.

With every external IdP, you take a dependency on the availability of that IdP. With some methods of connecting to IdPs, there are things you can do to increase your resilience.

NOTE

Azure AD B2B has the built-in ability to authenticate any user from any [Azure Active Directory](#) tenant, or with a personal [Microsoft Account](#). You do not have to do any configuration with these built-in options.

Considerations for resilience with other IdPs

When using external IdPs for guest user authentication, there are certain configurations that you must ensure you maintain to prevent disruptions.

AUTHENTICATION METHOD	RESILIENCE CONSIDERATIONS
Federation with social IdPs like Facebook or Google .	You must maintain your account with the IdP and configure your Client ID and Client Secret.
Direct Federation with SAML and WS-Federation Identity Providers	You must collaborate with the IdP owner for access to their endpoints, upon which you're dependent. You must maintain the metadata that contain the certificates and endpoints.
Email one-time passcode	With this method you're dependent on Microsoft's email system, the user's email system, and the user's email client.

Self-service sign-up (preview)

As an alternative to sending invitations or links, you can enable [Self-service sign-up](#). This allows external users to request access to an application. You must create an [API connector](#) and associate it with a user flow. You associate user flows that define the user experience with one or more applications.

It's possible to use [API connectors](#) to integrate your self-service sign-up user flow with external systems' APIs. This API integration can be used for [custom approval workflows](#), [performing identity verification](#), and other tasks such as overwriting user attributes. Using APIs requires that you manage the following dependencies.

- **API Connector Authentication:** Setting up a connector requires an endpoint URL, a username, and a password. Set up a process by which these credentials are maintained, and work with the API owner to ensure you know any expiration schedule.

- **API Connector Response:** Design API Connectors in the sign-up flow to fail gracefully if the API isn't available. Examine and provide to your API developers these [example API responses](#) and the [best practices for troubleshooting](#). Work with the API development team to test all possible response scenarios, including continuation, validation-error, and blocking responses.

Next steps

Resilience resources for administrators and architects

- [Build resilience with credential management](#)
- [Build resilience with device states](#)
- [Build resilience by using Continuous Access Evaluation \(CAE\)](#)
- [Build resilience in your hybrid authentication](#)
- [Build resilience in application access with Application Proxy](#)

Resilience resources for developers

- [Build IAM resilience in your applications](#)
- [Build resilience in your CIAM systems](#)

Build resilience in your hybrid architecture

4/10/2022 • 3 minutes to read • [Edit Online](#)

Hybrid authentication allows users to access cloud-based resources with their identities mastered on-premises. A hybrid infrastructure includes both cloud and on-premises components.

- Cloud components include Azure AD, Azure resources and services, your organization's cloud-based apps, and SaaS applications.
- On-premises components include on-premises applications, resources like SQL databases, and an identity provider like Windows Server Active Directory.

IMPORTANT

As you plan for resilience in your hybrid infrastructure, it's key to minimize dependencies and single points of failure.

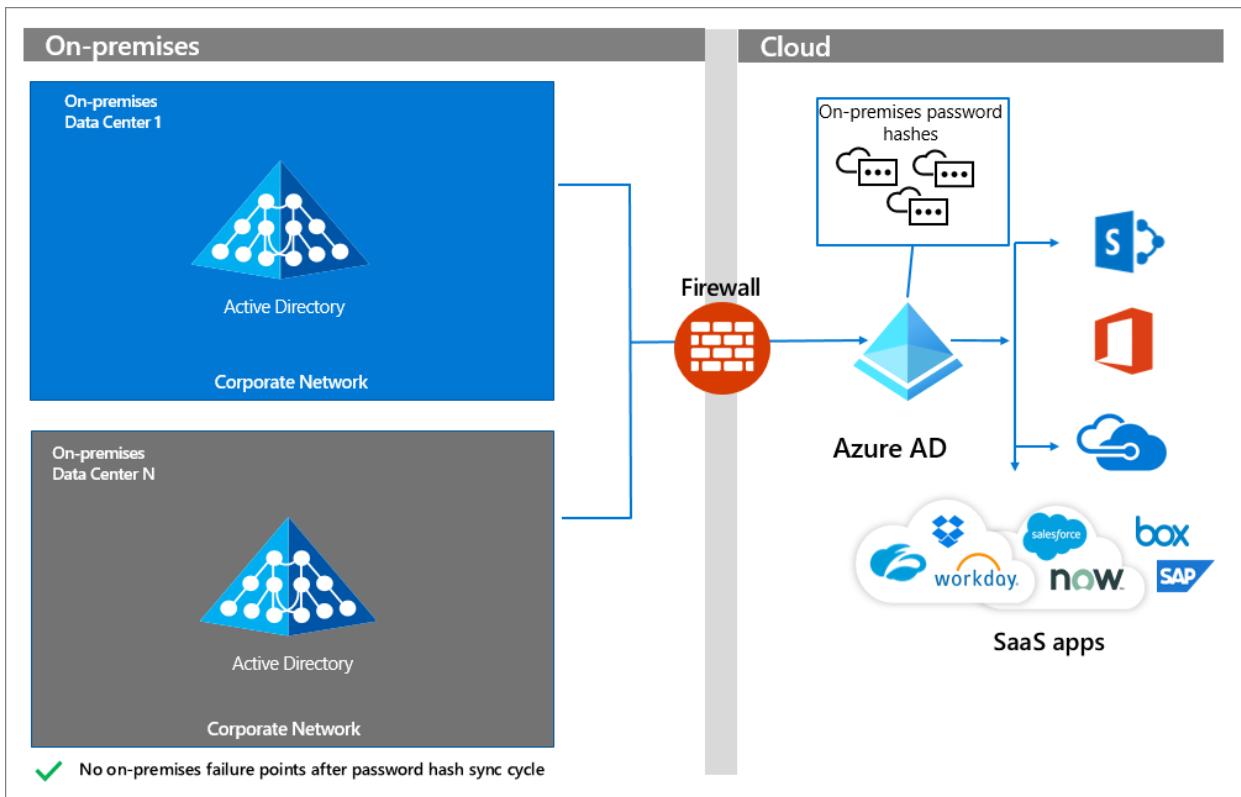
Microsoft offers three mechanisms for hybrid authentication. The options are listed in order of resilience. We recommend that you implement password hash synchronization if possible.

- [Password hash synchronization](#) (PHS) uses Azure AD Connect to sync the identity and a hash of the hash of the password to Azure AD, enabling users to sign-in to cloud-based resources with their password mastered on-premises. PHS has on-premises dependencies only for synchronization, not for authentication.
- [Pass-through Authentication](#) (PTA) redirects users to Azure AD for sign-in. Then, the username and password are validated against Active Directory on premises, through an agent that is deployed in the corporate network. PTA has an on-premises footprint of its Azure AD PTA agents that reside on servers on-premises.
- [Federation](#) customers deploy a federation service such as AD FS, and then Azure AD validates the SAML assertion produced by the federation service. Federation has the highest dependency on on-premises infrastructure, and therefore more failure points.

You may be using one or more of these methods in your organization. For more information, see [Choose the right authentication method for your Azure AD hybrid identity solution](#). This article contains a decision tree that can help you decide on your methodology.

Password hash synchronization

The simplest and most resilient hybrid authentication option for Azure AD is [Password Hash Synchronization](#) which does not have any on-premises identity infrastructure dependency when processing authentication requests. Once identities with password hashes are synchronized to Azure AD, users can authenticate to cloud resources with no dependency on the on-premises identity components.



If you choose this authentication option, you will not experience disruption when on-premises identity components become unavailable. On-premises disruption can occur for many reasons, including hardware failure, power outages, natural disasters, and malware attacks.

How do I implement PHS?

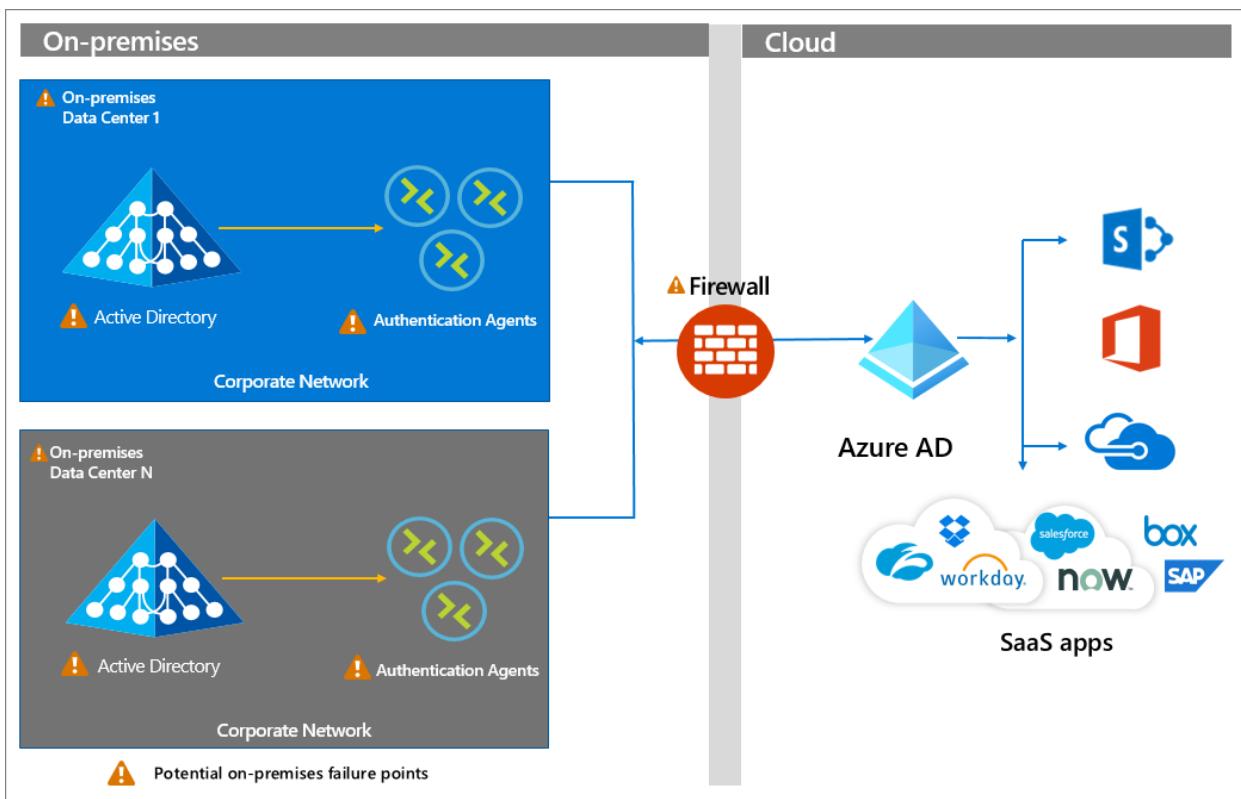
To implement PHS, see the following resources:

- [Implement password hash synchronization with Azure AD Connect](#)
- [Enable password hash synchronization](#)

If your requirements are such that you cannot use PHS, use Pass-through Authentication.

Pass-through Authentication

Pass-through Authentication has a dependency on authentication agents that reside on-premises on servers. A persistent connection, or service bus, is present between Azure AD and the on-premises PTA agents. The firewall, servers hosting the authentication agents, and the on-premises Windows Server Active Directory (or other identity provider) are all potential failure points.



How do I implement PTA?

To implement Pass-through Authentication, see the following resources.

- [How Pass-through Authentication works](#)
- [Pass-through Authentication security deep dive](#)
- [Install Azure AD Pass-through Authentication](#)
- If you are using PTA, define a [highly available topology](#).

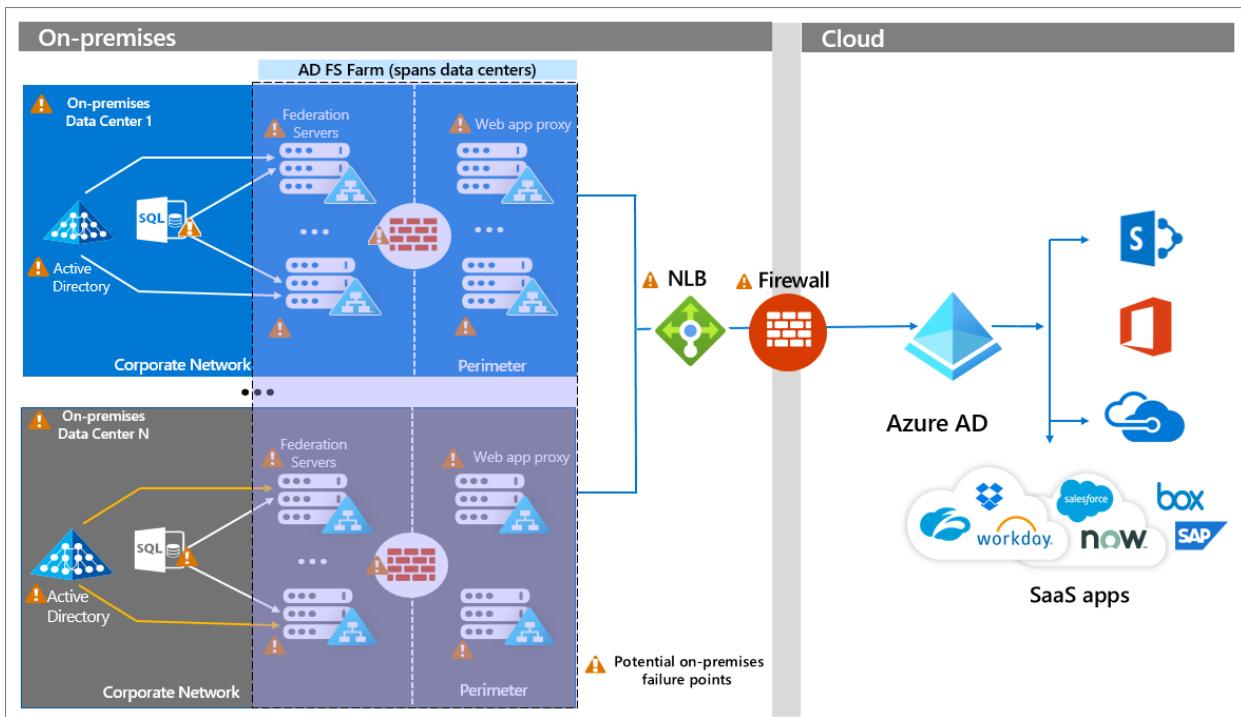
Federation

Federation involves the creation of a trust relationship between Azure AD and the federation service, which includes the exchange of endpoints, token signing certificates, and other metadata. When a request comes to Azure AD, it reads the configuration and redirects the user to the endpoints configured. At that point, the user interacts with the federation service, which issues a SAML assertion that is validated by Azure AD.

The following diagram shows a topology of an enterprise Active Directory Federation Services (AD FS), deployment that includes redundant federation and web application proxy servers across multiple on-premises data centers. This configuration relies on enterprise networking infrastructure components like DNS, Network Load Balancing with geo-affinity capabilities, firewalls, etc. All on-premises components and connections are susceptible to failure. Visit the [AD FS Capacity Planning Documentation](#) for more information.

NOTE

Federation has the highest number of on-premises dependencies, and therefore the most potential points of failure. While this diagram shows AD FS, other on-premises identity providers are subject to similar design considerations to achieve high availability, scalability, and fail over.



How do I implement federation?

If you are implementing a federated authentication strategy or want to make it more resilient, see the following resources.

- [What is federated authentication](#)
- [How federation works](#)
- [Azure AD federation compatibility list](#)
- Follow the [AD FS capacity planning documentation](#)
- [Deploying AD FS in Azure IaaS](#)
- [Enable PHS along with your federation](#)

Next steps

Resilience resources for administrators and architects

- [Build resilience with credential management](#)
- [Build resilience with device states](#)
- [Build resilience by using Continuous Access Evaluation \(CAE\)](#)
- [Build resilience in external user authentication](#)
- [Build resilience in application access with Application Proxy](#)

Resilience resources for developers

- [Build IAM resilience in your applications](#)
- [Build resilience in your CIAM systems](#)

Build resilience in application access with Application Proxy

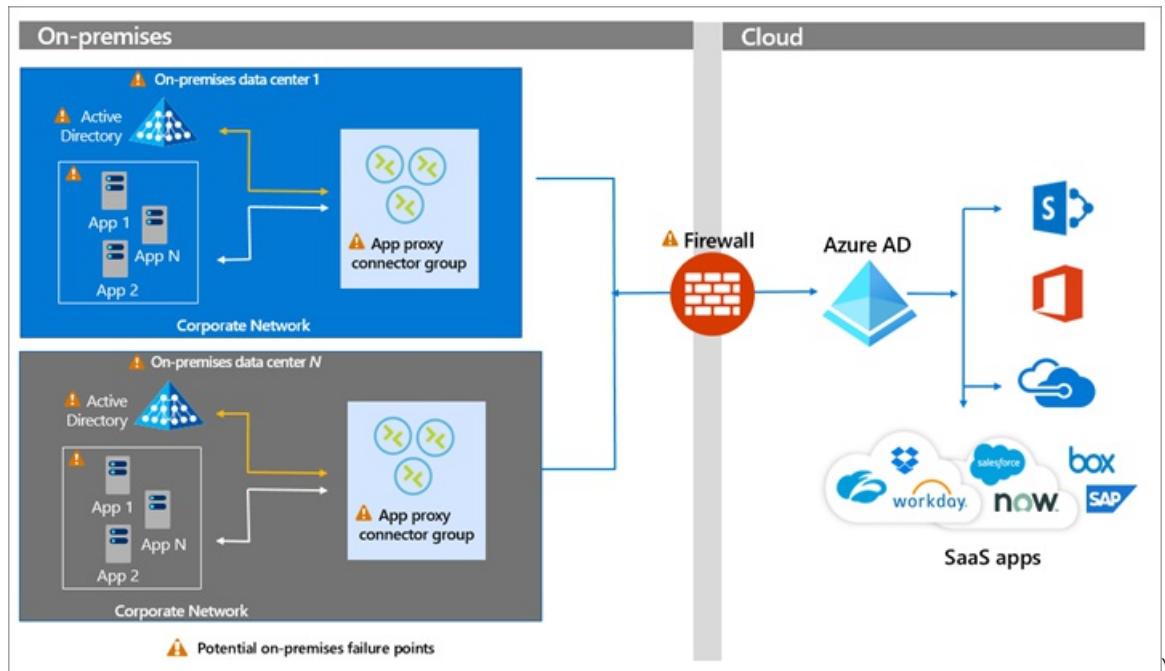
4/10/2022 • 2 minutes to read • [Edit Online](#)

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service in the cloud, and the Application Proxy connectors, which run on an on-premises server.

Users access on-premises resources through a URL published via Application Proxy. They are redirected to the Azure AD sign in page. The Application Proxy service in Azure AD then sends a token to the Application Proxy connector in the corporate network, which passes the token to the on-premises Active Directory. The authenticated user can then access the on-premises resource. In the diagram below, [connectors](#) are shown in a [connector group](#).

IMPORTANT

When you publish your applications via Application Proxy, you must implement [capacity planning and appropriate redundancy for the Application Proxy connectors](#).



How do I implement Application Proxy?

To implement remote access with Azure AD Application Proxy, see the following resources.

- [Planning an Application Proxy deployment](#)
- [High availability and load balancing best practices](#)
- [Configure proxy servers](#)
- [Design a resilient access control strategy](#)

Next steps

Resilience resources for administrators and architects

- [Build resilience with credential management](#)
- [Build resilience with device states](#)
- [Build resilience by using Continuous Access Evaluation \(CAE\)](#)
- [Build resilience in external user authentication](#)
- [Build resilience in your hybrid authentication](#)

Resilience resources for developers

- [Build IAM resilience in your applications](#)
- [Build resilience in your CIAM systems](#)

Build resilience in your customer identity and access management with Azure Active Directory B2C

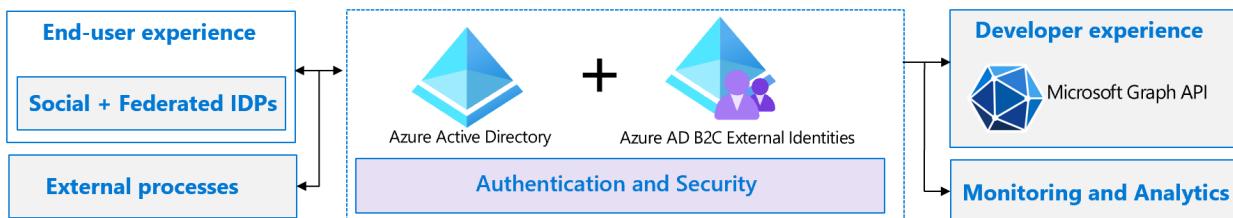
4/10/2022 • 2 minutes to read • [Edit Online](#)

Azure Active Directory (AD) B2C is a Customer Identity and Access Management (CIAM) platform that is designed to help you launch your critical customer facing applications successfully. We have many built-in features for [resilience](#) that are designed to help our service scale to your needs and improve resilience in the face of potential outage situations. In addition, when launching a mission critical application, it's important to consider various design and configuration elements in your application, as well as how the application is configured within Azure AD B2C to ensure that you get a resilient behavior in response to outage or failure scenarios. In this article, we'll discuss some of the best practices to help you increase resilience.

A resilient service is one that continues to function despite disruptions. You can help improve resilience in your service by:

- understanding all the components
- eliminating single points of failures
- isolating failing components to limit their impact
- providing redundancy with fast failover mechanisms and recovery paths

As you develop your application, we recommend considering how to [increase resilience of authentication and authorization in your applications](#) with the identity components of your solution. This article attempts to address enhancements for resilience specific to Azure AD B2C applications. Our recommendations are grouped by CIAM functions.



In the subsequent sections, we'll guide you to build resilience in the following areas:

- **End-user experience:** Enable a fallback plan for your authentication flow and mitigate the potential impact from a disruption of Azure AD B2C authentication service.
- **Interfaces with external processes:** Build resilience in your applications and interfaces by recovering from errors.
- **Developer best practices:** Avoid fragility because of common custom policy issues and improve error handling in the areas like interactions with claims verifiers, third-party applications, and REST APIs.
- **Monitoring and analytics:** Assess the health of your service by monitoring key indicators and detect failures and performance disruptions through alerting.
- **Build resilience in your authentication infrastructure**
- **Increase resilience of authentication and authorization in your applications**

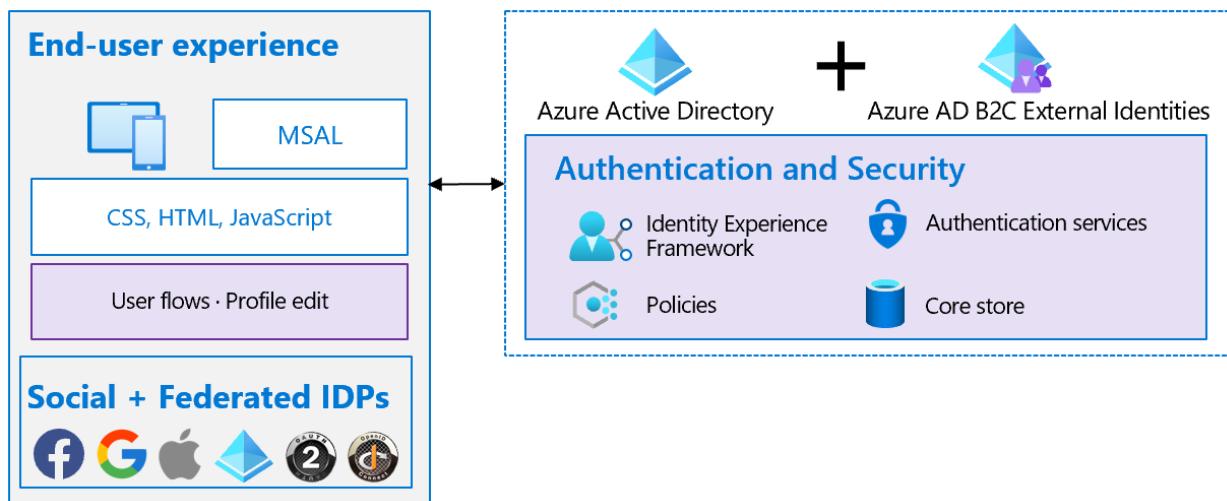
Watch this video to know how to build resilient and scalable flows using Azure AD B2C.

Resilient end-user experience

4/10/2022 • 4 minutes to read • [Edit Online](#)

The sign-up and sign-in end-user experience is made up of the following elements:

- The interfaces the user interacts with – such as CSS, HTML, and JavaScript
- The user flows and custom policies you create – such as sign-up, sign-in, and profile edit
- The identity providers (IDPs) for your application – such as local account username/password, Outlook, Facebook, and Google



Choose between user flow and custom policy

To help you set up the most common identity tasks, Azure AD B2C provides built-in configurable [user flows](#). You can also build your own [custom policies](#), that offers you maximum flexibility. However, it's recommended to use custom policies only to address complex scenarios.

How to decide between user flow and custom policy

Choose built-in user flows if your business requirements can be met by them. Since extensively tested by Microsoft, you can minimize the testing needed for validating policy-level functional, performance, or scale of these identity user flows. You still need to test your applications for functionality, performance, and scale.

Should you [choose custom policies](#) because of your business requirements, make sure you perform policy-level testing for functional, performance, or scale in addition to application-level testing.

See the article that [compares user flows and custom policies](#) to help you decide.

Choose multiple IDPs

When using an [external identity provider](#) such as Facebook, make sure to have a fallback plan in case the external provider becomes unavailable.

How to set up multiple IDPs

As part of the external identity provider registration process, include a verified identity claim such as the user's mobile number or email address. Commit the verified claims to the underlying Azure AD B2C directory instance. If the external provider is unavailable, revert to the verified identity claim, and fall back to the phone number as an authentication method. Another option is to send the user a one-time passcode to allow the user to sign in..

Follow these steps to [build alternate authentication paths](#):

1. Configure your sign-up policy to allow sign up by local account and external IDPs.
2. Configure a profile policy to allow users to [link the other identity to their account](#) after they sign in.
3. Notify and allow users to [switch to an alternate IDP](#) during an outage.

Availability of Multi-factor authentication

When using a [phone service for Multi-factor authentication \(MFA\)](#), make sure to consider an alternative service provider. The local Telco or phone service provider may experience disruptions in their service.

How to choose an alternate MFA

The Azure AD B2C service uses a built-in phone-based MFA provider, to deliver time-based One-time passcodes (OTPs). It is in the form of a voice call and text message to user's pre-registered phone number. The following alternative methods are available for various scenarios:

When using **user flows**, there are two methods to build resilience:

- **Change user flow configuration:** Upon detecting a disruption in the phone-based OTP delivery, change the OTP delivery method from phone-based to email-based and redeploy the user flow, leaving the applications unchanged.

The screenshot shows the 'Create' blade for 'Sign up and sign in (Recommended)'. It includes a note about the new Ocean Blue template. Under '3. Multifactor authentication', it says: 'Enabling multifactor authentication (MFA) requires your users to verify their identity with a second factor before allowing them into your application. [Learn more about multifactor authentication](#)'. There are two sections: 'MFA method' (radio buttons for 'SMS or phone call' and 'Email') and 'MFA enforcement' (radio buttons for 'Conditional (Recommended)' and 'Always on'). A note below 'MFA enforcement' states: 'Conditional delegates the MFA decision to conditional access policies. When conditional is selected, MFA will be OFF unless a conditional access policy requires it.'

- **Change applications:** For each identity task such as sign-up and sign-in, define two sets of user flows. Configure first set to use phone-based OTP and the second to email-based OTP. Upon detecting a disruption in the phone-based OTP delivery, change and redeploy the applications to switch from the first set of user flows to the second, leaving the user flows unchanged.

When using **custom policies**, there are four methods to build resilience. Below list is in the order of complexity and you'll need to redeploy updated policies.

- **Enable user selection of either phone-based OTP or email-based OTP:** Expose both options to the users and enable users to self-select one of the options. There is no need to make changes to the policies or applications.
- **Dynamically switch between phone-based OTP and email-based OTP:** Collect both phone and email information at sign-up. Define custom policy in advance to conditionally switch during a phone disruption, from phone-based to email-based OTP delivery. There is no need to make changes to the policies or applications.
- **Use an Authenticator app:** Update custom policy to use an [Authenticator app](#). If your normal MFA is either phone-based or email-based OTP, then redeploy your custom policies to switch to use the Authenticator app.

NOTE

Users need to configure Authenticator app integration during the sign-up.

- **Use Security Questions:** If none of the above methods are applicable, implement Security Questions as a backup. Set up Security Questions for users during onboarding or profile edit and store the answers in a separate database other than the directory. This method doesn't meet the MFA requirement of "something you have" for example, phone, but offers a secondary "something that you know".

Use a content delivery network

Content delivery networks (CDNs) are better performant and less expensive than blob stores for storage of custom user flow UI. The web page content is delivered faster from a geographically distributed network of highly available servers.

Periodically test your CDN's availability and the performance of content distribution through end-to-end scenario and load testing. If you're planning for an upcoming surge because of promotion or holiday traffic, revise your estimates for load testing.

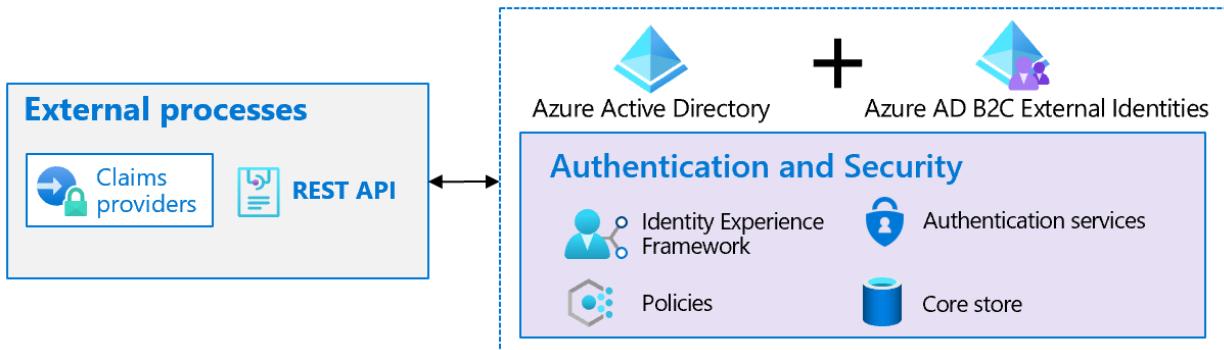
Next steps

- [Resilience resources for Azure AD B2C developers](#)
 - Resilient interfaces with external processes
 - Resilience through developer best practices
 - Resilience through monitoring and analytics
- [Build resilience in your authentication infrastructure](#)
- [Increase resilience of authentication and authorization in your applications](#)

Resilient interfaces with external processes

4/10/2022 • 3 minutes to read • [Edit Online](#)

In this article, we provide you guidance on how to plan for and implement the RESTful APIs in the user journey and make your application more resilient to API failures.



Ensure correct placement of the APIs

Identity experience framework (IEF) policies allow you to call an external system using a [RESTful API technical profile](#). External systems are not controlled by the IEF runtime environment and are a potential failure point.

How to manage external systems using APIs

- While calling an interface to access certain data, check whether the data is going to drive the authentication decision. Assess whether the information is essential to the core functionality of the application. For example, an e-commerce vs. a secondary functionality such as an administration. If the information isn't needed for authentication and only required for secondary scenarios, then consider moving the call to the application logic.
- If the data that is necessary for authentication is relatively static and small, and has no other business reason to be externalized from the directory, then consider having it in the directory.
- Remove API calls from the pre-authenticated path whenever possible. If you can't, then you must place strict protections for Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks in front of your APIs. Attackers can load the sign-in page and try to flood your API with DoS attacks and cripple your application. For example, using CAPTCHA in your sign in, sign up flow can help.
- Use [API connectors of built-in sign-up user flow](#) wherever possible to integrate with web APIs either After federating with an identity provider during sign-up or before creating the user. Since the user flows are already extensively tested, it's likely that you don't have to perform user flow-level functional, performance, or scale testing. You still need to test your applications for functionality, performance, and scale.
- Azure AD RESTful API [technical profiles](#) don't provide any caching behavior. Instead, RESTful API profile implements a retry logic and a timeout that is built into the policy.
- For APIs that need writing data, queue up a task to have such tasks executed by a background worker. Services like [Azure queues](#) can be used. This will make the API return efficiently increasing the policy execution performance.

API error handling

As the APIs live outside the Azure AD B2C system, it's needed to have proper error handling within the technical profile. Make sure the end user is informed appropriately and the application can deal with failure gracefully.

How to gracefully handle API errors

- An API could fail for various reasons, make your application resilient to such failures. [Return an HTTP 4XX error message](#) if the API is unable to complete the request. In the Azure AD B2C policy, try to gracefully handle the unavailability of the API and perhaps render a reduced experience.
- [Handle transient errors gracefully](#). The RESTful API profile allows you to configure error messages for various [circuit breakers](#).
- Proactively monitor and using Continuous Integration/Continuous Delivery (CI/CD), rotate the API access credentials such as passwords and certificates used by the [Technical profile engine](#).

API management - best practices

While you deploy the REST APIs and configure the RESTful technical profile, following the recommended best practices will help you from not making common mistakes and things being overlooked.

How to manage APIs

- API Management (APIM) publishes, manages, and analyzes your APIs. APIM also handles authentication to provide secure access to backend services and microservices. Use an API gateway to scale out API deployments, caching, and load balancing.
- Recommendation is to get the right token at the beginning of the user journey instead of calling multiple times for each API and [secure an Azure APIM API](#).

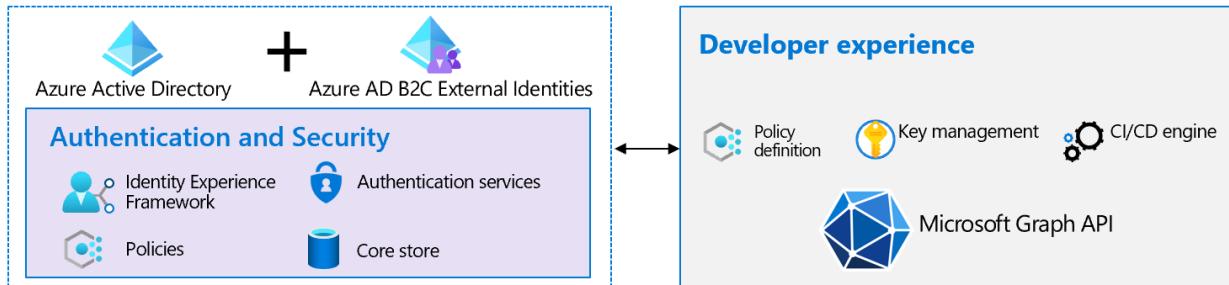
Next steps

- [Resilience resources for Azure AD B2C developers](#)
 - [Resilient end-user experience](#)
 - [Resilience through developer best practices](#)
 - [Resilience through monitoring and analytics](#)
- [Build resilience in your authentication infrastructure](#)
- [Increase resilience of authentication and authorization in your applications](#)

Resilience through developer best practices

4/10/2022 • 7 minutes to read • [Edit Online](#)

In this article, we share some learnings that are based on our experience from working with large customers. You may consider these recommendations in the design and implementation of your services.



Use the Microsoft Authentication Library (MSAL)

The [Microsoft Authentication Library \(MSAL\)](#) and the [Microsoft identity web authentication library for ASP.NET](#) simplify acquiring, managing, caching, and refreshing the tokens an application requires. These libraries are optimized specifically to support Microsoft Identity including features that improve application resiliency.

Developers should adopt latest releases of MSAL and stay up to date. See [how to increase resilience of authentication and authorization](#) in your applications. Where possible, avoid implementing your own authentication stack and use well-established libraries.

Optimize directory reads and writes

The Microsoft Azure AD B2C directory service supports billions of authentications a day. It's designed for a high rate of reads per second. Optimize your writes to minimize dependencies and increase resilience.

How to optimize directory reads and writes

- **Avoid write functions to the directory on sign-in:** Never execute a write on sign-in without a precondition (if clause) in your custom policies. One use case that requires a write on a sign-in is [just-in-time migration of user passwords](#). Avoid any scenario that requires a write on every sign-in.
 - [Preconditions](#) in a user journey will look like this:

```
<Precondition Type="ClaimEquals" ExecuteActionsIf="true">
<Value>requiresMigration</Value>
...
<Precondition/>
```
 - Build resistance to bot-driven [sign-ups by integrating with a CAPTCHA system](#).
 - Use a [load testing sample](#) to simulate sign-up and sign-in.
- **Understand throttling:** The directory implements both application and tenant level throttling rules. There are further rate limits for Read/GET, Write/POST, Update/PUT, and Delete/DELETE operations and each operation have different limits.
 - A write at the time of sign-in will fall under a POST for new users or PUT for existing users.
 - A custom policy that creates or updates a user on every sign-in, can potentially hit an application

level PUT or POST rate limit. The same limits apply when updating directory objects via Azure AD or Microsoft Graph. Similarly, examine the reads to keep the number of reads on every sign-in to the minimum.

- Estimate peak load to predict the rate of directory writes and avoid throttling. Peak traffic estimates should include estimates for actions such as sign-up, sign-in, and Multi-factor authentication (MFA). Be sure to test both the Azure AD B2C system and your application for peak traffic. It's possible that Azure AD B2C can handle the load without throttling, when your downstream applications or services won't.
- Understand and plan your migration timeline. When planning to migrate users to Azure AD B2C using Microsoft Graph, consider the application and tenant limits to calculate the time needed to complete the migration of users. If you split your user creation job or script using two applications, you can use the per application limit. It would still need to remain below the per tenant threshold.
- Understand the effects of your migration job on other applications. Consider the live traffic served by other relying applications to make sure you don't cause throttling at the tenant level and resource starvation for your live application. For more information, see the [Microsoft Graph throttling guidance](#).

Extend token lifetimes

In an unlikely event, when the Azure AD B2C authentication service is unable to complete new sign-ups and sign-ins, you can still provide mitigation for users who are signed in. With [configuration](#), you can allow users that are already signed in to continue using the application without any perceived disruption until the user signs out from the application or the [session](#) times out due to inactivity.

Your business requirements and desired end-user experience will dictate your frequency of token refresh for both web and Single-page applications (SPAs).

How to extend token lifetimes

- **Web applications:** For web applications where the authentication token is validated at the beginning of sign-in, the application depends on the session cookie to continue to extend the session validity.
 - Enable users to remain signed in by implementing rolling session times that will continue to renew sessions based on user activity. If there is a long-term token issuance outage, these session times can be further increased as a onetime configuration on the application. Keep the lifetime of the session to the maximum allowed.
- **SPAs:** A SPA may depend on access tokens to make calls to the APIs. A SPA traditionally uses the implicit flow that doesn't result in a refresh token. The SPA can use a hidden iframe to perform new token requests against the authorization endpoint if the browser still has an active session with the Azure AD B2C. For SPAs, there are a few options available to allow the user to continue to use the application.
 - Extend the access token's validity duration to meet your business requirements.
 - Build your application to use an API gateway as the authentication proxy. In this configuration, the SPA loads without any authentication and the API calls are made to the API gateway. The API gateway sends the user through a sign-in process using an [authorization code grant](#) based on a policy and authenticates the user. Subsequently, the authentication session between the API gateway and the client is maintained using an authentication cookie. The APIs are serviced from the API gateway using the token that is obtained by the API gateway or some other direct authentication method such as certificates, client credentials, or API keys.
 - [Migrate your SPA from implicit grant to authorization code grant flow](#) with Proof Key for Code Exchange (PKCE) and Cross-origin Resource Sharing (CORS) support. Migrate your application from MSAL.js 1.x to MSAL.js 2.x to realize the resiliency of Web applications.

- For mobile applications, it's recommended to extend both the refresh and access token lifetimes.
- **Backend or microservice applications:** Because backend (daemon) applications are non-interactive and aren't in a user context, the prospect of token theft is greatly diminished. Recommendation is to strike a balance between security and lifetime and set a long token lifetime.

Configure Single sign-on

With [Single sign-on \(SSO\)](#), users sign in once with a single account and get access to multiple applications. The application can be a web, mobile, or a Single page application (SPA), regardless of platform or domain name. When the user initially signs in to an application, Azure AD B2C persists a [cookie-based session](#).

Upon subsequent authentication requests, Azure AD B2C reads and validates the cookie-based session and issues an access token without prompting the user to sign in again. If SSO is configured with a limited scope at a policy or an application, later access to other policies and applications will require fresh authentication.

How to configure SSO

[Configure SSO](#) to be tenant-wide (default) to allow multiple applications and user flows in your tenant to share the same user session. Tenant-wide configuration provides most resiliency to fresh authentication.

Safe deployment practices

The most common disrupters of service are the code and configuration changes. Adoption of Continuous Integration and Continuous Delivery (CICD) processes and tools help with rapid deployment at a large scale and reduces human errors during testing and deployment into production. Adopt CICD for error reduction, efficiency, and consistency. [Azure Pipelines](#) is an example of CICD.

Web application firewall

Protect your applications against known vulnerabilities such as Distributed Denial of Service (DDoS) attacks, SQL injections, cross-site scripting, remote code execution, and many others as documented in [OWASP Top 10](#). Deployment of a Web Application Firewall (WAF) can defend against common exploits and vulnerabilities.

- Use Azure [WAF](#), which provides centralized protection against attacks.
- Use WAF with Azure AD [Identity Protection and Conditional Access](#) to provide multi-layer protection when using Azure AD B2C.

Secrets rotation

Azure AD B2C uses secrets for applications, APIs, policies, and encryption. The secrets secure authentication, external interactions, and storage. The National Institute of Standards and Technology (NIST) calls the time span during which a specific key is authorized for use by legitimate entities a cryptoperiod. Choose the right length of [cryptoperiod](#) to meet your business needs. Developers need to manually set the expiration and rotate secrets well in advance of their expiration.

How to implement secret rotation

- Use [managed identities](#) for supported resources to authenticate to any service that supports Azure AD authentication. When you use managed identities, you can manage resources automatically, including rotation of credentials.
- Take an inventory of all the [keys and certificates configured](#) in Azure AD B2C. This list is likely to include keys used in custom policies, [APIs](#), signing ID token, and certificates for SAML.
- Using CICD, rotate secrets that are about to expire within two months from the anticipated peak season. The recommended maximum cryptoperiod of private keys associated to a certificate is one year.

- Proactively monitor and rotate the API access credentials such as passwords, and certificates.

Test REST APIs

In the context of resiliency, testing of REST APIs needs to include verification of – HTTP codes, response payload, headers, and performance. Testing shouldn't include only happy path tests, but also check whether the API handles problem scenarios gracefully.

How to test APIs

We recommend your test plan to include [comprehensive API tests](#). If you're planning for an upcoming surge because of promotion or holiday traffic, you need to revise your load testing with the new estimates. Conduct load testing of your APIs and Content Delivery Network (CDN) in a developer environment and not in production.

Next steps

- [Resilience resources for Azure AD B2C developers](#)
 - Resilient end-user experience
 - Resilient interfaces with external processes
 - Resilience through monitoring and analytics
- [Build resilience in your authentication infrastructure](#)
- [Increase resilience of authentication and authorization in your applications](#)

Resilience through monitoring and analytics

4/10/2022 • 3 minutes to read • [Edit Online](#)

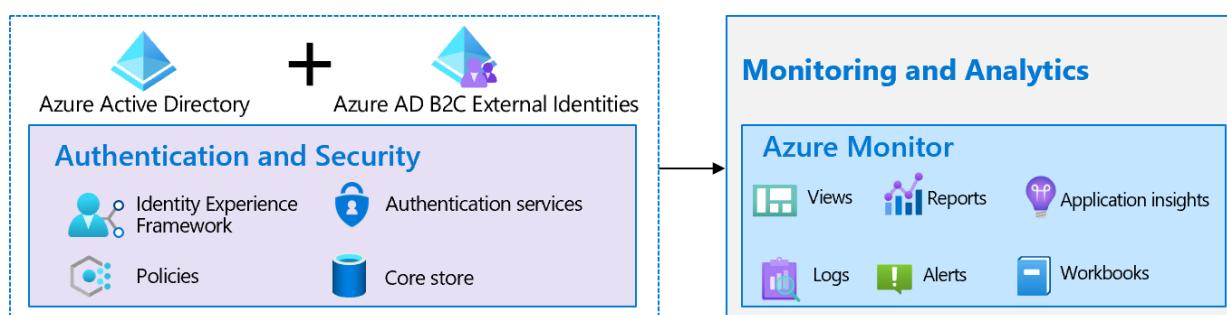
Monitoring maximizes the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your infrastructure and applications. Alerts proactively notify you when issues are found with your service or applications. They allow you to identify and address issues before the end users of your service notice them. [Azure AD Log Analytics](#) helps you analyze, search the audit logs and sign-in logs, and build custom views.

Watch this video to learn how to set up monitoring and reporting in Azure AD B2C using Azure Monitor.

Monitor and get notified through alerts

Monitoring your system and infrastructure is critical to ensure the overall health of your services. It starts with the definition of business metrics, such as, new user arrival, end user's authentication rates, and conversion. Configure such indicators to monitor. If you're planning for an upcoming surge because of promotion or holiday traffic, revise your estimates specifically for the event and corresponding benchmark for the business metrics. After the event, fall back to the previous benchmark.

Similarly, to detect failures or performance disruptions, setting up a good baseline and then defining alerting is an indispensable practice to respond to emerging issues promptly.



How to implement monitoring and alerting

- **Monitoring:** Use [Azure Monitor](#) to continuously monitor health against key Service Level Objectives (SLO) and get notification whenever a critical change happens. Begin by identifying Azure AD B2C policy or an application as a critical component of your business whose health needs to be monitored to maintain SLO. Identify key indicators that align with your SLOs. For example, track the following metrics, since a sudden drop in either will lead to a loss in business.

- **Total requests:** The total "n" number of requests sent to Azure AD B2C policy.
- **Success rate (%):** Successful requests/Total number of requests.

Access the [key indicators in application insights](#) where Azure AD B2C policy-based logs, [audit logs](#), and sign-in logs are stored.

- **Visualizations:** Using Log analytics build dashboards to visually monitor the key indicators.
- **Current period:** Create temporal charts to show changes in the Total requests and Success rate (%) in the current period, for example, current week.
- **Previous period:** Create temporal charts to show changes in the Total requests and Success rate

(%) over some previous period for reference purposes, for example, last week.

- **Alerting:** Using log analytics define [alerts](#) that get triggered when there are sudden changes in the key indicators. These changes may negatively impact the SLOs. Alerts use various forms of notification methods including email, SMS, and webhooks. Start by defining a criterion that acts as a threshold against which alert will be triggered. For example:
 - Alert against abrupt drop in Total requests: Trigger an alert when number of total requests drop abruptly. For example, when there is a 25% drop in the total number of requests compared to previous period, raise an alert.
 - Alert against significant drop in Success rate (%): Trigger an alert when success rate of the selected policy significantly drops.
 - Upon receiving an alert, troubleshoot the issue using [Log Analytics](#), [Application Insights](#), and [VS Code extension](#) for Azure AD B2C. After resolving the issue and deploying an updated application or policy, it continues to monitor the key indicators until they return back to normal range.
- **Service alerts:** Use the [Azure AD B2C service level alerts](#) to get notified of service issues, planned maintenance, health advisory, and security advisory.
- **Reporting:** [By using log analytics](#), build reports that help you gain understanding about user insights, technical challenges, and growth opportunities.
 - **Health Dashboard:** Create [custom dashboards using Azure Dashboard](#) feature, which supports adding charts using Log Analytics queries. For example, identify pattern of successful and failed sign-ins, failure reasons and telemetry about devices used to make the requests.
 - **Abandon Azure AD B2C journeys:** Use the [workbook](#) to track the list of abandoned Azure AD B2C journeys where user started the sign-in or sign-up journey but never finished it. It provides you details about policy ID and breakdown of steps that are taken by the user before abandoning the journey.
 - **Azure AD B2C monitoring workbooks:** Use the [monitoring workbooks](#), which includes Azure AD B2C dashboard, Multi-factor authentication (MFA) operations, Conditional Access report, and Search logs by correlationId, to get better insights into the health of your Azure AD B2C environment.

Next steps

- [Resilience resources for Azure AD B2C developers](#)
 - Resilient end-user experience
 - Resilient interfaces with external processes
 - Resilience through developer best practices
- [Build resilience in your authentication infrastructure](#)
- [Increase resilience of authentication and authorization in your applications](#)

Increase resilience of authentication and authorization applications you develop

4/10/2022 • 2 minutes to read • [Edit Online](#)

Microsoft Identity uses modern, token-based authentication and authorization. This means that a client application acquires tokens from an Identity provider to authenticate the user and to authorize the application to call protected APIs. A service will validate tokens.

A token is valid for a certain length of time before the app must acquire a new one. Rarely, a call to retrieve a token could fail due to an issue like network or infrastructure failure or authentication service outage. In this document, we outline steps a developer can take to increase resilience in their applications if a token acquisition failure occurs.

These articles provide guidance on increasing resiliency in apps using the Microsoft identity platform and Azure Active Directory. There is guidance for both for client and service applications that work on behalf of a signed in user as well as daemon applications that work on their own behalf. They contain best practices for using tokens as well as calling resources.

- [Build resilience into applications that sign-in users](#)
- [Build resilience into applications without users](#)
- [Build resilience in your identity and access management infrastructure](#)
- [Build resilience in your CIAM systems](#)
- [Build services that are resilient to metadata refresh](#)

Increase the resilience of authentication and authorization in client applications you develop

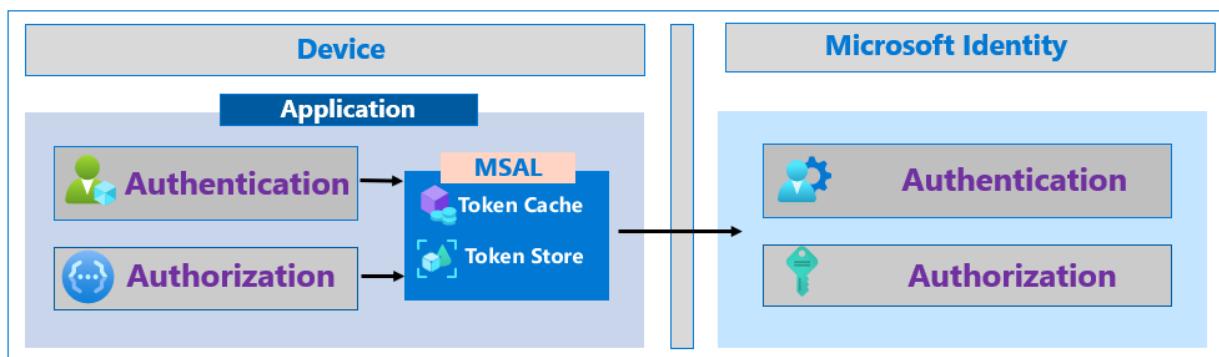
4/10/2022 • 12 minutes to read • [Edit Online](#)

This section provides guidance on building resilience into client applications that use the Microsoft identity platform and Azure Active Directory to sign in users and perform actions on behalf of those users.

Use the Microsoft Authentication Library (MSAL)

The [Microsoft Authentication Library \(MSAL\)](#) is a key part of the [Microsoft identity platform](#). It simplifies and manages acquiring, managing, caching, and refreshing tokens, and uses best practices for resilience. MSAL is designed to enable a secure solution without developers having to worry about the implementation details.

MSAL caches tokens and uses a silent token acquisition pattern. It also automatically serializes the token cache on platforms that natively provide secure storage like Windows UWP, iOS and Android. Developers can customize the serialization behavior when using [Microsoft.Identity.Web](#), [MSAL.NET](#), [MSAL for Java](#), and [MSAL for Python](#).



When using MSAL, token caching, refreshing, and silent acquisition is supported automatically. You can use simple patterns to acquire the tokens necessary for modern authentication. We support many languages, and you can find a sample that matches your language and scenario on our [Samples](#) page.

- [C#](#)
- [JavaScript](#)

```
try
{
    result = await app.AcquireTokenSilent(scopes, account).ExecuteAsync();
}
catch(MsalUiRequiredException ex)
{
    result = await app.AcquireToken(scopes).WithClaims(ex.Claims).ExecuteAsync()
}
```

MSAL can in some cases proactively refresh tokens. When Microsoft Identity issues a long-lived token, it can send information to the client for the optimal time to refresh the token ("refresh_in"). MSAL will proactively refresh the token based on this information. The app will continue to run while the old token is valid but will have a longer timeframe during which to make another successful token acquisition.

Stay up to date

Developers should have a process for updating to the latest MSAL release. Authentication is part of your app security and your app needs to stay current with the security improvements contained in new MSAL releases. This is generally good practice for libraries under continuous development and doing so will ensure you have the most up to date code with respect to app resilience. As Microsoft Identity continues to innovate on ways for applications to be more resilient, apps that use the latest MSAL will be the most prepared to build on these innovations.

[Check the latest MSAL.js version and release notes](#)

[Check the latest MSAL .NET version and release notes](#)

[Check the latest MSAL Python version and release notes](#)

[Check the latest MSAL Java version and release notes](#)

[Check the latest MSAL iOS and macOS version and release notes](#)

[Check the latest MSAL Android version and release notes](#)

[Check the latest MSAL Angular version and release notes](#)

[Check the latest Microsoft.Identity.Web version and release notes](#)

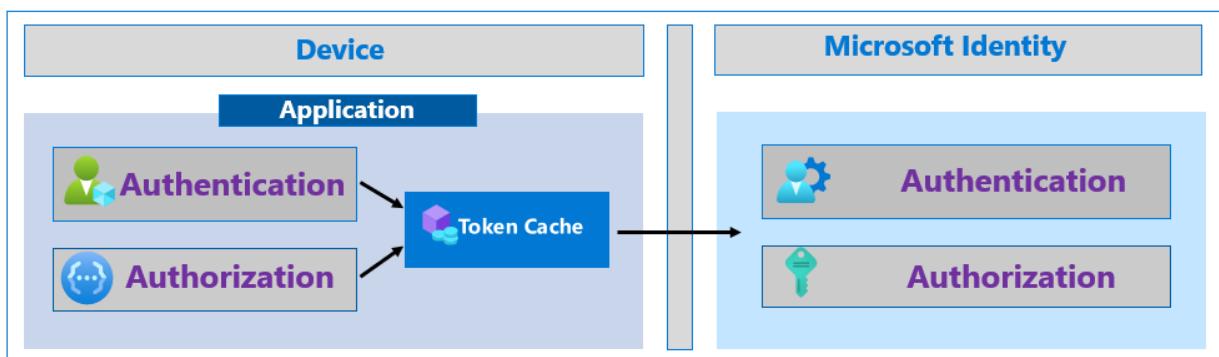
Use resilient patterns for token handling

If you are not using MSAL, you can use these resilient patterns for token handling. These best practices are implemented automatically by the MSAL library.

In general, an application that uses modern authentication will call an endpoint to retrieve tokens that authenticate the user or authorize the application to call protected APIs. MSAL is meant to handle the details of authentication and implements several patterns to improve resilience of this process. Use the guidance in this section to implement best practices if you choose to use a library other than MSAL. If you use MSAL, you get all of these best-practices for free, as MSAL implements them automatically.

Cache tokens

Apps should properly cache tokens received from Microsoft Identity. When your app receives tokens, the HTTP response that contains the tokens also contains an "expires_in" property that tells the application how long to cache, and reuse, the token. It is important that applications use the "expires_in" property to determine the lifespan of the token. Application must never attempt to decode an API access token.

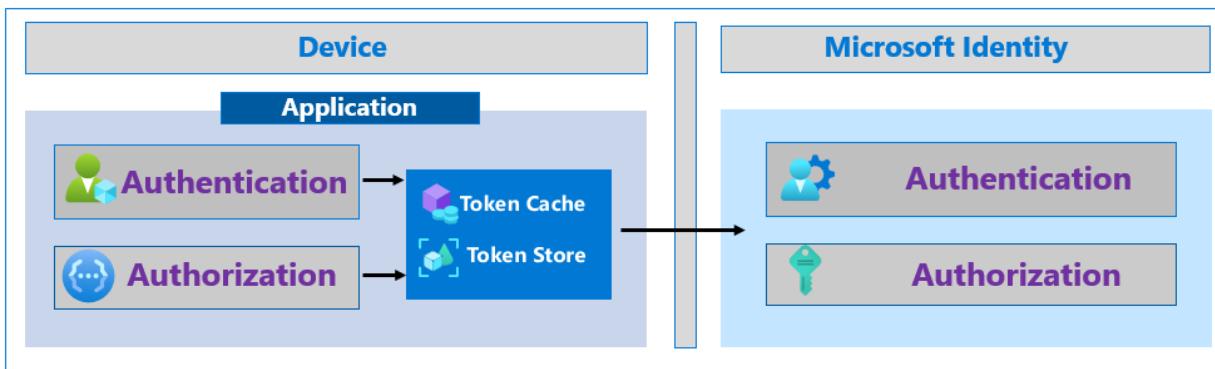


Using the cached token prevents unnecessary traffic between your app and Microsoft Identity, and makes your app less susceptible to token acquisition failures by reducing the number of token acquisition calls. Cached tokens also improve your application's performance as the app needs to block on acquiring tokens less. Your user can stay signed-in to your application for the length of that token's lifetime.

Serialize and persist tokens

Apps should securely serialize their token cache to persist the tokens between instances of the app. Tokens can

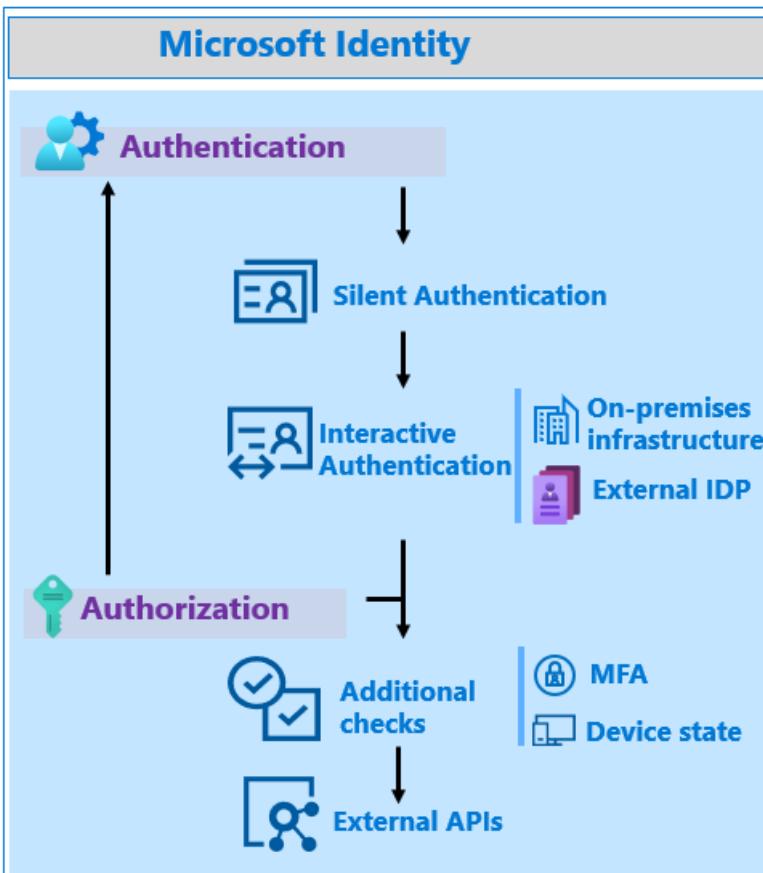
be reused as long as they are within their valid lifetime. [Refresh tokens](#), and, increasingly, [access tokens](#), are issued for many hours. This valid time can span a user starting your application many times. When your app starts, it should check to see if there is a valid access or refresh token that can be used. This will increase the app's resilience and performance as it avoids any unnecessary calls to Microsoft Identity.



The persistent token storage should be access controlled and encrypted to the owning user or process identity. On platforms like mobile, Windows and Mac, the developer should take advantage of built-in capabilities for storing credentials.

Acquire tokens silently

The process of authenticating a user or retrieving authorization to call an API can require multiple steps in Microsoft Identity. For example, when the user signs in for the first time they may need to enter credentials and perform a multi-factor authentication via a text message. Each step adds a dependency on the resource that provides that service. The best experience for the user, and the one with the least dependencies, is to attempt to acquire a token silently to avoid these extra steps before requesting user interaction.



Acquiring a token silently starts with using a valid token from the app's token cache. If there is no valid token available, the app should attempt to acquire a token using a refresh token, if available, and the token endpoint. If neither of these options is available, the app should acquire a token using the "prompt=none" parameter. This

will use the authorization endpoint, but not show any UI to the user. If the Microsoft Identity can provide a token to the app without interacting with the user, it will. If none of these methods result in a token, then a user will need to re-authenticate interactively.

NOTE

In general, apps should avoid using prompts like "login" and "consent" as they will force user interaction even when no interaction is required.

Handle service responses properly

While applications should handle all error responses, there are some responses that can impact resilience. If your application receives an HTTP 429 response code, Too Many Requests, Microsoft Identity is throttling your requests. If your app continues to make too many requests, it will continue to be throttled preventing your app from receiving tokens. Your application should not attempt to acquire a token again until after the time, in seconds, in the Retry-After response field has passed. Receiving a 429 response is often an indication that the application is not caching and reusing tokens correctly. Developers should review how tokens are cached and reused in the application.

When an application receives an HTTP 5xx response code the app must not enter a fast retry loop. When present, the application should honor the same Retry-After handling as it does for a 429 response. If no Retry-After header is provided by the response, we recommend implementing an exponential back-off retry with the first retry at least 5 seconds after the response.

When a request times out applications should not retry immediately. Implement an exponential back-off retry with the first retry at least 5 seconds after the response.

Evaluate options for retrieving authorization related information

Many applications and APIs need specific information about the user to make authorization decisions. There are a few ways for an application to get this information. Each method has its advantages and disadvantages. Developers should weigh these to determine which strategy is best for resilience in their app.

Tokens

Identity (ID) tokens and access tokens contain standard claims that provide information about the subject. These are documented in [Microsoft identity platform ID tokens](#) and [Microsoft identity platform access tokens](#). If the information your app needs is already in the token, then the most efficient technique for retrieving that data is to use token claims as that will save the overhead of an additional network call to retrieve information separately. Fewer network calls mean higher overall resilience for the application.

NOTE

Some applications call the UserInfo endpoint to retrieve claims about the user that authenticated. The information available in the ID token that your app can receive is a superset of the information it can get from the UserInfo endpoint. Your app should use the ID token to get information about the user instead of calling the UserInfo endpoint.

An app developer can augment standard token claims with [optional claims](#). One common optional claim is [groups](#). There are several ways to add group claims. The "Application Group" option only includes groups assigned to the application. The "All" or "Security groups" options include groups from all apps in the same tenant, which can add many groups to the token. It is important to evaluate the effect in your case, as it can potentially negate the efficiency gained by requesting groups in the token by causing token bloat and even requiring additional calls to get the full list of groups.

Instead of using groups in your token you can instead use and include app roles. Developers can define [app](#)

[roles](#) for their apps and APIs which the customer can manage from their directory using the portal or APIs. IT Pros can then assign roles to different users and groups to control who has access to what content and functionality. When a token is issued for the application or API, the roles assigned to the user will be available in the roles claim in the token. Getting this information directly in a token can save additional APIs calls.

Finally, IT Admins can also add claims based on specific information in a tenant. For example, an enterprise can have an extension to have an enterprise specific User ID.

In all cases, adding information from the directory directly to a token can be efficient and increase the apps resilience by reducing the number of dependencies the app has. On the other hand, it does not address any resilience issues from being unable to acquire a token. You should only add optional claims for the main scenarios of your application. If the app requires information only for the admin functionality, then it is best for the application to obtain that information only as needed.

Microsoft Graph

Microsoft Graph provides a unified API endpoint to access the Microsoft 365 data that describes the patterns of productivity, identity and security in an organization. Applications that use Microsoft Graph can potentially use any of the information across Microsoft 365 for authorization decisions.

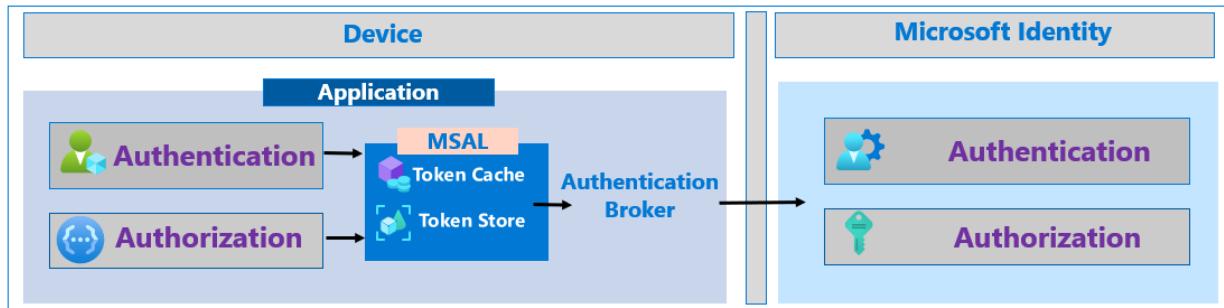
Apps require just a single token to access all of Microsoft 365. This is more resilient than using the older APIs that are specific to Microsoft 365 components like Microsoft Exchange or Microsoft SharePoint where multiple tokens are required.

When using Microsoft Graph APIs, we suggest you use a [Microsoft Graph SDK](#). The Microsoft Graph SDKs are designed to simplify building high-quality, efficient, and resilient applications that access Microsoft Graph.

For authorization decisions, developers should consider when to use the claims available in a token as an alternative to some Microsoft Graph calls. As mentioned above, developers could request groups, app roles, and optional claims in their tokens. In terms of resilience, using Microsoft Graph for authorization requires additional network calls that rely on Microsoft Identity (to get the token to access Microsoft Graph) as well as Microsoft Graph itself. However, if your application already relies on Microsoft Graph as its data layer, then relying on the Graph for authorization is not an additional risk to take.

Use broker authentication on mobile devices

On mobile devices, using an authentication broker like Microsoft Authenticator will improve resilience. The broker adds benefits above what is available with other options such as the system browser or an embedded WebView. The authentication broker can utilize a [primary refresh token](#) (PRT) that contains claims about the user and the device and can be used to get authentication tokens to access other applications from the device. When a PRT is used to request access to an application, its device and MFA claims are trusted by Azure AD. This increases resilience by avoiding additional steps to authenticate the device again. Users won't be challenged with multiple MFA prompts on the same device, therefore increasing resilience by reducing dependencies on external services and improving the user experience.



Broker authentication is automatically supported by MSAL. You can find more information on using brokered authentication on the following pages:

- [Configure SSO on macOS and iOS](#)
- [How to enable cross-app SSO on Android using MSAL](#)

Adopt Continuous Access Evaluation

Continuous Access Evaluation (CAE) is a recent development that can increase application security and resilience with long-lived tokens. CAE is an emerging industry standard being developed in the Shared Signals and Events Working Group of the OpenID Foundation. With CAE, an access token can be revoked based on [critical events](#) and [policy evaluation](#), rather than relying on a short token lifetime. For some resource APIs, because risk and policy are evaluated in real time, CAE can substantially increase token lifetime up to 28 hours. As resource APIs and applications adopt CAE, Microsoft Identity will be able to issue access tokens that are revocable and are valid for extended periods of time. These long-lived tokens will be proactively refreshed by MSAL.

While CAE is in early phases, it is possible to [develop client applications today that will benefit from CAE](#) when the resources (APIs) the application uses adopt CAE. As more resources adopt CAE, your application will be able to acquire CAE enabled tokens for those resources as well. The Microsoft Graph API, and [Microsoft Graph SDKs](#), will preview CAE capability early 2021. If you would like to participate in the public preview of Microsoft Graph with CAE, you can let us know you are interested here: <https://aka.ms/GraphCAEPreview>.

If you develop resource APIs, we encourage you to participate in the [Shared Signals and Events WG](#). We are working with this group to enable the sharing of security events between Microsoft Identity and resource providers.

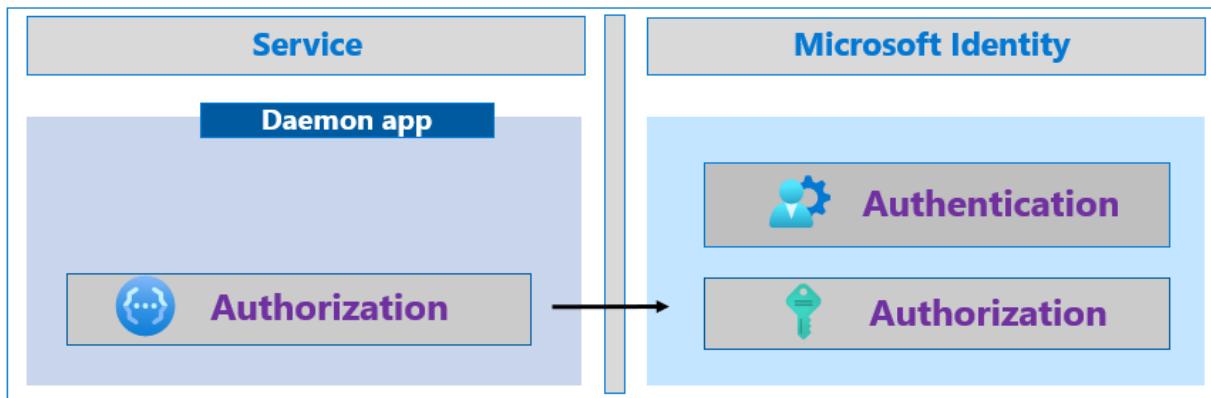
Next steps

- [How to use Continuous Access Evaluation enabled APIs in your applications](#)
- [Build resilience into daemon applications](#)
- [Build resilience in your identity and access management infrastructure](#)
- [Build resilience in your CIAM systems](#)

Increase the resilience of authentication and authorization in daemon applications you develop

4/10/2022 • 3 minutes to read • [Edit Online](#)

This article provides guidance on how developers can use the Microsoft identity platform and Azure Active Directory to increase the resilience of daemon applications. This includes background processes, services, server to server apps, and applications without users.



Use Managed Identities for Azure Resources

Developers building daemon apps on Microsoft Azure can use [Managed Identities for Azure Resources](#). Managed Identities eliminate the need for developers to manage secrets and credentials. The feature improves resilience by avoiding mistakes around certificate expiry, rotation errors, or trust. It also has several built-in features meant specifically to increase resilience.

Managed Identities use long lived access tokens and information from Microsoft Identity to proactively acquire new tokens within a large window of time before the existing token expires. Your app can continue to run while attempting to acquire a new token.

Managed Identities also use regional endpoints to improve performance and resilience against out-of-region failures. Using a regional endpoint helps to keep all traffic inside a geographical area. For example, if your Azure Resource is in WestUS2, all the traffic, including Microsoft Identity generated traffic, should stay in WestUS2. This eliminates possible points of failure by consolidating the dependencies of your service.

Use the Microsoft Authentication Library

Developers of daemon apps who do not use Managed Identities can use the [Microsoft Authentication Library \(MSAL\)](#), which makes implementing authentication and authorization simple, and automatically uses best practices for resilience. MSAL will make the process of providing the required Client Credentials easier. For example, your application does not need to implement creating and signing JSON Web Token assertions when using certificate-based credentials.

Use Microsoft.Identity.Web for .NET Developers

Developers building daemon apps on ASP.NET Core can use the [Microsoft.Identity.Web](#) library. This library is built on top of MSAL to make implementing authorization even easier for ASP.NET Core apps. It includes several [distributed token cache](#) strategies for distributed apps that can run in multiple regions.

Cache and store tokens

If you are not using MSAL to implement authentication and authorization, you can implement some best practices for caching and storing tokens. MSAL implements and follows these best practices automatically.

An application acquires tokens from an Identity provider to authorize the application to call protected APIs. When your app receives tokens, the response that contains the tokens also contains an "expires_in" property that tells the application how long to cache, and reuse, the token. It is important that applications use the "expires_in" property to determine the lifespan of the token. Application must never attempt to decode an API access token. Using the cached token prevents unnecessary traffic between your app and Microsoft Identity. Your user can stay signed-in to your application for the length of that token's lifetime.

Properly handle service responses

Finally, while applications should handle all error responses, there are some responses that can impact resilience. If your application receives an HTTP 429 response code, Too Many Requests, Microsoft Identity is throttling your requests. If your app continues to make too many requests, it will continue to be throttled preventing your app from receiving tokens. Your application should not attempt to acquire a token again until after the time, in seconds, in the "Retry-After" response field has passed. Receiving a 429 response is often an indication that the application is not caching and reusing tokens correctly. Developers should review how tokens are cached and reused in the application.

When an application receives an HTTP 5xx response code the app must not enter a fast retry loop. When present, the application should honor the same "Retry-After" handling as it does for a 429 response. If no "Retry-After" header is provided by the response, we recommend implementing an exponential back-off retry with the first retry at least 5 seconds after the response.

When a request times out applications should not retry immediately. Implement an exponential back-off retry with the first retry at least 5 seconds after the response.

Next steps

- [Build resilience into applications that sign-in users](#)
- [Build resilience in your identity and access management infrastructure](#)
- [Build resilience in your CIAM systems](#)

Build services that are resilient to Azure AD's OpenID Connect metadata refresh

4/10/2022 • 2 minutes to read • [Edit Online](#)

Protected web APIs need to validate access tokens. Web apps also validate the ID tokens. Token Validation has multiple parts, checking whether the token belongs to the application, has been issued by a trusted Identity Provider (IDP), has a lifetime that's still in range and hasn't been tampered with. There can also be special validations. For instance, the app needs to validate the signature and that signing keys (when embedded in a token) are trusted and that the token isn't being replayed. When the signing keys aren't embedded in the token, they need to be fetched from the identity provider (Discovery or Metadata). Sometimes it's also necessary to obtain keys dynamically at runtime.

Web apps and web APIs need to refresh stale OpenID Connect metadata for them to be resilient. This article helps guide on how to achieve resilient apps. It applies to ASP.NET Core, ASP.NET classic, and Microsoft.IdentityModel.

ASP.NET Core

Use latest version of [Microsoft.IdentityModel.*](#) and manually follow the guidelines below.

In the `ConfigureServices` method of the `Startup.cs`, ensure that `JwtBearerOptions.RefreshOnIssuerKeyNotFound` is set to true, and that you're using the latest [Microsoft.IdentityModel.*](#) library. This property should be enabled by default.

```
services.Configure<JwtBearerOptions>(AzureADDefaults.JwtBearerAuthenticationScheme, options =>
{
    ...
    // shouldn't be necessary as it's true by default
    options.RefreshOnIssuerKeyNotFound = true;
    ...
});
```

ASP.NET/ OWIN

Microsoft recommends that you move to ASP.NET Core, as development has stopped on ASP.NET.

If you're using ASP.NET classic, use the latest [Microsoft.IdentityModel.*](#).

OWIN has an automatic 24-hour refresh interval for the `OpenIdConnectConfiguration`. This refresh will only be triggered if a request is received after the 24-hour time span has passed. As far as we know, there's no way to change this value or trigger a refresh early, aside from restarting the application.

Microsoft.IdentityModel

If you validate your token yourself, for instance in an Azure Function, use the latest version of [Microsoft.IdentityModel.*](#) and follow the metadata guidance illustrated by the code snippets below.

```
var configManager =
    new ConfigurationManager<OpenIdConnectConfiguration>(
        "http://someaddress.com",
        new OpenIdConnectConfigurationRetriever());

var config = await configManager.GetConfigurationAsync().ConfigureAwait(false);
var validationParameters = new TokenValidationParameters()
{
    ...
    IssuerSigningKeys = config.SigningKeys;
    ...
};

var tokenHandler = new JsonWebTokenHandler();
result = Handler.ValidateToken(jwtToken, validationParameters);
if (result.Exception != null && result.Exception is SecurityTokenSignatureKeyNotFoundException)
{
    configManager.RequestRefresh();
    config = await configManager.GetConfigurationAsync().ConfigureAwait(false);
    validationParameters = new TokenValidationParameters()
    {
        ...
        IssuerSigningKeys = config.SigningKeys,
        ...
    };
}

// attempt to validate token again after refresh
result = Handler.ValidateToken(jwtToken, validationParameters);
}
```

Next steps

To learn more, see [token validation in a protected web API](#)

Monitoring application sign-in health for resilience

4/10/2022 • 9 minutes to read • [Edit Online](#)

To increase infrastructure resilience, set up monitoring of application sign-in health for your critical applications so that you receive an alert if an impacting incident occurs. To assist you in this effort, you can configure alerts based on the sign-in health workbook.

This workbook enables administrators to monitor authentication requests for applications in your tenant. It provides these key capabilities:

- Configure the workbook to monitor all or individual apps with near real-time data.
- Configure alerts to notify you when authentication patterns change so that you can investigate and take action.
- Compare trends over a period, for example week over week, which is the workbook's default setting.

NOTE

To see all available workbooks, and the prerequisites for using them, please see [How to use Azure Monitor workbooks for reports](#).

During an impacting event, two things may happen:

- The number of sign-ins for an application may drop precipitously because users can't sign in.
- The number of sign-in failures can increase.

This article walks through setting up the sign-in health workbook to monitor for disruptions to your users' sign-ins.

Prerequisites

- An Azure AD tenant.
- A user with global administrator or security administrator role for the Azure AD tenant.
- A Log Analytics workspace in your Azure subscription to send logs to Azure Monitor logs.
 - Learn how to [create a Log Analytics workspace](#)
- Azure AD logs integrated with Azure Monitor logs
 - Learn how to [Integrate Azure AD Sign- in Logs with Azure Monitor Stream](#).

Configure the App sign in health workbook

To access workbooks, open the [Azure portal](#), select **Azure Active Directory**, and then select **Workbooks**.

You'll see workbooks under Usage, Conditional Access, and Troubleshoot. The App sign in health workbook appears in the usage section.

Once you use a workbook, it may appear in the Recently modified workbooks section.

Home > Woodgrove

Woodgrove | Workbooks | Gallery

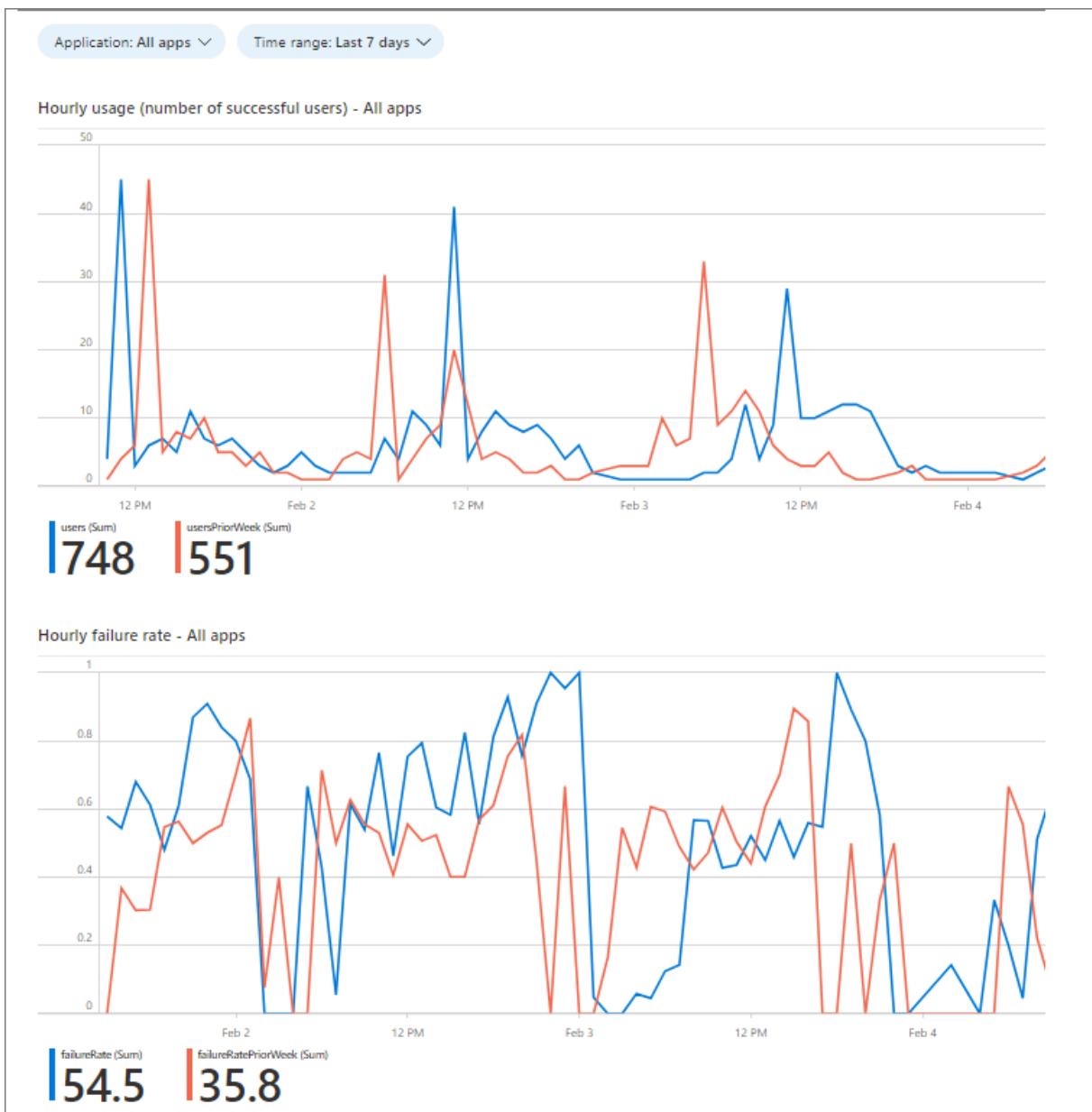
Azure Active Directory

The screenshot shows the Azure Active Directory Workbooks gallery interface. On the left, there's a sidebar with various categories like Identity Governance, Application proxy, Licenses, etc. Below that is a 'Monitoring' section with options like Sign-ins, Audit logs, Provisioning logs (Preview), Logs, Diagnostic settings, and Workbooks (which is currently selected). The main area has a navigation bar with 'New', 'Refresh', 'Feedback', 'Help', 'Community Git repo', and 'Browse across galleries'. Below the navigation is a tabs bar with 'All', 'Workbooks', 'Public Templates' (which is selected and underlined in blue), and 'My Templates'. A search bar contains the text 'App Sign-in'. Underneath, it says '1 Public Templates'. A table lists one template: 'App sign-in health' under the 'Health' category. The table has columns for 'Template name', 'Category', and 'Description'.

Template name	Category	Description
App sign-in health	Health	

The App sign in health workbook enables you to visualize what is happening with your sign-ins.

By default the workbook presents two graphs. These graphs compare what is happening to your app(s) now, versus the same period a week ago. The blue lines are current, and the orange lines are the previous week.



The first graph is **Hourly usage (number of successful users)**. Comparing your current number of successful users to a typical usage period helps you to spot a drop in usage that may require investigation. A drop in successful usage rate can help detect performance and utilization issues that the failure rate can't. For example if users can't reach your application to attempt to sign in, there would be no failures, only a drop in usage. A sample query for this data can be found in the following section.

The second graph is **hourly failure rate**. A spike in failure rate may indicate an issue with your authentication mechanisms. Failure rate can only be measured if users can attempt to authenticate. If users Can't gain access to make the attempt, failures Won't show.

You can configure an alert that notifies a specific group when the usage or failure rate exceeds a specified threshold. A sample query for this data can be found in the following section.

Configure the query and alerts

You create alert rules in Azure Monitor and can automatically run saved queries or custom log searches at regular intervals.

Use the following instructions to create email alerts based on the queries reflected in the graphs. Sample scripts below will send an email notification when

- the successful usage drops by 90% from the same hour two days ago, as in the hourly usage graph in the

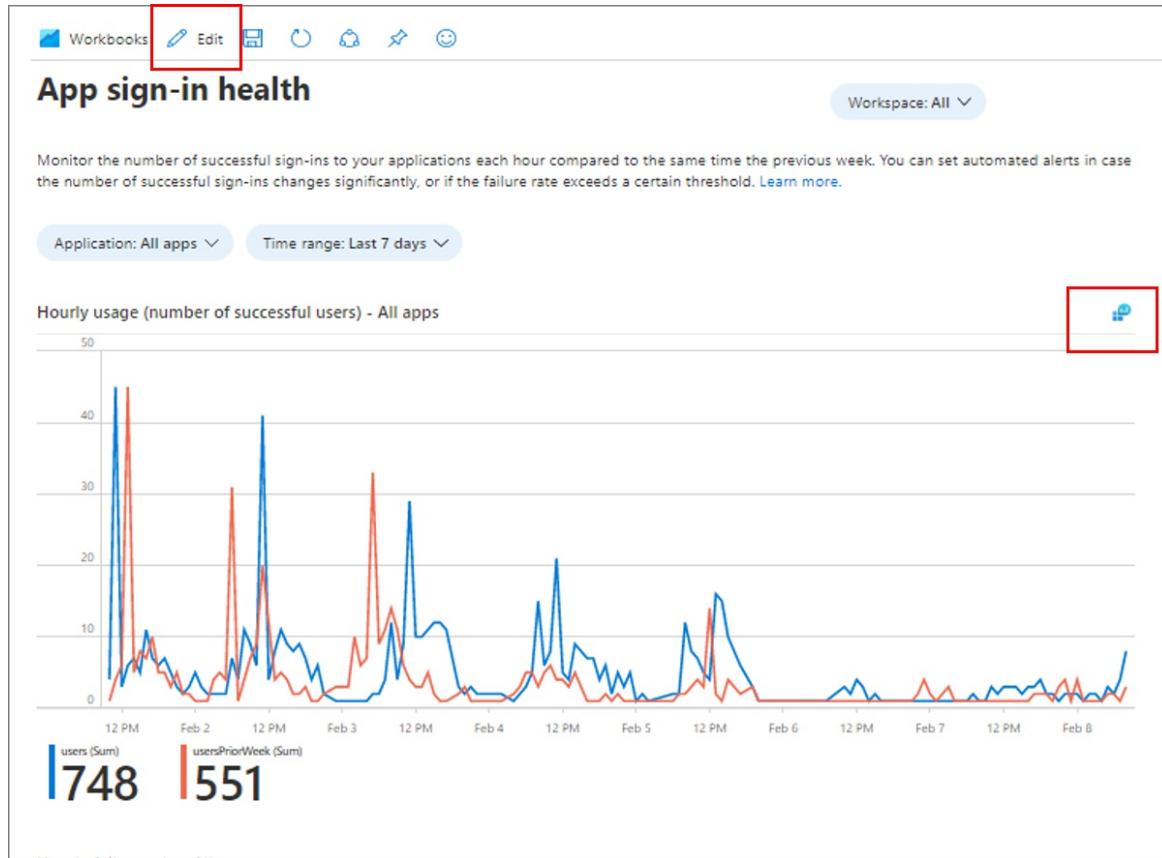
previous section.

- the failure rate increases by 90% from the same hour two days ago, as in the hourly failure rate graph in the previous section.

To configure the underlying query and set alerts, complete the following steps. You'll use the Sample Query as the basis for your configuration. An explanation of the query structure appears at the end of this section.

For more information on how to create, view, and manage log alerts using Azure Monitor see [Manage log alerts](#).

- In the workbook, select **Edit**, then select the **query icon** just above the right-hand side of the graph.



The query log opens.

The screenshot shows the Azure Log Analytics workspace interface. On the left, there's a sidebar with 'Tables', 'Queries', and 'Filter' tabs, along with a search bar and a 'Filter' dropdown. Below these are sections for 'Favorites' (Azure Monitor for VMs, Azure Sentinel, etc.) and 'Completed' queries. A Kusto query is pasted into the main area:

```

1 let thisweek = SigninLogs
2 | where TimeGenerated > ago(7d)
3 | project TimeGenerated, AppDisplayName, UserPrincipalName, status
4 | where Status.ErrorCode == 0
5 | where "All apps" == "All apps" or AppDisplayName has "All apps"
6 | summarize users = dcount(UserPrincipalName) by bin(TimeGenerated, 1hr)
7 | sort by TimeGenerated desc
8 | serialize rn = row_number();
9 let lastweek = SigninLogs
10 | where TimeGenerated between((ago(7d) - totimespan(7d)).(now() - totimespan(7d)))
11 | project TimeGenerated, AppDisplayName, UserPrincipalName, status

```

The results table shows data grouped by TimeGenerated [UTC], users, and usersPriorWeek. The data is as follows:

TimeGenerated [UTC]	users	usersPriorWeek
> 2/8/2021, 4:00:00.000 PM	37	3
> 2/8/2021, 3:00:00.000 PM	4	1
> 2/8/2021, 2:00:00.000 PM	2	2
> 2/8/2021, 1:00:00.000 PM	3	2
> 2/8/2021, 12:00:00.000 PM	1	1
> 2/8/2021, 11:00:00.000 AM	2	1
> 2/8/2021, 10:00:00.000 AM	2	1
> 2/8/2021, 9:00:00.000 AM	1	1
> 2/8/2021, 8:00:00.000 AM	2	4
> 2/8/2021, 7:00:00.000 AM	2	1
> 2/8/2021, 6:00:00.000 AM	2	4
> 2/8/2021, 5:00:00.000 AM	1	3
> 2/8/2021, 4:00:00.000 AM	2	1
> 2/8/2021, 3:00:00.000 AM	2	2
> 2/8/2021, 2:00:00.000 AM	4	2
> 2/8/2021, 1:00:00.000 AM	3	2
> 2/8/2021, 12:00:00.000 AM	3	1

2. Copy one of the sample scripts for a new Kusto query.

- [Kusto query for increase in failure rate](#)
- [Kusto query for drop in usage](#)

3. Paste the query in the window and select **Run**. Ensure you see the Completed message shown in the image below, and results below that message.

The screenshot shows the Azure Log Analytics workspace interface, similar to the previous one but with some UI changes. The Run button is highlighted. The 'Completed' message in the top right is also highlighted with a red box. The rest of the interface and data are identical to the first screenshot.

4. Highlight the query, and select + New alert rule.

```

1 let thisWeek = SigninLogs
2 | where TimeGenerated > ago(7d)
3 | project TimeGenerated, AppDisplayName, UserPrincipalName, Status
4 | where Status.errorCode == 0
5 | where "All apps" == "All apps" or AppDisplayName has "All apps"
6 | summarize users = dcount(UserPrincipalName) by bin(TimeGenerated, 1hr)
7 | sort by TimeGenerated desc
8 | serialize rn = row_number();
9 let lastWeek = SigninLogs
10 | where TimeGenerated between((ago(7d) - totimespan(7d)..(now() - totimespan(7d)))
11 | project TimeGenerated, AppDisplayName, UserPrincipalName, Status

```

5. Configure alert conditions. In the Condition section, select the link **Whenever the average custom log search is greater than logic defined count**. In the configure signal logic pane, scroll to Alert logic

Condition
Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name

Whenever the average custom log search is greater than <logic undefined>

Add condition

You can define only one log signal per alert rule. To alert on more signals, create another

Alert logic

Based on	Operator	Threshold value *
Number of results	Greater than	0

Condition preview
Whenever count of results in **Custom log search** log query for last 2 days is greater than 0. Evaluated every 1 hour.

Evaluated based on

Period (in minutes) *	Frequency (in minutes)
2880	60

Done

- **Threshold value:** 0. This value will alert on any results.
- **Evaluation period (in minutes):** 2880. This value looks at an hour of time
- **Frequency (in minutes):** 60. This value sets the evaluation period to once per hour for the previous hour.
- Select **Done**.

6. In the **Actions** section, configure these settings:

Create alert rule

Rules management

Actions

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group. [Learn more](#)

Action group name	Contains actions
No action group selected yet	
Add action groups	

Customize actions

Email subject ⓘ

Include custom Json payload for webhook ⓘ

Alert rule details

Provide details on your alert rule so that you can identify and manage it later.

Alert rule name *	<input type="text" value="Specify the alert rule name"/>
Description	<input type="text" value="Specify the alert rule description"/>
Save alert rule to resource group *	<input type="text" value="Woodgrove-RG"/>
Severity *	<input type="text" value="Sev 3"/>
Enable alert rule upon creation	<input checked="" type="checkbox"/>
Suppress alerts ⓘ	<input type="checkbox"/>

- Under **Actions**, choose **Select action group**, and add the group you want to be notified of alerts.
- Under **Customize actions** select **Email alerts**.
- Add a **subject line**.

7. Under **Alert rule details**, configure these settings:

- Add a descriptive name and a description.
- Select the **resource group** to which to add the alert.
- Select the default **severity** of the alert.
- Select **Enable alert rule upon creation** if you want it live immediately, else select **Suppress alerts**.

8. Select **Create alert rule**.

9. Select **Save**, enter a name for the query, **Save as a Query with a category of Alert**. Then select **Save** again.

The screenshot shows the Azure Log Analytics workspace interface. At the top, there's a toolbar with various icons like Run, Save, Copy link, New alert rule, Export, Pin to dashboard, and Feedback. A red box highlights the 'Save' button. Below the toolbar, there's a search bar with the placeholder 'Time range : Set in query'. The main area contains a query editor with the following Kusto query:

```

1 let thisWeek = SigninLogs
2 | where TimeGenerated > ago(7d)
3 | project TimeGenerated, AppDisplayName, UserPrincipalName, Status
4 | where Status.errorCode == 0
5 | where "All apps" == "All apps" or AppDisplayName has "All apps"
6 | summarize users = dcountr(UserPrincipalName) by bin(TimeGenerated, 1hr)
7 | sort by TimeGenerated desc
8 | serialize rn = row_number();
9 let lastWeek = SigninLogs
10 | where TimeGenerated between((ago(7d) - totimespan(7d))..(now() - totimespan(7d)))
11 | project TimeGenerated, AppDisplayName, UserPrincipalName, Status ...

```

To the right of the query editor, a 'Save' dialog box is open. It has fields for 'Name' (set to 'Azure AD sign in alerts'), 'Save as' (set to 'Query'), and 'Category' (set to 'Alerts').

Refine your queries and alerts

Modify your queries and alerts for maximum effectiveness.

- Be sure to test your alerts.
- Modify alert sensitivity and frequency so that you get important notifications. Admins can become desensitized to alerts if they get too many and miss something important.
- Ensure the email from which alerts come in your administrator's email clients is added to allowed senders list. Otherwise you may miss notifications due to a spam filter on your email client.
- Alerts query in Azure Monitor can only include results from past 48 hours. [This is a current limitation by design.](#)

Sample scripts

Kusto query for increase in failure rate

The ratio at the bottom can be adjusted as necessary and represents the percent change in traffic in the last hour as compared to the same time yesterday. 0.5 means that there is a 50% difference in the traffic.

```
let today = SigninLogs
| where TimeGenerated > ago(1h) // Query failure rate in the last hour
| project TimeGenerated, UserPrincipalName, AppDisplayName, status = case(Status.errorCode == "0",
"success", "failure")
// Optionally filter by a specific application
//| where AppDisplayName == **APP NAME**
| summarize success = countif(status == "success"), failure = countif(status == "failure") by
bin(TimeGenerated, 1h) // hourly failure rate
| project TimeGenerated, failureRate = (failure * 1.0) / ((failure + success) * 1.0)
| sort by TimeGenerated desc
| serialize lineNumber = row_number();
let yesterday = SigninLogs
| where TimeGenerated between((ago(1h) - totimespan(1d))..(now() - totimespan(1d))) // Query failure rate at
the same time yesterday
| project TimeGenerated, UserPrincipalName, AppDisplayName, status = case(Status.errorCode == "0",
"success", "failure")
// Optionally filter by a specific application
//| where AppDisplayName == **APP NAME**
| summarize success = countif(status == "success"), failure = countif(status == "failure") by
bin(TimeGenerated, 1h) // hourly failure rate at same time yesterday
| project TimeGenerated, failureRateYesterday = (failure * 1.0) / ((failure + success) * 1.0)
| sort by TimeGenerated desc
| serialize lineNumber = row_number();
today
| join (yesterday) on lineNumber // join data from same time today and yesterday
| project TimeGenerated, failureRate, failureRateYesterday
// Set threshold to be the percent difference in failure rate in the last hour as compared to the same time
yesterday
// Day variable is the number of days since the previous Sunday. Optionally ignore results on Sat, Sun, and
Mon because large variability in traffic is expected.
| extend day = dayofweek(now())
| where day != time(6.00:00:00) // exclude Sat
| where day != time(0.00:00:00) // exclude Sun
| where day != time(1.00:00:00) // exclude Mon
| where abs(failureRate - failureRateYesterday) > 0.5
```

Kusto query for drop in usage

In the following query, we are comparing traffic in the last hour to the same time yesterday. We are excluding Saturday, Sunday, and Monday because it's expected on those days that there would be large variability in the

traffic at the same time the previous day.

The ratio at the bottom can be adjusted as necessary and represents the percent change in traffic in the last hour as compared to the same time yesterday. 0.5 means that there is a 50% difference in the traffic.

You should adjust these values to fit your business operation model.

```
let today = SigninLogs // Query traffic in the last hour
| where TimeGenerated > ago(1h)
| project TimeGenerated, AppDisplayName, UserPrincipalName
// Optionally filter by AppDisplayName to scope query to a single application
||| where AppDisplayName contains "Office 365 Exchange Online"
| summarize users = dcount(UserPrincipalName) by bin(TimeGenerated, 1hr) // Count distinct users in the last
hour
| sort by TimeGenerated desc
| serialize rn = row_number();
let yesterday = SigninLogs // Query traffic at the same hour yesterday
| where TimeGenerated between((ago(1h) - totimespan(1d))..(now() - totimespan(1d))) // Count distinct users
in the same hour yesterday
| project TimeGenerated, AppDisplayName, UserPrincipalName
// Optionally filter by AppDisplayName to scope query to a single application
||| where AppDisplayName contains "Office 365 Exchange Online"
| summarize usersYesterday = dcount(UserPrincipalName) by bin(TimeGenerated, 1hr)
| sort by TimeGenerated desc
| serialize rn = row_number();
today
| join // Join data from today and yesterday together
(
yesterday
)
on rn
// Calculate the difference in number of users in the last hour compared to the same time yesterday
| project TimeGenerated, users, usersYesterday, difference = abs(users - usersYesterday), max =
max_of(users, usersYesterday)
| extend ratio = (difference * 1.0) / max // Ratio is the percent difference in traffic in the last hour as
compared to the same time yesterday
// Day variable is the number of days since the previous Sunday. Optionally ignore results on Sat, Sun, and
Mon because large variability in traffic is expected.
| extend day = dayofweek(now())
| where day != time(6.00:00:00) // exclude Sat
| where day != time(0.00:00:00) // exclude Sun
| where day != time(1.00:00:00) // exclude Mon
| where ratio > 0.7 // Threshold percent difference in sign-in traffic as compared to same hour yesterday
```

Create processes to manage alerts

Once you have set up the query and alerts, create business processes to manage the alerts.

- Who will monitor the workbook and when?
- When an alert is generated, who will investigate?
- What are the communication needs? Who will create the communications and who will receive them?
- If an outage occurs, what business processes need to be triggered?

Next steps

[Learn more about workbooks](#)

Certificate authorities used by Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

IMPORTANT

The information in this page is relevant only to entities that explicitly specify a list of acceptable Certificate Authorities (CAs). This practice, known as certificate pinning, should be avoided unless there are no other options.

Any entity trying to access Azure Active Directory (Azure AD) identity services via the TLS/SSL protocols will be presented with certificates from the CAs listed below. If the entity trusts those CAs, it may use the certificates to verify the identity and legitimacy of the identity services and establish secure connections.

Certificate Authorities can be classified into root CAs and intermediate CAs. Typically, root CAs have one or more associated intermediate CAs. This article lists the root CAs used by Azure AD identity services and the intermediate CAs associated with each of those roots. For each CA, we include Uniform Resource Identifiers (URIs) to download the associated Authority Information Access (AIA) and the Certificate Revocation List Distribution Point (CDP) files. When appropriate, we also provide a URI to the Online Certificate Status Protocol (OCSP) endpoint.

CAs used in Azure Public and Azure US Government clouds

Different services may use different root or intermediate CAs. Therefore all entries listed below may be required.

DigiCert Global Root G2

ROOT CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
DigiCert Global Root G2	033af1e6a711a9a0bb2864b11d09fae5	August 1, 2013 January 15, 2038	df3c24f9bfd666761b268073fe06d1cc8d4f82a4	AIA CDP

Associated Intermediate CAs

ISSUING AND INTERMEDIATE CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
Microsoft Azure TLS Issuing CA 01	0aafa6c5ca63c45141ea3be1f7c75317	July 29, 2020 June 27, 2024	2f2877c5d778c31e0f29c7e371df5471bd673173	AIA CDP
Microsoft Azure TLS Issuing CA 02	0c6ae97cced599838690a00a9ea53214	July 29, 2020 June 27, 2024	e7eea674ca718e3befd90858e09f8372ad0ae2aa	AIA CDP
Microsoft Azure TLS Issuing CA 05	0d7bede97d8209967a 52631b8bdd18bd	July 29, 2020 June 27, 2024	6c3af02e7f269aa73afd0eff2a88a4a1f04ed1e5	AIA CDP

ISSUING AND INTERMEDIATE CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
Microsoft Azure TLS Issuing CA 06	02e79171fb8021e93 fe 2d983834c50c0	July 29, 2020 June 27, 2024	30e01761ab97e59a0 6b 41ef20af6f2de7ef4f7 b0	AIA CDP

Baltimore CyberTrust Root

ROOT CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
Baltimore CyberTrust Root	020000b9	May 12, 2000 May 12, 2025	d4de20d05e66fc53fe 1a50882c78db2852c ae474	CDP OCSP

Associated Intermediate CAs

ISSUING AND INTERMEDIATE CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
Microsoft RSA TLS CA 01	703d7a8f0ebf55aaa 59f98eaf4a206004eb 2516a	July 21, 2020 October 8, 2024	417e225037fbfaa4f9 5761d5ae729e1aea7 e3a42	AIA CDP OCSP
Microsoft RSA TLS CA 02	b0c2d2d13cd56cda a 6ab6e2c04440be4a4 29c75	July 21, 2020 May 20, 2024	54d9d20239080c32 316ed 9ff980a48988f4adf2 d	AIA CDP OCSP

DigiCert Global Root CA

ROOT CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
DigiCert Global Root CA	083be056904246 b1a1756ac95991c74 a	November 9, 2006 November 9, 2031	a8985d3a65e5e5c4b 2d7 d66d40c6dd2fb19c5 436	CDP OCSP

Associated Intermediate CAs

ISSUING AND INTERMEDIATE CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
DigiCert SHA2 Secure Server CA	01fda3eb6eca75c 888438b724bcfbc91	March 8, 2013 March 8, 2023	1fb86b1168ec74315 4062 e8c9cc5b171a4b7ccb 4	AIA CDP OCSP
DigiCert SHA2 Secure Server CA	02742eaa17ca8e21 c717bb1ffcf0ca0	September 22, 2020 September 22, 2030	626d44e704d1ceabe 3bf 0d53397464ac8080 142c	AIA CDP OCSP

CAs used in Azure China 21Vianet cloud

DigiCert Global Root CA

ROOT CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
DigiCert Global Root CA	083be056904246b1a1756ac95991c74a	Nov. 9, 2006 Nov. 9, 2031	a8985d3a65e5e5c4b2d7d66d40c6dd2fb19c5436	CDP OCSP

Associated Intermediate CA

ISSUING AND INTERMEDIATE CA	SERIAL NUMBER	ISSUE DATE EXPIRATION DATE	SHA1 THUMBPRINT	URIS
DigiCert Basic RSA CN CA G2	02f7e1f982bad009aff47dc95741b2f6	March 4, 2020 March 4, 2030	4d1fa5d1fb1ac3917c08e43f65015e6aea571179	AIA CDP OCSP

Next Steps

[Learn about Microsoft 365 Encryption chains](#)

Azure Active Directory feature deployment guide

4/10/2022 • 6 minutes to read • [Edit Online](#)

It can seem scary to deploy Azure Active Directory (Azure AD) for your organization and keep it secure. This article identifies common tasks that customers find helpful to complete in phases, over the course of 30, 60, 90 days, or more, to enhance their security posture. Even organizations who have already deployed Azure AD can use this guide to ensure they're getting the most out of their investment.

A well-planned and executed identity infrastructure paves the way for secure access to your productivity workloads and data by known users and devices only.

Additionally customers can check their [identity secure score](#) to see how aligned they're to Microsoft best practices. Check your secure score before and after implementing these recommendations to see how well you're doing compared to others in your industry and to other organizations of your size.

Prerequisites

Many of the recommendations in this guide can be implemented with Azure AD Free or no license at all. Where licenses are required we state which license is required at minimum to accomplish the task.

Additional information about licensing can be found on the following pages:

- [Azure AD licensing](#)
- [Microsoft 365 Enterprise](#)
- [Enterprise Mobility + Security](#)
- [Azure AD External Identities pricing](#)

Phase 1: Build a foundation of security

In this phase, administrators enable baseline security features to create a more secure and easy to use foundation in Azure AD before we import or create normal user accounts. This foundational phase ensures you are in a more secure state from the start and that your end-users only have to be introduced to new concepts one time.

TASK	DETAIL	REQUIRED LICENSE
Create more than one global administrator	Assign at least two cloud-only permanent global administrator accounts for use in an emergency. These accounts aren't to be used daily and should have long and complex passwords.	Azure AD Free
Use non-global administrative roles where possible	Give your administrators only the access they need to only the areas they need access to. Not all administrators need to be global administrators.	Azure AD Free
Enable Privileged Identity Management for tracking admin role use	Enable Privileged Identity Management to start tracking administrative role usage.	Azure AD Premium P2

Task	Detail	Required License
Roll out self-service password reset	Reduce helpdesk calls for password resets by allowing staff to reset their own passwords using policies you as an administrator control.	Azure AD Premium P1
Create an organization specific custom banned password list	Prevent users from creating passwords that include common words or phrases from your organization or area.	Azure AD Premium P1
Enable on-premises integration with Azure AD password protection	Extend the banned password list to your on-premises directory, to ensure passwords set on-premises are also in compliance with the global and tenant-specific banned password lists.	Azure AD Premium P1
Enable Microsoft's password guidance	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.	Azure AD Free
Disable periodic password resets for cloud-based user accounts	Periodic password resets encourage your users to increment their existing passwords. Use the guidelines in Microsoft's password guidance doc and mirror your on-premises policy to cloud-only users.	Azure AD Free
Customize Azure Active Directory smart lockout	Stop lockouts from cloud-based users from being replicated to on-premises Active Directory users	Azure AD Premium P1
Enable Extranet Smart Lockout for AD FS	AD FS extranet lockout protects against brute force password-guessing attacks, while letting valid AD FS users continue to use their accounts.	
Block legacy authentication to Azure AD with Conditional Access	Block legacy authentication protocols like POP, SMTP, IMAP, and MAPI that can't enforce Multi-Factor Authentication, making them a preferred entry point for adversaries.	Azure AD Premium P1
Deploy Azure AD Multi-Factor Authentication using Conditional Access policies	Require users to do two-step verification when accessing sensitive applications using Conditional Access policies.	Azure AD Premium P1
Enable Azure Active Directory Identity Protection	Enable tracking of risky sign-ins and compromised credentials for users in your organization.	Azure AD Premium P2
Use risk detections to trigger multi-factor authentication and password changes	Enable automation that can trigger events such as multi-factor authentication, password reset, and blocking of sign-ins based on risk.	Azure AD Premium P2

Task	Detail	Required License
Enable combined registration for self-service password reset and Azure AD Multi-Factor Authentication	Allow your users to register from one common experience for both Azure AD Multi-Factor Authentication and self-service password reset.	Azure AD Premium P1

Phase 2: Import users, enable synchronization, and manage devices

Next, we add to the foundation laid in phase 1 by importing our users and enabling synchronization, planning for guest access, and preparing to support more functionality.

Task	Detail	Required License
Install Azure AD Connect	Prepare to synchronize users from your existing on-premises directory to the cloud.	Azure AD Free
Implement Password Hash Sync	Synchronize password hashes to allow password changes to be replicated, bad password detection and remediation, and leaked credential reporting.	Azure AD Free
Implement Password Writeback	Allow password changes in the cloud to be written back to an on-premises Windows Server Active Directory environment.	Azure AD Premium P1
Implement Azure AD Connect Health	Enable monitoring of key health statistics for your Azure AD Connect servers, AD FS servers, and domain controllers.	Azure AD Premium P1
Assign licenses to users by group membership in Azure Active Directory	Save time and effort by creating licensing groups that enable or disable features by group instead of setting per user.	Azure AD Premium P1
Create a plan for guest user access	Collaborate with guest users by letting them sign in to your apps and services with their own work, school, or social identities.	Azure AD External Identities pricing
Decide on device management strategy	Decide what your organization allows regarding devices. Registering vs joining, Bring Your Own Device vs company provided.	
Deploy Windows Hello for Business in your organization	Prepare for passwordless authentication using Windows Hello	
Deploy passwordless authentication methods for your users	Provide your users with convenient passwordless authentication methods	Azure AD Premium P1

Phase 3: Manage applications

As we continue to build on the previous phases, we identify candidate applications for migration and integration with Azure AD and complete the setup of those applications.

TASK	DETAIL	REQUIRED LICENSE
Identify your applications	Identify applications in use in your organization: on-premises, SaaS applications in the cloud, and other line-of-business applications. Determine if these applications can and should be managed with Azure AD.	No license required
Integrate supported SaaS applications in the gallery	Azure AD has a gallery that contains thousands of pre-integrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal.	Azure AD Free
Use Application Proxy to integrate on-premises applications	Application Proxy enables users to access on-premises applications by signing in with their Azure AD account.	Azure AD Premium P1

Phase 4: Audit privileged identities, complete an access review, and manage user lifecycle

Phase 4 sees administrators enforcing least privilege principles for administration, completing their first access reviews, and enabling automation of common user lifecycle tasks.

TASK	DETAIL	REQUIRED LICENSE
Enforce the use of Privileged Identity Management	Remove administrative roles from normal day-to-day user accounts. Make administrative users eligible to use their role after succeeding a multi-factor authentication check, providing a business justification, or requesting approval from approvers.	Azure AD Premium P2
Complete an access review for Azure AD directory roles in PIM	Work with your security and leadership teams to create an access review policy to review administrative access based on your organization's policies.	Azure AD Premium P2
Implement dynamic group membership policies	Use dynamic groups to automatically assign users to groups based on their attributes from HR (or your source of truth), such as department, title, region, and other attributes.	Azure AD Premium P1
Implement group based application provisioning	Use group-based access management provisioning to automatically provision users for SaaS applications.	Azure AD Premium P1

TASK	DETAIL	REQUIRED LICENSE
Automate user provisioning and deprovisioning	Remove manual steps from your employee account lifecycle to prevent unauthorized access. Synchronize identities from your source of truth (HR System) to Azure AD.	Azure AD Premium P1

Next steps

[Azure AD licensing and pricing details](#)

[Identity and device access configurations](#)

[Common recommended identity and device access policies](#)

Azure Active Directory deployment plans

4/10/2022 • 5 minutes to read • [Edit Online](#)

Looking for complete guidance on deploying Azure Active Directory (Azure AD) capabilities? Azure AD deployment plans walk you through the business value, planning considerations, and operational procedures needed to successfully deploy common Azure AD capabilities.

From any of the plan pages, use your browser's Print to PDF capability to create an up-to-date offline version of the documentation.

Deploy authentication

CAPABILITY	DESCRIPTION
Azure AD multifactor authentication	Azure AD Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution. Using admin-approved authentication methods, Azure AD MFA helps safeguard access to your data and applications while meeting the demand for a simple sign in process. Watch this video on How to configure and enforce multi-factor authentication in your tenant
Conditional Access	With Conditional Access, you can implement automated access control decisions for who can access your cloud apps, based on conditions.
Self-service password reset	Self-service password reset helps your users reset their passwords without administrator intervention, when and where they need to.
Passwordless	Implement passwordless authentication using the Microsoft Authenticator app or FIDO2 Security keys in your organization

Deploy application and device management

CAPABILITY	DESCRIPTION
Single sign-on	Single sign-on helps your users' access the apps and resources they need to do business while signing in only once. After they've signed in, they can go from Microsoft Office to SalesForce to Box to internal applications without being required to enter credentials a second time.
My Apps	Offer your users a simple hub to discover and access all their applications. Enable them to be more productive with self-service capabilities, like requesting access to apps and groups, or managing access to resources on behalf of others.

CAPABILITY	DESCRIPTION
Devices	This article helps you evaluate the methods to integrate your device with Azure AD, choose the implementation plan, and provides key links to supported device management tools.

Deploy hybrid scenarios

CAPABILITY	DESCRIPTION
AD FS to cloud user authentication	Learn to migrate your user authentication from federation to cloud authentication with either pass through authentication or password hash sync.
Azure AD Application Proxy	Employees today want to be productive at any place, at any time, and from any device. They need to access SaaS apps in the cloud and corporate apps on-premises. Azure AD Application proxy enables this robust access without costly and complex virtual private networks (VPNs) or demilitarized zones (DMZs).
Seamless SSO	Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. With this feature, users won't need to type in their passwords to sign in to Azure AD and usually won't need to enter their usernames. This feature provides authorized users with easy access to your cloud-based applications without needing any extra on-premises components.

Deploy user provisioning

CAPABILITY	DESCRIPTION
User provisioning	Azure AD helps you automate the creation, maintenance, and removal of user identities in cloud (SaaS) applications, such as Dropbox, Salesforce, ServiceNow, and more.
Cloud HR user provisioning	Cloud HR user provisioning to Active Directory creates a foundation for ongoing identity governance and enhances the quality of business processes that rely on authoritative identity data. Using this feature with your cloud HR product, such as Workday or Successfactors, you can seamlessly manage the identity lifecycle of employees and contingent workers by configuring rules that map Joiner-Mover-Leaver processes (such as New Hire, Terminate, Transfer) to IT provisioning actions (such as Create, Enable, Disable)

Deploy governance and reporting

CAPABILITY	DESCRIPTION
------------	-------------

CAPABILITY	DESCRIPTION
Privileged Identity Management	Azure AD Privileged Identity Management (PIM) helps you manage privileged administrative roles across Azure AD, Azure resources, and other Microsoft Online Services. PIM provides solutions like just-in-time access, request approval workflows, and fully integrated access reviews so you can identify, uncover, and prevent malicious activities of privileged roles in real time.
Reporting and Monitoring	The design of your Azure AD reporting and monitoring solution depends on your legal, security, and operational requirements as well as your existing environment and processes. This article presents the various design options and guides you to the right deployment strategy.
Access Reviews	Access Reviews are an important part of your governance strategy, enabling you to know and manage who has access, and to what they have access. This article helps you plan and deploy access reviews to achieve your desired security and collaboration postures.

Include the right stakeholders

When beginning your deployment planning for a new capability, it's important to include key stakeholders across your organization. We recommend that you identify and document the person or people who fulfill each of the following roles, and work with them to determine their involvement in the project.

Roles might include the following

ROLE	DESCRIPTION
End-user	A representative group of users for which the capability will be implemented. Often previews the changes in a pilot program.
IT Support Manager	IT support organization representative who can provide input on the supportability of this change from a helpdesk perspective.
Identity Architect or Azure Global Administrator	Identity management team representative in charge of defining how this change is aligned with the core identity management infrastructure in your organization.
ApplicationBusiness Owner	The overall business owner of the affected application(s), which may include managing access. May also provide input on the user experience and usefulness of this change from an end user's perspective.
SecurityOwner	A representative from the security team that can sign off that the plan will meet the security requirements of your organization.
Compliance Manager	The person within your organization responsible for ensuring compliance with corporate, industry, or governmental requirements.

Levels of involvement might include:

- Responsible for implementing project plan and outcome
- Approval of project plan and outcome
- Contributor to project plan and outcome
- Informed of project plan and outcome

Best practices for a pilot

A pilot allows you to test with a small group before turning on a capability for everyone. Ensure that as part of your testing, each use case within your organization is thoroughly tested. It's best to target a specific group of pilot users before rolling this deployment out to your organization as a whole.

In your first wave, target IT, usability, and other appropriate users who can test and provide feedback. Use this feedback to further develop the communications and instructions you send to your users, and to give insights into the types of issues your support staff may see.

Widening the rollout to larger groups of users should be carried out by increasing the scope of the group(s) targeted. This can be done through [dynamic group membership](#), or by manually adding users to the targeted group(s).

Azure Active Directory B2C deployment plans

4/10/2022 • 9 minutes to read • [Edit Online](#)

Azure Active Directory B2C is a scalable identity and access management solution. Its high flexibility to meet your business expectations and smooth integration with existing infrastructure enables further digitalization.

To help organizations understand the business requirements and respect compliance boundaries, a step-by-step approach is recommended throughout an Azure Active Directory (Azure AD) B2C deployment.

CAPABILITY	DESCRIPTION
Plan	Prepare Azure AD B2C projects for deployment. Start by identifying the stakeholders and later defining a project timeline.
Implement	Start with enabling authentication and authorization and later perform full application onboarding.
Monitor	Enable logging, auditing, and reporting once an Azure AD B2C solution is in place.

Plan an Azure AD B2C deployment

This phase includes the following capabilities:

CAPABILITY	DESCRIPTION
Business requirements review	Assess your organization's status and expectations
Stakeholders	Build your project team
Communication	Communicate with your team about the project
Timeline	Reminder of key project milestones

Business requirements review

- Assess the primary reason to switch off existing systems and [move to Azure AD B2C](#).
- For a new application, [plan and design](#) the Customer Identity Access Management (CIAM) system
- Identify customer's location and [create a tenant in the corresponding datacenter](#).
- Check the type of applications you have
 - Check the platforms that are currently supported - [MSAL](#) or [Open source](#).
 - For backend services, use the [client credentials flow](#).
- If you intend to migrate from an existing Identity Provider (IdP)
 - Consider using the [seamless migration approach](#)
 - Learn [how to migrate the existing applications](#)
 - Ensure the coexistence of multiple solutions at once.

- Decide the protocols you want to use
 - If you're currently using Kerberos, NTLM, and WS-Fed, [migrate and refactor your applications](#). Once migrated, your applications can support modern identity protocols such as OAuth 2.0 and OpenID Connect (OIDC) to enable further identity protection and security.

Stakeholders

When technology projects fail, it's typically because of mismatched expectations on impact, outcomes, and responsibilities. To avoid these pitfalls, [ensure that you're engaging the right stakeholders](#) and that stakeholders understand their roles.

- Identify the primary architect, project manager, and owner for the application.
- Consider providing a Distribution List (DL). Using this DL, you can communicate product issues with the Microsoft account team or engineering. You can ask questions, and receive important notifications.
- Identify a partner or resource outside of your organization who can support you.

Communication

Communication is critical to the success of any new service. Proactively communicate to your users about the change. Timely inform them about how their experience will change, when it will change, and how to gain support if they experience issues.

Timeline

Define clear expectations and follow up plans to meet key milestones:

- Expected pilot date
- Expected launch date
- Any dates that may affect project delivery date

Implement an Azure AD B2C deployment

This phase includes the following capabilities:

CAPABILITY	DESCRIPTION
Deploy authentication and authorization	Understand the authentication and authorization scenarios
Deploy applications and user identities	Plan to deploy client application and migrate user identities
Client application onboarding and deliverables	Onboard the client application and test the solution
Security	Enhance the security of your Identity solution
Compliance	Address regulatory requirements
User experience	Enable a user-friendly service

Deploy authentication and authorization

- Start with [setting up an Azure AD B2C tenant](#).
- For business driven authorization, use the [Azure AD B2C Identity Experience Framework \(IEF\) sample user journeys](#)
- Try [Open policy agent](#).

Learn more about Azure AD B2C in [this developer course](#).

Follow this sample checklist for more guidance:

- Identify the different personas that need access to your application.
- Define how you manage permissions and entitlements in your existing system today and how to plan for the future.
- Check if you have a permission store and if there are any permissions that need to be added to the directory.
- If you need delegated administration define how to solve it. For example, your customers' customers management.
- Check if your application calls directly an API Manager (APIM). There may be a need to call from the IdP before issuing a token to the application.

Deploy applications and user identities

All Azure AD B2C projects start with one or more client applications, which may have different business goals.

1. [Create or configure client applications](#). Refer to these [code samples](#) for implementation.
2. Next, setup your user journey based on built-in or custom user flows. [Learn when to use user flows vs. custom policies](#).
3. Setup IdPs based on your business need. [Learn how to add Azure Active Directory B2C as an IdP](#).
4. Migrate your users. [Learn about user migration approaches](#). Refer to [Azure AD B2C IEF sample user journeys](#) for advanced scenarios.

Consider this sample checklist as you **deploy your applications**:

- Check the number of applications that are in scope for the CIAM deployment.
- Check the type of applications that are in use. For example, traditional web applications, APIs, Single page apps (SPA), or Native mobile applications.
- Check the kind of authentication that is in place. For example, forms based, federated with SAML, or federated with OIDC.
 - If OIDC, check the response type - code or id_token.
- Check if all the frontend and backend applications are hosted in on-premises, cloud, or hybrid-cloud.
- Check the platforms/languages used such as, [ASP.NET](#), Java, and Node.js.
- Check where the current user attributes are stored. It could be Lightweight Directory Access Protocol (LDAP) or databases.

Consider this sample checklist as you **deploy user identities**:

- Check the number of users accessing the applications.
- Check the type of IdPs that are needed. For example, Facebook, local account, and [Active Directory Federation Services \(AD FS\)](#).
- Outline the claim schema that is required from your application, [Azure AD B2C](#), and your IdPs if applicable.
- Outline the information that is required to capture during a [sign-in/sign-up flow](#).

Client application onboarding and deliverables

Consider this sample checklist while you **onboard an application**:

TASK	DESCRIPTION
Define the target group of the application	Check if this application is an end customer application, business customer application, or a digital service. Check if there is a need for employee login.
Identify the business value behind an application	Understand the full business case behind an application to find the best fit of Azure AD B2C solution and integration with further client applications.
Check the identity groups you have	Cluster identities in different types of groups with different types of requirements, such as Business to Customer (B2C) for end customers and business customers, Business to Business (B2B) for partners and suppliers, Business to Employee (B2E) for your employees and external employees, Business to Machine (B2M) for IoT device logins and service accounts.
Check the IdP you need for your business needs and processes	Azure AD B2C supports several types of IdPs and depending on the use case the right IdP should be chosen. For example, for a Customer to Customer mobile application a fast and easy user login is required. In another use case, for a Business to Customer with digital services additional compliance requirements are necessary. The user may need to log in with their business identity such as E-mail login.
Check the regulatory constraints	Check if there is any reason to have remote profiles or specific privacy policies.
Design the sign-in and sign-up flow	Decide whether an email verification or email verification inside sign-ups will be needed. First check-out process such as Shop systems or Azure AD Multi-Factor Authentication (MFA) is needed or not. Watch this video .
Check the type of application and authentication protocol used or that will be implemented	Information exchange about the implementation of client application such as Web application, SPA, or Native application. Authentication protocols for client application and Azure AD B2C could be OAuth, OIDC, and SAML. Watch this video
Plan user migration	Discuss the possibilities of user migration with Azure AD B2C . There are several scenarios possible such as Just In Times (JIT) migration, and bulk import/export. Watch this video . You can also consider using Microsoft Graph API for user migration.

Consider this sample checklist while you **deliver**.

CAPABILITY	DESCRIPTION
Protocol information	Gather the base path, policies, metadata URL of both variants. Depending on the client application, specify the attributes such as sample login, client application ID, secrets, and redirects.
Application samples	Refer to the provided sample codes .

CAPABILITY	DESCRIPTION
Pen testing	Before the tests, inform your operations team about the pen tests and then test all user flows including the OAuth implementation. Learn more about Penetration testing and the Microsoft Cloud unified penetration testing rules of engagement .
Unit testing	Perform unit testing and generate tokens using Resource owner password credential (ROPC) flows . If you hit the Azure AD B2C token limit, contact the support team . Reuse tokens to reduce investigation efforts on your infrastructure. Setup a ROPC flow .
Load testing	Expect reaching Azure AD B2C service limits . Evaluate the expected number of authentications per month your service will have. Evaluate the expected number of average user logins per month. Assess the expected high load traffic durations and business reason such as holidays, migrations, and events. Evaluate the expected peak sign-up rate, for example, number of requests per second. Evaluate the expected peak traffic rate with MFA, for example, requests per second. Evaluate the expected traffic geographic distribution and their peak rates.

Security

Consider this sample checklist to enhance the security of your application depending on your business needs:

- Check if strong authentication method such as [MFA](#) is required. For users who trigger high value transactions or other risk events its suggested to use MFA. For example, for banking and finance applications, online shops - first checkout process.
- Check if MFA is required, [check the methods available to do MFA](#) such as SMS/Phone, email, and third-party services.
- Check if any anti-bot mechanism is in use today with your applications.
- Assess the risk of attempts to create fraudulent accounts and log-ins. Use [Microsoft Dynamics 365 Fraud Protection assessment](#) to block or challenge suspicious attempts to create new fake accounts or to compromise existing accounts.
- Check for any special conditional postures that need to be applied as part of sign-in or sign-up for accounts with your application.

NOTE

You can use [Conditional Access rules](#) to adjust the difference between user experience and security based on your business goals.

For more information, see [Identity Protection and Conditional Access in Azure AD B2C](#).

Compliance

To satisfy certain regulatory requirements you may consider using vNets, IP restrictions, Web Application Firewall (WAF), and similar services to enhance the security of your backend systems.

To address basic compliance requirements, consider:

- The specific regulatory compliance requirements, for example, PCI-DSS that you need to support.

- Check if it's required to store data into a separate database store. If so, check if this information must never be written into the directory.

User experience

Consider the sample checklist to define the user experience (UX) requirements:

- Identify the required integrations to [extend CIAM capabilities and build seamless end-user experiences](#).
- Provide screenshots and user stories to show the end-user experience for the existing application. For example, provide screenshots for sign-in, sign-up, combined sign-up sign-in (SUSI), profile edit, and password reset.
- Look for existing hints passed through using queryString parameters in your current CIAM solution.
- If you expect high UX customization such as pixel to pixel, you may need a front-end developer to help you.
- Azure AD B2C provides capabilities for customizing HTML and CSS, however, it has additional requirements for [JavaScript](#).
- An embedded experience can be implemented [using iframe support](#). For a single-page application, you'll also need a second "sign-in" HTML page that loads into the `<iframe>` element.

Monitor an Azure AD B2C solution

This phase includes the following capabilities:

CAPABILITY	DESCRIPTION
Monitoring	Monitor Azure AD B2C with Azure Monitor . Watch this video
Auditing and Logging	Access and review audit logs

More information

To accelerate Azure AD B2C deployments and monitor the service at scale, see these articles:

- [Manage Azure AD B2C with Microsoft Graph](#)
- [Manage Azure AD B2C user accounts with Microsoft Graph](#)
- [Deploy custom policies with Azure Pipelines](#)
- [Manage Azure AD B2C custom policies with Azure PowerShell](#)
- [Monitor Azure AD B2C with Azure Monitor](#)

Next steps

- [Azure AD B2C best practices](#)
- [Azure AD B2C service limits](#)

Frontline worker management

4/10/2022 • 2 minutes to read • [Edit Online](#)

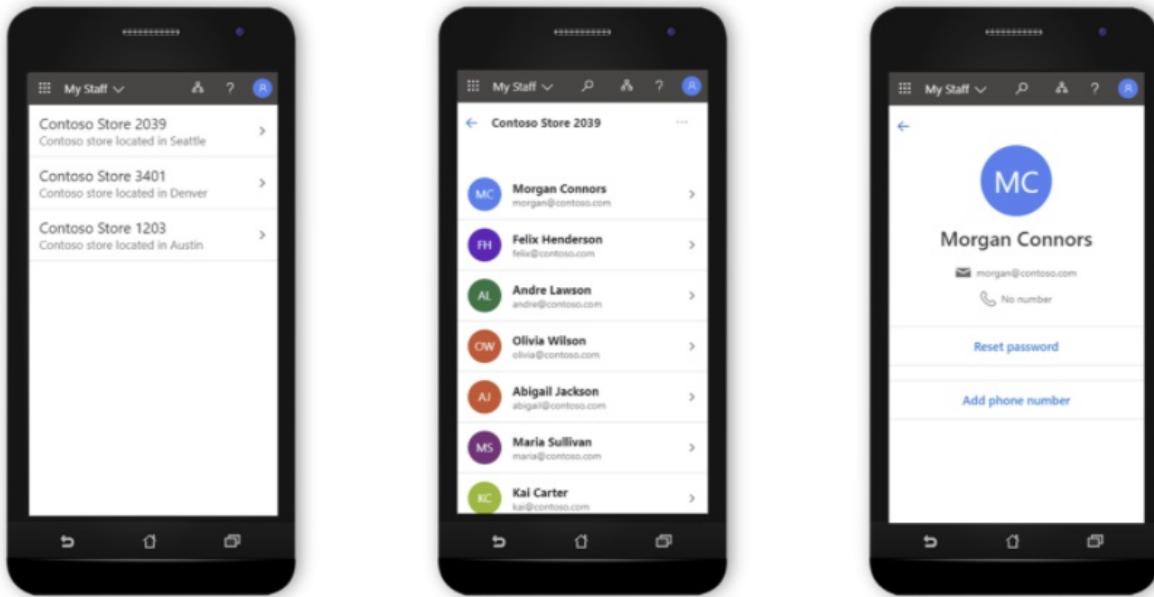
Frontline workers account for over 80 percent of the global workforce. Yet because of high scale, rapid turnover, and fragmented processes, frontline workers often lack the tools to make their demanding jobs a little easier. Frontline worker management brings digital transformation to the entire frontline workforce. The workforce may include managers, frontline workers, operations, and IT.

Frontline worker management empowers the frontline workforce by making the following activities easier to accomplish:

- Streamlining common IT tasks with My Staff
- Easy onboarding of frontline workers through simplified authentication
- Seamless provisioning of shared devices and secure sign-out of frontline workers

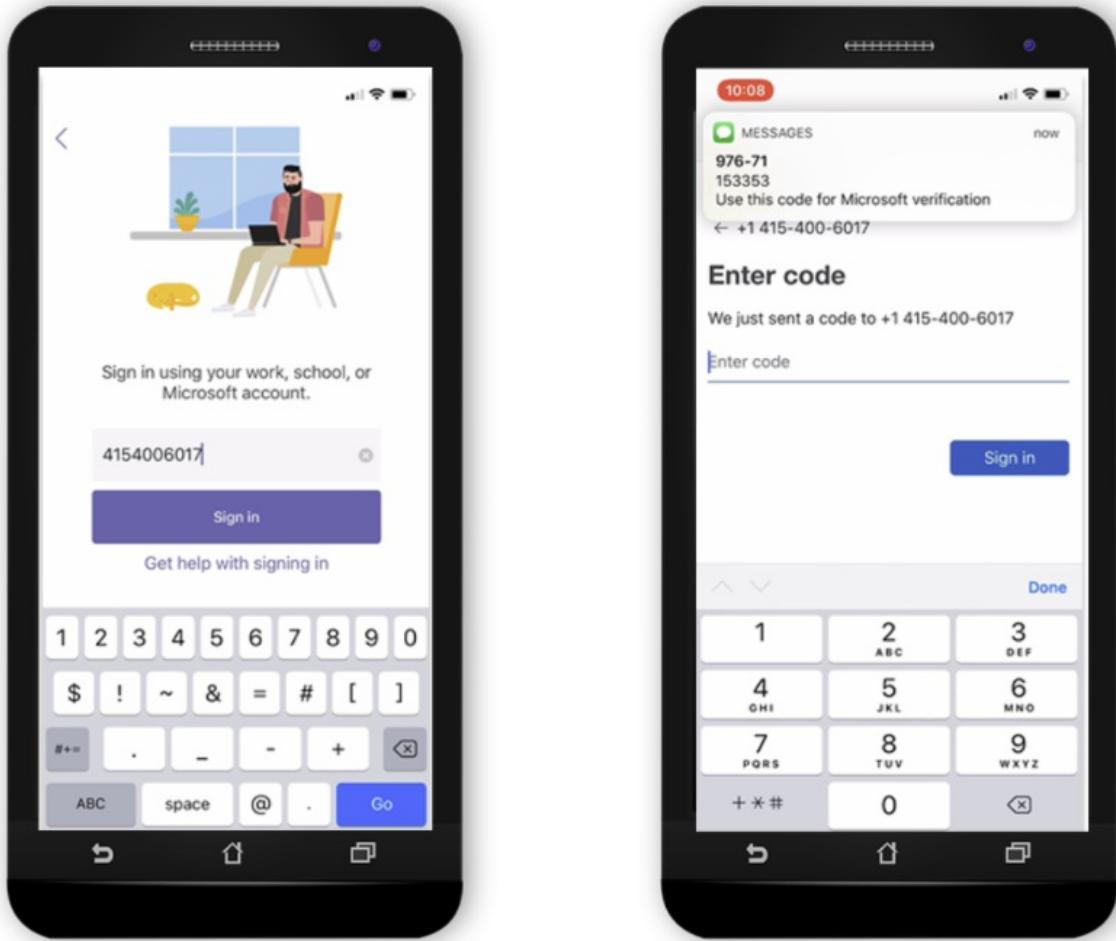
Delegated user management through My Staff

Azure Active Directory (Azure AD) provides the ability to delegate user management to frontline managers through the [My Staff portal](#), helping save valuable time and reduce risks. By enabling simplified password resets and phone management directly from the store or factory floor, managers can grant access to employees without routing the request through the help-desk, IT, or operations.



Accelerated onboarding with simplified authentication

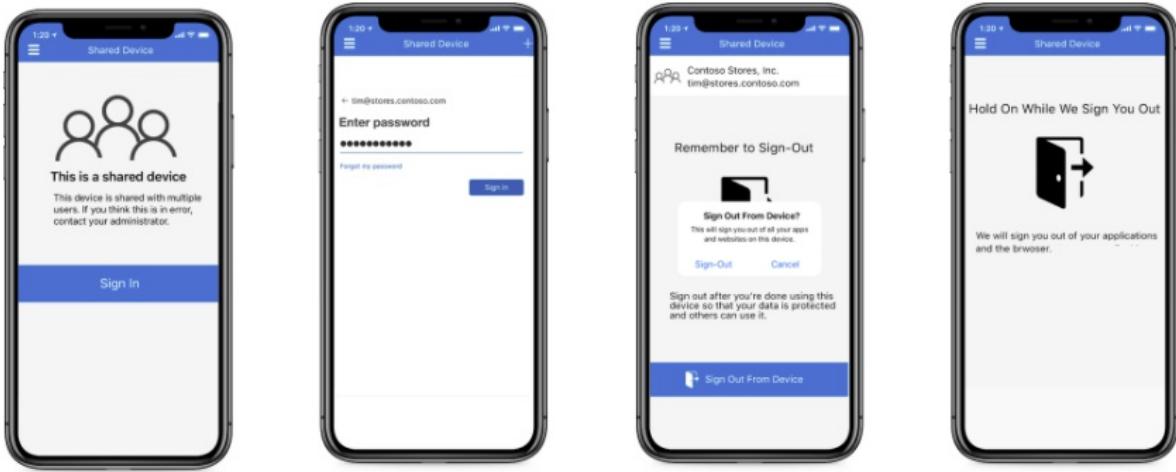
My Staff also enables frontline managers to register their team members' phone numbers for [SMS sign-in](#). In many verticals, frontline workers maintain a local username and password combination, a solution that is often cumbersome, expensive, and error-prone. When IT enables authentication using SMS sign-in, frontline workers can log in with [single sign-on \(SSO\)](#) for Microsoft Teams and other apps using just their phone number and a one-time passcode (OTP) sent via SMS. This makes signing in for frontline workers simple and secure, delivering quick access to the apps they need most.



Frontline managers can also use Managed Home Screen (MHS) application to allow workers to have access to a specific set of applications on their Intune-enrolled Android dedicated devices. The dedicated devices are enrolled with [Azure AD shared device mode](#). When configured in multi-app kiosk mode in the Microsoft Endpoint Manager (MEM) console, MHS is automatically launched as the default home screen on the device and appears to the end user as the *only* home screen. To learn more, see how to [configure the Microsoft Managed Home Screen app for Android Enterprise](#).

Secure sign-out of frontline workers from shared devices

Many companies use shared devices so frontline workers can do inventory management and point-of-sale transactions, without the IT burden of provisioning and tracking individual devices. With shared device sign-out, it's easy for a frontline worker to securely sign out of all apps on any shared device before handing it back to a hub or passing it off to a teammate on the next shift. Microsoft Teams is one of the apps that is currently supported on shared devices and it allows frontline workers to view tasks that are assigned to them. Once a worker signs out of a shared device, Intune and Azure AD clear all of the company data so the device can safely be handed off to the next associate. You can choose to integrate this capability into all your line-of-business [iOS](#) and [Android](#) apps using the [Microsoft Authentication Library](#).



Next steps

- For more information on delegated user management, see [My Staff user documentation](#).
- For inbound user provisioning from SAP SuccessFactors, see the tutorial on [configuring SAP SuccessFactors to Active Directory user provisioning](#).
- For inbound user provisioning from Workday, see the tutorial on [configuring Workday for automatic user provisioning](#).

Azure Active Directory operations reference guide

4/10/2022 • 2 minutes to read • [Edit Online](#)

This operations reference guide describes the checks and actions you should take to secure and maintain the following areas:

- **Identity and access management** - ability to manage the lifecycle of identities and their entitlements.
- **Authentication management** - ability to manage credentials, define authentication experience, delegate assignment, measure usage, and define access policies based on enterprise security posture.
- **Governance** - ability to assess and attest the access granted non-privileged and privileged identities, audit, and control changes to the environment.
- **Operations** - optimize the operations Azure Active Directory (Azure AD).

Some recommendations here might not be applicable to all customers' environment, for example, AD FS best practices might not apply if your organization uses password hash sync.

NOTE

These recommendations are current as of the date of publishing but can change over time. Organizations should continuously evaluate their identity practices as Microsoft products and services evolve over time. Recommendations can change when organizations subscribe to a different Azure AD Premium license. For example, Azure AD Premium P2 will include more governance recommendations.

Stakeholders

Each section in this reference guide recommends assigning stakeholders to plan and implement key tasks successfully. The following table outlines the list of all the stakeholders in this guide:

STAKEHOLDER	DESCRIPTION
IAM Operations Team	This team handles managing the day to day operations of the Identity and Access Management system
Productivity Team	This team owns and manages the productivity applications such as email, file sharing and collaboration, instant messaging, and conferencing.
Application Owner	This team owns the specific application from a business and usually a technical perspective in an organization.
InfoSec Architecture Team	This team plans and designs the Information Security practices of an organization.
InfoSec Operations Team	This team runs and monitors the implemented Information Security practices of the InfoSec Architecture team.

Next steps

Get started with the [Identity and access management checks and actions](#).

Azure Active Directory Identity and access management operations reference guide

4/10/2022 • 11 minutes to read • [Edit Online](#)

This section of the [Azure AD operations reference guide](#) describes the checks and actions you should consider to secure and manage the lifecycle of identities and their assignments.

NOTE

These recommendations are current as of the date of publishing but can change over time. Organizations should continuously evaluate their identity practices as Microsoft products and services evolve over time.

Key operational processes

Assign owners to key tasks

Managing Azure Active Directory requires the continuous execution of key operational tasks and processes that may not be part of a rollout project. It is still important you set up these tasks to maintain your environment.

The key tasks and their recommended owners include:

TASK	OWNER
Define the process how to create Azure subscriptions	Varies by organization
Decide who gets Enterprise Mobility + Security licenses	IAM Operations Team
Decide who gets Microsoft 365 licenses	Productivity Team
Decide who gets other licenses, for example, Dynamics, Visual Studio Codespaces	Application Owner
Assign licenses	IAM Operations Team
Troubleshoot and remediate license assignment errors	IAM Operations Team
Provision identities to applications in Azure AD	IAM Operations Team

As you review your list, you may find you need to either assign an owner for tasks that are missing an owner or adjust ownership for tasks with owners that aren't aligned with the recommendations above.

Assigning owners recommended reading

- [Assigning administrator roles in Azure Active Directory](#)
- [Governance in Azure](#)

On-premises identity synchronization

Identify and resolve synchronization issues

Microsoft recommends you have a good baseline and understanding of the issues in your on-premises environment that can result in synchronization issues to the cloud. Since automated tools such as [IdFix](#) and

Azure AD Connect Health can generate a high volume of false positives, we recommend you identify synchronization errors that have been left unaddressed for more than 100 days by cleaning up those objects in error. Long term unresolved synchronization errors can generate support incidents. [Troubleshooting errors during synchronization](#) provides an overview of different types of sync errors, some of the possible scenarios that cause those errors and potential ways to fix the errors.

Azure AD Connect Sync configuration

To enable all hybrid experiences, device-based security posture, and integration with Azure AD, it is required that you synchronize user accounts that your employees use to login to their desktops.

If you don't synchronize the forest users log into, then you should change the synchronization to come from the proper forest.

Synchronization scope and object filtering

Removing known buckets of objects that aren't required to be synchronized has the following operational benefits:

- Fewer sources of sync errors
- Faster sync cycles
- Less "garbage" to carry forward from on-premises, for example, pollution of the global address list for on-premises service accounts that aren't relevant in the cloud

NOTE

If you find you are importing many objects that aren't being exported to the cloud, you should filter by OU or specific attributes.

Examples of objects to exclude are:

- Service Accounts that aren't used for cloud applications
- Groups that aren't meant to be used in cloud scenarios such as those used to grant access to resources
- Users or contacts that are external identities that are meant to be represented with Azure AD B2B Collaboration
- Computer Accounts where employees aren't meant to access cloud applications from, for example, servers

NOTE

If a single human identity has multiple accounts provisioned from something such as a legacy domain migration, merger, or acquisition, you should only synchronize the account used by the user on a day-to-day basis, for example, what they use to log in to their computer.

Ideally, you will want to reach a balance between reducing the number of objects to synchronize and the complexity in the rules. Generally, a combination between OU/container [filtering](#) plus a simple attribute mapping to the cloudFiltered attribute is an effective filtering combination.

IMPORTANT

If you use group filtering in production, you should transition to another filtering approach.

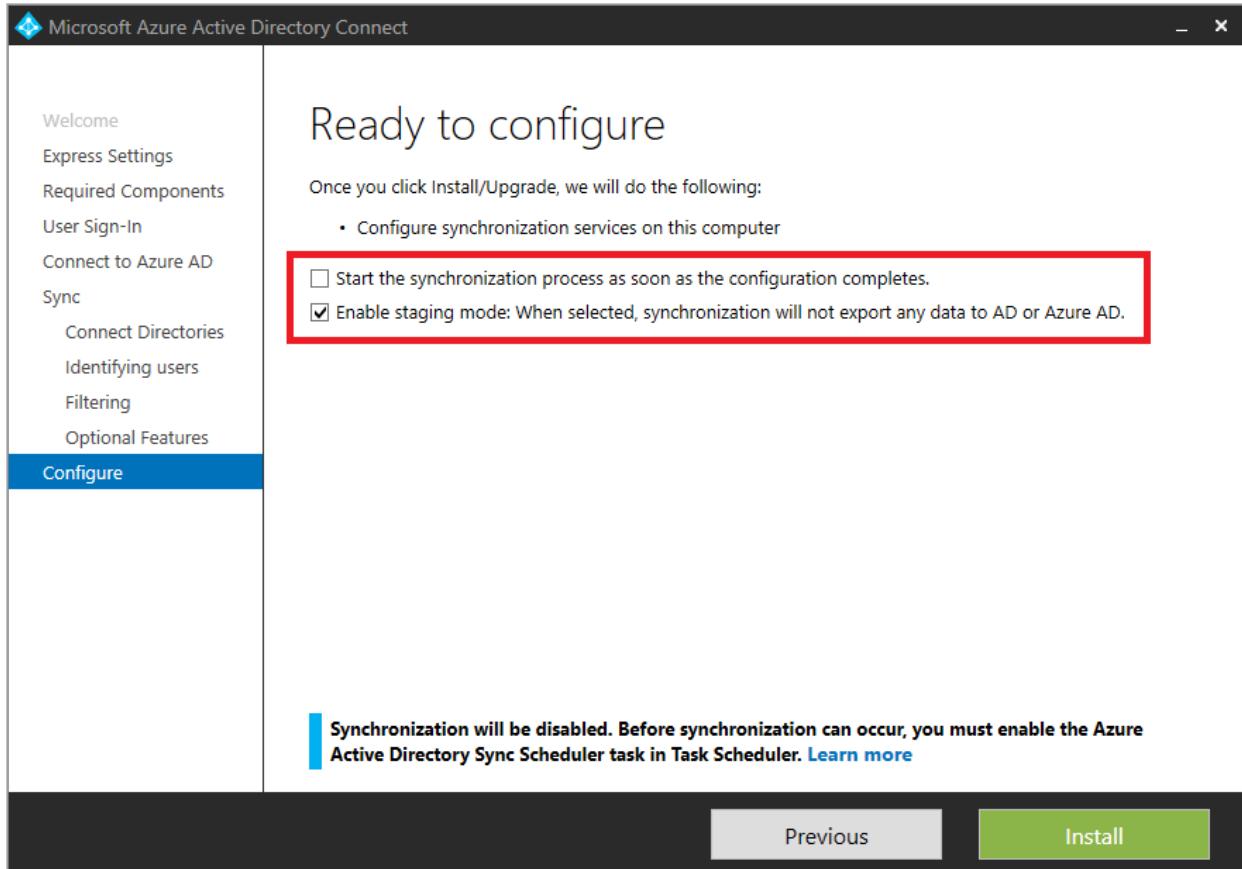
Sync failover or disaster recovery

Azure AD Connect plays a key role in the provisioning process. If the Sync Server goes offline for any reason, changes to on-premises cannot be updated in the cloud and can result in access issues for users. Therefore, it is important to define a failover strategy that allows administrators to quickly resume synchronization after the

sync server goes offline. Such strategies may fall into the following categories:

- **Deploy Azure AD Connect Server(s) in Staging Mode** - allows an administrator to "promote" the staging server to production by a simple configuration switch.
- **Use Virtualization** - If the Azure AD connect is deployed in a virtual machine (VM), admins can leverage their virtualization stack to live migrate or quickly redeploy the VM and therefore resume synchronization.

If your organization is lacking a disaster recovery and failover strategy for Sync, you shouldn't hesitate to deploy Azure AD Connect in Staging Mode. Likewise, if there is a mismatch between your production and staging configuration, you should re-baseline Azure AD Connect staging mode to match the production configuration, including software versions and configurations.



Stay current

Microsoft updates Azure AD Connect regularly. Stay current to take advantage of the performance improvements, bug fixes, and new capabilities that each new version provides.

If your Azure AD Connect version is more than six months behind, you should upgrade to the most recent version.

Source anchor

Using **ms-DS-consistencyguid** as the [source anchor](#) allows an easier migration of objects across forests and domains, which is common in AD Domain consolidation/cleanup, mergers, acquisitions, and divestitures.

If you're currently using **ObjectGuid** as the source anchor, we recommend you switch to using **ms-DS-ConsistencyGuid**.

Custom rules

Azure AD Connect custom rules provide the ability to control the flow of attributes between on-premises objects and cloud objects. However, overusing or misusing custom rules can introduce the following risks:

- Troubleshooting complexity
- Degradation of performance when performing complex operations across objects
- Higher probability of divergence of configuration between the production server and staging server

- Additional overhead when upgrading Azure AD Connect if custom rules are created within the precedence greater than 100 (used by built-in rules)

If you are using overly complex rules, you should investigate the reasons for the complexity and find opportunities for simplification. Likewise, if you have created custom rules with precedence value over 100, you should fix the rules so they aren't at risk or conflict with the default set.

Examples of misusing custom rules include:

- **Compensate for dirty data in the directory** - In this case, it is recommended to work with the owners of the AD team and clean up the data in the directory as a remediation task, and adjust processes to avoid reintroduction of bad data.
- **One-off remediation of individual users** - It is common to find rules that special case outliers, usually because of an issue with a specific user.
- **Overcomplicated "CloudFiltering"** - While reducing the number of objects is a good practice, there is a risk of creating and overcomplicated sync scope using many sync rules. If there is complex logic to include/exclude objects beyond the OU filtering, it is recommended to deal with this logic outside of sync and label the objects with a simple "cloudFiltered" attribute that can flow with a simple Sync Rule.

Azure AD Connect configuration documenter

The [Azure AD Connect Configuration Documenter](#) is a tool you can use to generate documentation of an Azure AD Connect installation to enable a better understanding of the sync configuration, build confidence in getting things right, and to know what was changed when you applied a new build or configuration of Azure AD Connect or added or updated custom sync rules. The current capabilities of the tool include:

- Documentation of the complete configuration of Azure AD Connect sync.
- Documentation of any changes in the configuration of two Azure AD Connect sync servers or changes from a given configuration baseline.
- Generation of a PowerShell deployment script to migrate the sync rule differences or customizations from one server to another.

Assignment to apps and resources

Group-based licensing for Microsoft cloud services

Azure Active Directory streamlines the management of licenses through [group-based licensing](#) for Microsoft cloud services. This way, IAM provides the group infrastructure and delegated management of those groups to the proper teams in the organizations. There are multiple ways to set up the membership of groups in Azure AD, including:

- **Synchronized from on-premises** - Groups can come from on-premises directories, which could be a good fit for organizations that have established group management processes that can be extended to assign licenses in Microsoft 365.
- **Attribute-based / dynamic** - Groups can be created in the cloud based on an expression based on user attributes, for example, Department equals "sales". Azure AD maintains the members of the group, keeping it consistent with the expression defined. Using this kind of group for license assignment enables an attribute-based license assignment, which is a good fit for organizations that have high data quality in their directory.
- **Delegated ownership** - Groups can be created in the cloud and can be designated owners. This way, you can empower business owners, for example, Collaboration team or BI team, to define who should have access.

If you are currently using a manual process to assign licenses and components to users, we recommend you implement group-based licensing. If your current process does not monitor licensing errors or what is Assigned

versus Available, you should define improvements to the process to address licensing errors and monitor licensing assignment.

Another aspect of license management is the definition of service plans (components of the license) that should be enabled based on job functions in the organization. Granting access to service plans that aren't necessary, can result in users seeing tools in the Office portal that they have not been trained for or should not be using. It can drive additional help desk volume, unnecessary provisioning, and put your compliance and governance at risk, for example, when provisioning OneDrive for Business to individuals that might not be allowed to share content.

Use the following guidelines to define service plans to users:

- Administrators should define "bundles" of service plans to be offered to users based on their role, for instance, white-collar worker versus floor worker.
- Create groups by cluster and assign the license with service plan.
- Optionally, an attribute can be defined to hold the packages for users.

IMPORTANT

Group-based licensing in Azure AD introduces the concept of users in a licensing error state. If you notice any licensing errors, then you should immediately [identify and resolve](#) any license assignment problems.

PRODUCTS	STATE	ENABLED SERVICES
Office 365 Enterprise E1	Active	11/12

Lifecycle management

If you are currently using a tool, such as [Microsoft Identity Manager](#) or third-party system, that relies on an on-premises infrastructure, we recommend you offload assignment from the existing tool, implement group-based licensing and define a group lifecycle management based on [groups](#). Likewise, if your existing process doesn't account for new employees or employees that leave the organization, you should deploy group-based licensing based on dynamic groups and define a group membership lifecycle. Finally, if group-based licensing is deployed against on-premises groups that lack lifecycle management, consider using cloud groups to enable capabilities such as delegated ownership or attribute-based dynamic membership.

Assignment of apps with "All users" group

Resource owners may believe that the **All users** group contains only **Enterprise Employees** when they may actually contain both **Enterprise Employees** and **Guests**. As a result, you should take special care when using the **All users** group for application assignment and granting access to resources such as SharePoint content or applications.

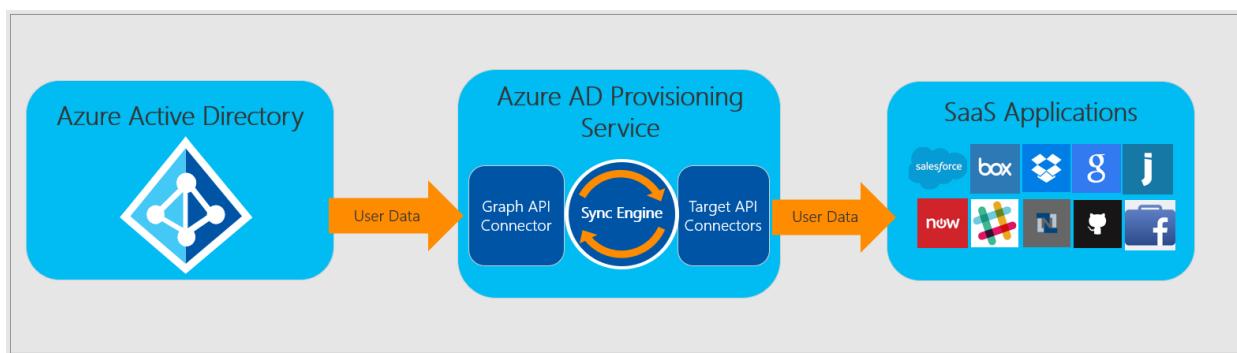
IMPORTANT

If the All users group is enabled and used for conditional access policies, app or resource assignment, make sure to [secure the group](#) if you don't want it to include guest users. Furthermore, you should fix your licensing assignments by creating and assigning to groups that contain **Enterprise Employees** only. On the other hand, if you find that the All users group is enabled but not being used to grant access to resources, make sure your organization's operational guidance is to intentionally use that group (which includes both **Enterprise Employees** and **Guests**).

Automated user provisioning to apps

[Automated user provisioning](#) to applications is the best way to create a consistent provisioning, deprovisioning, and lifecycle of identities across multiple systems.

If you are currently provisioning apps in an ad-hoc manner or using things like CSV files, JIT, or an on-premises solution that does not address lifecycle management, we recommend you [implement application provisioning](#) with Azure AD for supported applications and define a consistent pattern for applications that aren't yet supported by Azure AD.



Azure AD Connect delta sync cycle baseline

It is important to understand the volume of changes in your organization and make sure that it isn't taking too long to have a predictable synchronization time.

The [default delta sync](#) frequency is 30 minutes. If the delta sync is taking longer than 30 minutes consistently, or there are significant discrepancies between the delta sync performance of staging and production, you should investigate and review the [factors influencing the performance of Azure AD Connect](#).

Azure AD Connect troubleshooting recommended reading

- [Prepare directory attributes for synchronization with Microsoft 365 by using the IdFix tool](#)
- [Azure AD Connect: Troubleshooting Errors during synchronization](#)

Summary

There are five aspects to a secure identity infrastructure. This list will help you quickly find and take the necessary actions to secure and manage the lifecycle of identities and their entitlements in your organization.

- Assign owners to key tasks.
- Find and resolve synchronization issues.
- Define a failover strategy for disaster recovery.
- Streamline the management of licenses and assignment of apps.
- Automate user provisioning to apps.

Next steps

Get started with the [Authentication management checks and actions](#).

Azure Active Directory Authentication management operations reference guide

4/10/2022 • 20 minutes to read • [Edit Online](#)

This section of the [Azure AD operations reference guide](#) describes the checks and actions you should take to secure and manage credentials, define authentication experience, delegate assignment, measure usage, and define access policies based on enterprise security posture.

NOTE

These recommendations are current as of the date of publishing but can change over time. Organizations should continuously evaluate their identity practices as Microsoft products and services evolve over time.

Key operational processes

Assign owners to key tasks

Managing Azure Active Directory requires the continuous execution of key operational tasks and processes, which may not be part of a rollout project. It is still important you set up these tasks to optimize your environment. The key tasks and their recommended owners include:

TASK	OWNER
Manage lifecycle of single sign-on (SSO) configuration in Azure AD	IAM Operations Team
Design conditional access policies for Azure AD applications	InfoSec Architecture Team
Archive sign-in activity in a SIEM system	InfoSec Operations Team
Archive risk events in a SIEM system	InfoSec Operations Team
Triage and investigate security reports	InfoSec Operations Team
Triage and investigate risk events	InfoSec Operations Team
Triage and investigate users flagged for risk and vulnerability reports from Azure AD Identity Protection	InfoSec Operations Team

NOTE

Azure AD Identity Protection requires an Azure AD Premium P2 license. To find the right license for your requirements, see [Comparing generally available features of the Azure AD Free and Azure AD Premium editions](#).

As you review your list, you may find you need to either assign an owner for tasks that are missing an owner or adjust ownership for tasks with owners that aren't aligned with the recommendations above.

Owner recommended reading

- [Assigning administrator roles in Azure Active Directory](#)

- Governance in Azure

Credentials management

Password policies

Managing passwords securely is one of the most critical parts of identity and access management and often the biggest target of attacks. Azure AD supports several features that can help prevent an attack from being successful.

Use the table below to find the recommended solution for mitigating the issue that needs to be addressed:

ISSUE	RECOMMENDATION
No mechanism to protect against weak passwords	Enable Azure AD self-service password reset (SSPR) and password protection
No mechanism to detect leaked passwords	Enable password hash sync (PHS) to gain insights
Using AD FS and unable to move to managed authentication	Enable AD FS Extranet Smart Lockout and / or Azure AD Smart Lockout
Password policy uses complexity-based rules such as length, multiple character sets, or expiration	Reconsider in favor of Microsoft Recommended Practices and switch your approach to password management and deploy Azure AD password protection .
Users aren't registered to use multi-factor authentication (MFA)	Register all user's security information so it can be used as a mechanism to verify the user's identity along with their password
There is no revocation of passwords based on user risk	Deploy Azure AD Identity Protection user risk policies to force password changes on leaked credentials using SSPR
There is no smart lockout mechanism to protect malicious authentication from bad actors coming from identified IP addresses	Deploy cloud-managed authentication with either password hash sync or pass-through authentication (PTA)

Password policies recommended reading

- [Azure AD and AD FS best practices: Defending against password spray attacks - Enterprise Mobility + Security](#)

Enable self-service password reset and password protection

Users needing to change or reset their passwords is one of the biggest sources of volume and cost of help desk calls. In addition to cost, changing the password as a tool to mitigate a user risk is a fundamental step in improving the security posture of your organization.

At a minimum, it is recommended you deploy Azure AD [self-service password reset \(SSPR\)](#) and on-premises [password protection](#) to accomplish:

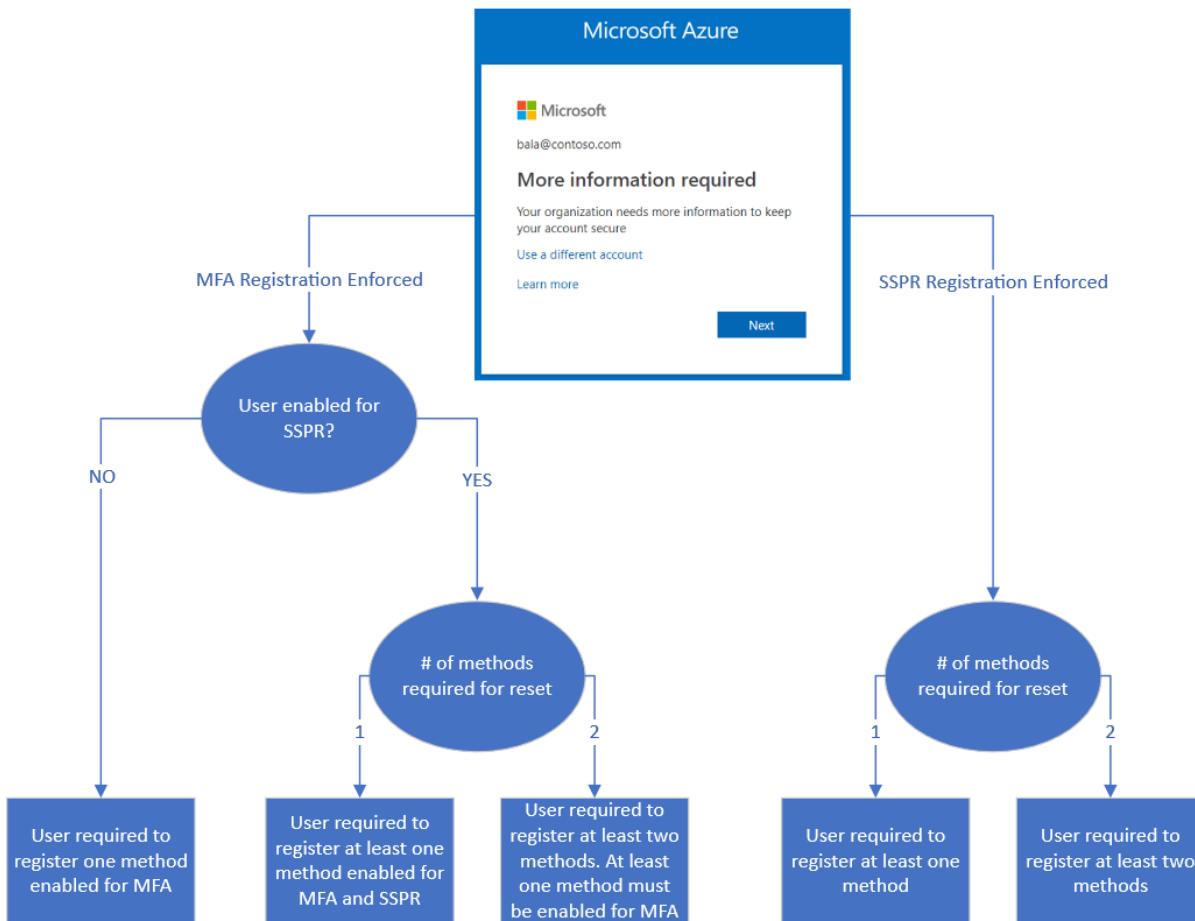
- Deflect help desk calls.
- Replace the use of temporary passwords.
- Replace any existing self-service password management solution that relies on an on-premises solution.
- [Eliminate weak passwords](#) in your organization.

NOTE

For organizations with an Azure AD Premium P2 subscription, it is recommended to deploy SSPR and use it as part of an [Identity Protection User Risk Policy](#).

Strong credential management

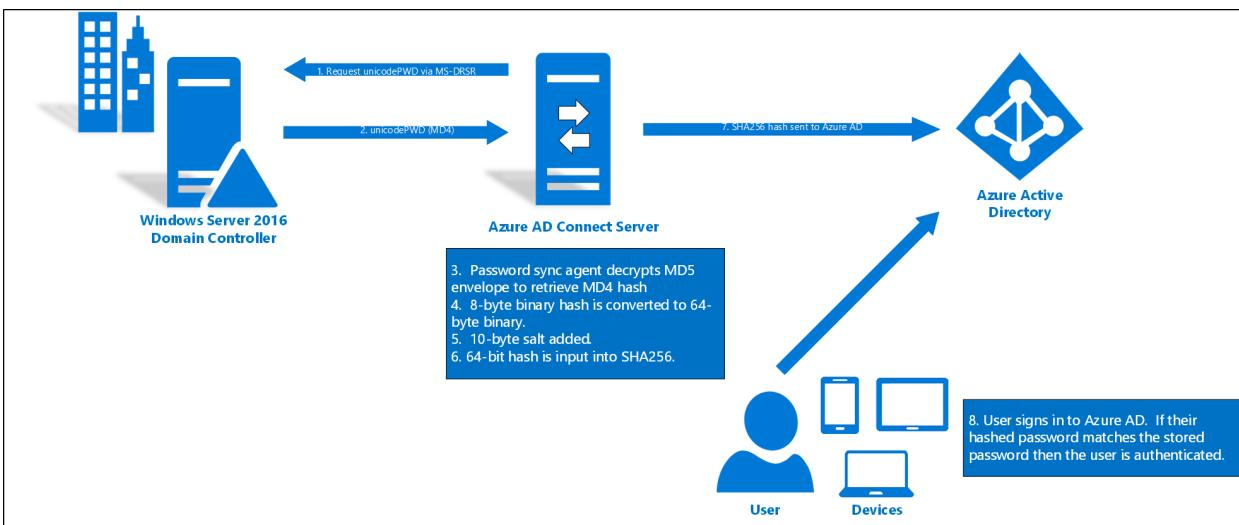
Passwords by themselves aren't secure enough to prevent bad actors from gaining access to your environment. At a minimum, any user with a privileged account must be enabled for multi-factor authentication (MFA). Ideally, you should enable [combined registration](#) and require all users to register for MFA and SSPR using the [combined registration experience](#). Eventually, we recommend you adopt a strategy to [provide resilience](#) to reduce the risk of lockout due to unforeseen circumstances.



On-premises outage authentication resiliency

In addition to the benefits of simplicity and enabling leaked credential detection, Azure AD Password Hash Sync (PHS) and Azure AD MFA allow users to access SaaS applications and Microsoft 365 in spite of on-premises outages due to cyberattacks such as [NotPetya](#). It is also possible to enable PHS while in conjunction with federation. Enabling PHS allows a fallback of authentication when federation services aren't available.

If your on-premises organization is lacking an outage resiliency strategy or has one that isn't integrated with Azure AD, you should deploy Azure AD PHS and define a disaster recovery plan that includes PHS. Enabling Azure AD PHS will allow users to authenticate against Azure AD should your on-premises Active Directory be unavailable.



To better understand your authentication options, see [Choose the right authentication method for your Azure Active Directory hybrid identity solution](#).

Programmatic usage of credentials

Azure AD scripts using PowerShell or applications using the Microsoft Graph API require secure authentication. Poor credential management executing those scripts and tools increase the risk of credential theft. If you are using scripts or applications that rely on hard-coded passwords or password prompts you should first review passwords in config files or source code, then replace those dependencies and use Azure Managed Identities, Integrated-Windows Authentication, or [certificates](#) whenever possible. For applications where the previous solutions aren't possible, consider using [Azure Key Vault](#).

If you determine that there are service principals with password credentials and you're unsure how those password credentials are secured by scripts or applications, contact the owner of the application to better understand usage patterns.

Microsoft also recommends you contact application owners to understand usage patterns if there are service principals with password credentials.

Authentication experience

On-premises authentication

Federated Authentication with integrated Windows authentication (IWA) or Seamless Single Sign-On (SSO) managed authentication with password hash sync or pass-through authentication is the best user experience when inside the corporate network with line-of-sight to on-premises domain controllers. It minimizes credential prompt fatigue and reduces the risk of users falling prey to phishing attacks. If you are already using cloud-managed authentication with PHS or PTA, but users still need to type in their password when authenticating on-premises, then you should immediately [deploy Seamless SSO](#). On the other hand, if you are currently federated with plans to eventually migrate to cloud-managed authentication, then you should implement Seamless SSO as part of the migration project.

Device trust access policies

Like a user in your organization, a device is a core identity you want to protect. You can use a device's identity to protect your resources at any time and from any location. Authenticating the device and accounting for its trust type improves your security posture and usability by:

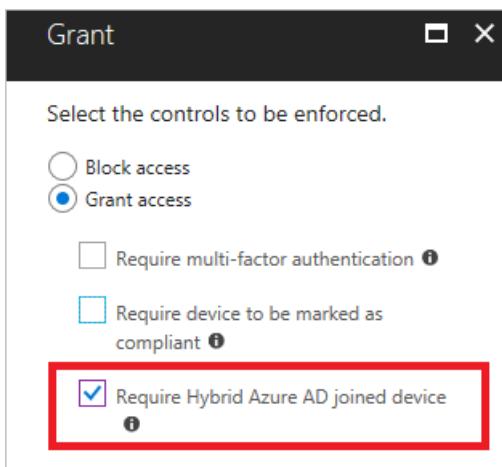
- Avoiding friction, for example, with MFA, when the device is trusted
- Blocking access from untrusted devices
- For Windows 10 devices, provide [single sign-on to on-premises resources seamlessly](#).

You can carry out this goal by bringing device identities and managing them in Azure AD by using one of the

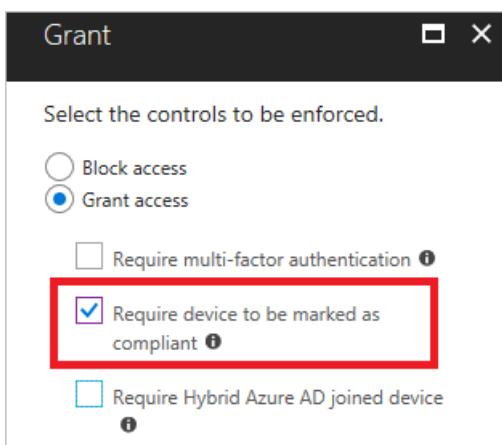
following methods:

- Organizations can use [Microsoft Intune](#) to manage the device and enforce compliance policies, attest device health, and set conditional access policies based on whether the device is compliant. Microsoft Intune can manage iOS devices, Mac desktops (Via JAMF integration), Windows desktops (natively using Mobile Device Management for Windows 10, and co-management with Microsoft Endpoint Configuration Manager) and Android mobile devices.
- [Hybrid Azure AD join](#) provides management with Group Policies or Microsoft Endpoint Configuration Manager in an environment with Active Directory domain-joined computers devices. Organizations can deploy a managed environment either through PHS or PTA with Seamless SSO. Bringing your devices to Azure AD maximizes user productivity through SSO across your cloud and on-premises resources while enabling you to secure access to your cloud and on-premises resources with [Conditional Access](#) at the same time.

If you have domain-joined Windows devices that aren't registered in the cloud, or domain-joined Windows devices that are registered in the cloud but without conditional access policies, then you should register the unregistered devices and, in either case, [use Hybrid Azure AD join as a control](#) in your conditional access policies.



If you are managing devices with MDM or Microsoft Intune, but not using device controls in your conditional access policies, then we recommend using [Require device to be marked as compliant](#) as a control in those policies.



Device trust access policies recommended reading

- [How To: Plan your hybrid Azure Active Directory join implementation](#)
- [Identity and device access configurations](#)

Windows Hello for Business

In Windows 10, [Windows Hello for Business](#) replaces passwords with strong two-factor authentication on PCs. Windows Hello for Business enables a more streamlined MFA experience for users and reduces your

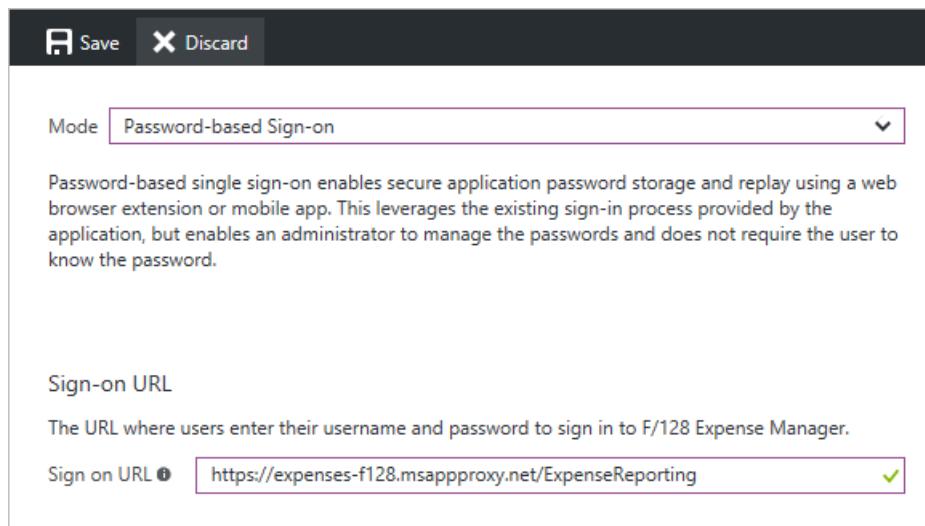
dependency on passwords. If you haven't begun rolling out Windows 10 devices, or have only partially deployed them, we recommend you upgrade to Windows 10 and [enable Windows Hello for Business](#) on all devices.

If you would like to learn more about passwordless authentication, see [A world without passwords with Azure Active Directory](#).

Application authentication and assignment

Single sign-on for apps

Providing a standardized single sign-on mechanism to the entire enterprise is crucial for best user experience, reduction of risk, ability to report, and governance. If you are using applications that support SSO with Azure AD but are currently configured to use local accounts, you should reconfigure those applications to use SSO with Azure AD. Likewise, if you are using any applications that support SSO with Azure AD but are using another Identity Provider, you should reconfigure those applications to use SSO with Azure AD as well. For applications that don't support federation protocols but do support forms-based authentication, we recommend you configure the application to use [password vaulting](#) with Azure AD Application Proxy.



The screenshot shows a configuration dialog for an application. At the top, there are 'Save' and 'Discard' buttons. Below them, a dropdown menu labeled 'Mode' is set to 'Password-based Sign-on'. A descriptive text box explains that this mode enables secure password storage and replay using a web browser extension or mobile app, leveraging the existing sign-in process provided by the application. In the 'Sign-on URL' section, the URL 'https://expenses-f128.msappproxy.net/ExpenseReporting' is listed with a green checkmark indicating it is valid. The entire dialog has a dark header bar.

NOTE

If you don't have a mechanism to discover unmanaged applications in your organization, we recommend implementing a discovery process using a cloud access security broker solution (CASB) such as [Microsoft Defender for Cloud Apps](#).

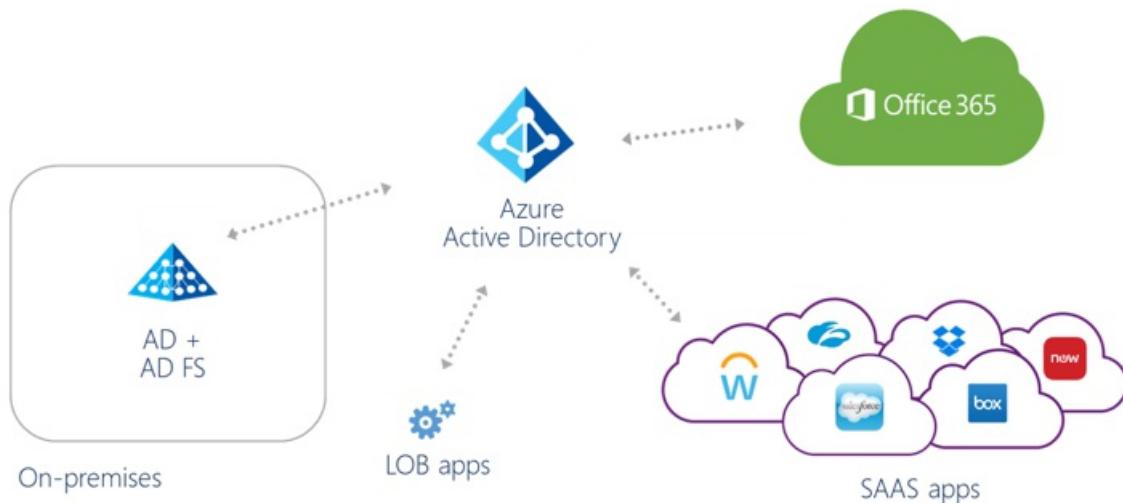
Finally, if you have an Azure AD app gallery and use applications that support SSO with Azure AD, we recommend [listing the application in the app gallery](#).

Single sign-on recommended reading

- [What is application access and single sign-on with Azure Active Directory](#)

Migration of AD FS applications to Azure AD

[Migrating apps from AD FS to Azure AD](#) enables additional capabilities on security, more consistent manageability, and a better collaboration experience. If you have applications configured in AD FS that support SSO with Azure AD, then you should reconfigure those applications to use SSO with Azure AD. If you have applications configured in AD FS with uncommon configurations unsupported by Azure AD, you should contact the app owners to understand if the special configuration is an absolute requirement of the application. If it isn't required, then you should reconfigure the application to use SSO with Azure AD.



NOTE

Azure AD Connect Health for ADFS can be used to collect configuration details about each application that can potentially be migrated to Azure AD.

Assign users to applications

Assigning users to applications is best mapped by using groups because they allow greater flexibility and ability to manage at scale. The benefits of using groups include [attribute-based dynamic group membership](#) and [delegation to app owners](#). Therefore, if you are already using and managing groups, we recommend you take the following actions to improve management at scale:

- Delegate group management and governance to application owners.
- Allow self-service access to the application.
- Define dynamic groups if user attributes can consistently determine access to applications.
- Implement attestation to groups used for application access using [Azure AD access reviews](#).

On the other hand, if you find applications that have assignment to individual users, be sure to implement [governance](#) around those applications.

Assign users to applications recommended reading

- [Assign users and groups to an application in Azure Active Directory](#)
- [Delegate app registration permissions in Azure Active Directory](#)
- [Dynamic membership rules for groups in Azure Active Directory](#)

Access policies

Named locations

With [named locations](#) in Azure AD, you can label trusted IP address ranges in your organization. Azure AD uses named locations to:

- Prevent false positives in risk events. Signing in from a trusted network location lowers a user's sign-in risk.
- Configure [location-based Conditional Access](#).

The screenshot shows the 'Conditional access - Named locations' page in Azure Active Directory. On the left, there's a sidebar with links like 'Policies', 'Named locations' (which is highlighted with a red box), 'Custom controls (preview)', 'Terms of use', 'VPN connectivity', 'Classic policies', 'Troubleshoot', and 'New support request'. At the top right, there are buttons for 'New location' (also highlighted with a red box) and 'Configure MFA trusted IPs'. Below these, a section explains that named locations help reduce false positives in security reports and conditional access policies. It includes a search bar and a table with columns 'NAME' and 'TRUSTED', showing one entry: 'No networks'.

Based on priority, use the table below to find the recommended solution that best meets your organization's needs:

PRIORITY	SCENARIO	RECOMMENDATION
1	If you use PHS or PTA and named locations haven't been defined	Define named locations to improve detection of risk events
2	If you are federated and don't use "insideCorporateNetwork" claim and named locations haven't been defined	Define named locations to improve detection of risk events
3	If you don't use named locations in conditional access policies and there is no risk or device controls in conditional access policies	Configure the conditional access policy to include named locations
4	If you are federated and do use "insideCorporateNetwork" claim and named locations haven't been defined	Define named locations to improve detection of risk events
5	If you are using trusted IP addresses with MFA rather than named locations and marking them as trusted	Define named locations and mark them as trusted to improve detection of risk events

Risk-based access policies

Azure AD can calculate the risk for every sign-in and every user. Using risk as a criterion in access policies can provide a better user experience, for example, fewer authentication prompts, and better security, for example, only prompt users when they are needed, and automate the response and remediation.



If you already own Azure AD Premium P2 licenses that support using risk in access policies, but they aren't being used, we highly recommend adding risk to your security posture.

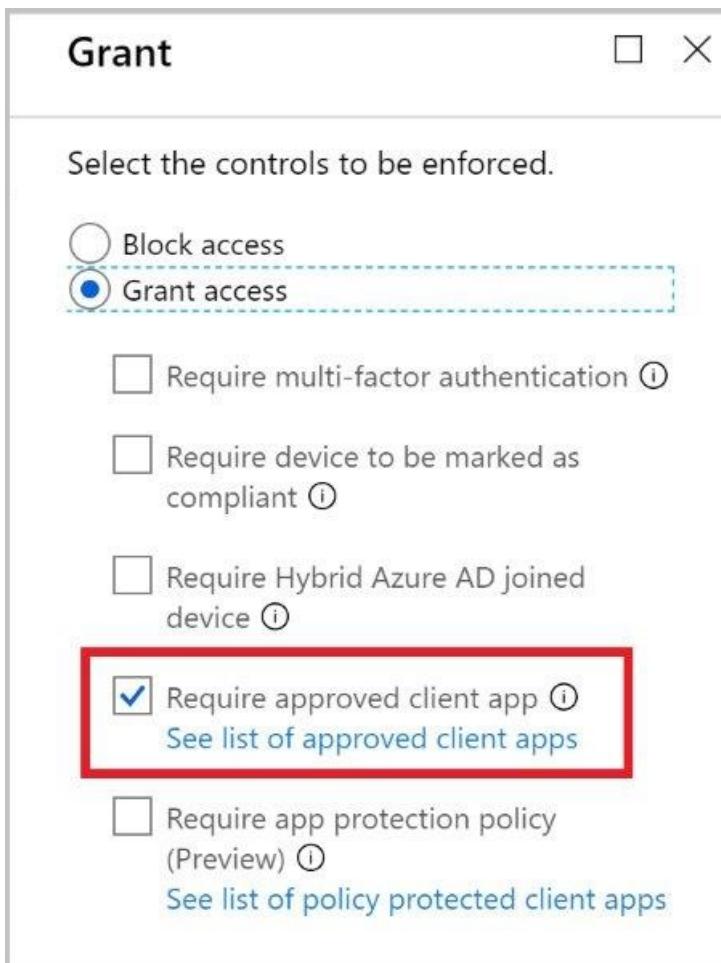
Risk-based access policies recommended reading

- [How To: Configure the sign-in risk policy](#)
- [How To: Configure the user risk policy](#)

Client application access policies

Microsoft Intune Application Management (MAM) provides the ability to push data protection controls such as storage encryption, PIN, remote storage cleanup, etc. to compatible client mobile applications such as Outlook Mobile. In addition, conditional access policies can be created to [restrict access](#) to cloud services such as Exchange Online from approved or compatible apps.

If your employees install MAM-capable applications such as Office mobile apps to access corporate resources such as Exchange Online or SharePoint Online, and you also support BYOD (bring your own device), we recommend you deploy application MAM policies to manage the application configuration in personally owned devices without MDM enrollment and then update your conditional access policies to only allow access from MAM-capable clients.



Should employees install MAM-capable applications against corporate resources and access is restricted on Intune Managed devices, then you should consider deploying application MAM policies to manage the application configuration for personal devices, and update Conditional Access policies to only allow access from

MAM capable clients.

Conditional Access implementation

Conditional Access is an essential tool for improving the security posture of your organization. Therefore, it is important you follow these best practices:

- Ensure that all SaaS applications have at least one policy applied
- Avoid combining the **All apps** filter with the **block** control to avoid lockout risk
- Avoid using the **All users** as a filter and inadvertently adding **Guests**
- **Migrate all "legacy" policies to the Azure portal**
- Catch all criteria for users, devices, and applications
- Use Conditional Access policies to [implement MFA](#), rather than using a **per-user MFA**
- Have a small set of core policies that can apply to multiple applications
- Define empty exception groups and add them to the policies to have an exception strategy
- Plan for [break glass](#) accounts without MFA controls
- Ensure a consistent experience across Microsoft 365 client applications, for example, Teams, OneDrive, Outlook, etc.) by implementing the same set of controls for services such as Exchange Online and SharePoint Online
- Assignment to policies should be implemented through groups, not individuals
- Do regular reviews of the exception groups used in policies to limit the time users are out of the security posture. If you own Azure AD P2, then you can use access reviews to automate the process

Conditional Access recommended reading

- [Best practices for Conditional Access in Azure Active Directory](#)
- [Identity and device access configurations](#)
- [Azure Active Directory Conditional Access settings reference](#)
- [Common Conditional Access policies](#)

Access surface area

Legacy authentication

Strong credentials such as MFA cannot protect apps using legacy authentication protocols, which make it the preferred attack vector by malicious actors. Locking down legacy authentication is crucial to improve the access security posture.

Legacy authentication is a term that refers to authentication protocols used by apps like:

- Older Office clients that don't use modern authentication (for example, Office 2010 client)
- Clients that use mail protocols such as IMAP/SMTP/POP

Attackers strongly prefer these protocols - in fact, nearly [100% of password spray attacks](#) use legacy authentication protocols! Hackers use legacy authentication protocols, because they don't support interactive sign-in, which is needed for additional security challenges like multi-factor authentication and device authentication.

If legacy authentication is widely used in your environment, you should plan to migrate legacy clients to clients that support [modern authentication](#) as soon as possible. In the same token, if you have some users already using modern authentication but others that still use legacy authentication, you should take the following steps to lock down legacy authentication clients:

1. Use [Sign-In Activity reports](#) to identify users who are still using legacy authentication and plan remediation:
 - a. Upgrade to modern authentication capable clients to affected users.

- b. Plan a cutover timeframe to lock down per steps below.
 - c. Identify what legacy applications have a hard dependency on legacy authentication. See step 3 below.
2. Disable legacy protocols at the source (for example Exchange Mailbox) for users who aren't using legacy auth to avoid more exposure.
 3. For the remaining accounts (ideally non-human identities such as service accounts), use [conditional access to restrict legacy protocols](#) post-authentication.

Legacy authentication recommended reading

- [Enable or disable POP3 or IMAP4 access to mailboxes in Exchange Server](#)

Consent grants

In an illicit consent grant attack, the attacker creates an Azure AD-registered application that requests access to data such as contact information, email, or documents. Users might be granting consent to malicious applications via phishing attacks when landing on malicious websites.

Below are a list of apps with permissions you might want to scrutinize for Microsoft cloud services:

- Apps with app or delegated *.ReadWrite Permissions
- Apps with delegated permissions can read, send, or manage email on behalf of the user
- Apps that are granted the using the following permissions:

RESOURCE	PERMISSION
Exchange Online	EAS.AccessAsUser.All
	EWS.AccessAsUser.All
	Mail.Read
Microsoft Graph API	Mail.Read
	Mail.Read.Shared
	Mail.ReadWrite

- Apps granted full user impersonation of the signed-in user. For example:

RESOURCE	PERMISSION
Microsoft Graph API	Directory.AccessAsUser.All
Azure REST API	user_impersonation

To avoid this scenario, you should refer to [detect and remediate illicit consent grants in Office 365](#) to identify and fix any applications with illicit grants or applications that have more grants than are necessary. Next, [remove self-service altogether](#) and [establish governance procedures](#). Finally, schedule regular reviews of app permissions and remove them when they are not needed.

Consent grants recommended reading

- [Microsoft Graph API permissions](#)

User and group settings

Below are the user and group settings that can be locked down if there isn't an explicit business need:

User settings

- **External Users** - external collaboration can happen organically in the enterprise with services like Teams, Power BI, SharePoint Online, and Azure Information Protection. If you have explicit constraints to control user-initiated external collaboration, it is recommended you enable external users by using [Azure AD Entitlement management](#) or a controlled operation such as through your help desk. If you don't want to allow organic external collaboration for services, you can [block members from inviting external users completely](#). Alternatively, you can also [allow or block specific domains](#) in external user invitations.
- **App Registrations** - when App registrations are enabled, end users can onboard applications themselves and grant access to their data. A typical example of App registration is users enabling Outlook plug-ins, or voice assistants such as Alexa and Siri to read their email and calendar or send emails on their behalf. If the customer decides to turn off App registration, the InfoSec and IAM teams must be involved in the management of exceptions (app registrations that are needed based on business requirements), as they would need to register the applications with an admin account, and most likely require designing a process to operationalize the process.
- **Administration Portal** - organizations can lock down the Azure AD blade in the Azure portal so that non-administrators can't access Azure AD management in the Azure portal and get confused. Go to the user settings in the Azure AD management portal to restrict access:

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications ⓘ

Yes No

Administration portal

Restrict access to Azure AD administration portal ⓘ

Yes No

NOTE

Non-administrators can still access to the Azure AD management interfaces via command-line and other programmatic interfaces.

Group settings

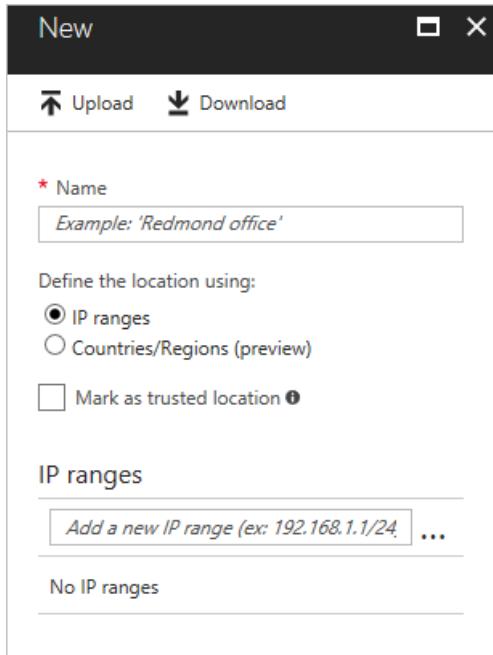
Self-Service Group Management / Users can create Security groups / Microsoft 365 groups. If there is no current self-service initiative for groups in the cloud, customers might decide to turn it off until they are ready to use this capability.

Groups recommended reading

- [What is Azure Active Directory B2B collaboration?](#)
- [Integrating Applications with Azure Active Directory](#)
- [Apps, permissions, and consent in Azure Active Directory.](#)
- [Use groups to manage access to resources in Azure Active Directory](#)
- [Setting up self-service application access management in Azure Active Directory](#)

Traffic from unexpected locations

Attackers originate from various parts of the world. Manage this risk by using conditional access policies with location as the condition. The [location condition](#) of a Conditional Access policy enables you to block access for locations from where there is no business reason to sign in from.



If available, use a security information and event management (SIEM) solution to analyze and find patterns of access across regions. If you don't use a SIEM product, or it isn't ingesting authentication information from Azure AD, we recommend you use [Azure Monitor](#) to identify patterns of access across regions.

Access usage

Azure AD logs archived and integrated with incident response plans

Having access to sign-in activity, audits and risk events for Azure AD is crucial for troubleshooting, usage analytics, and forensics investigations. Azure AD provides access to these sources through REST APIs that have a limited retention period. A security information and event management (SIEM) system, or equivalent archival technology, is key for long-term storage of audits and supportability. To enable long-term storage of Azure AD Logs, you must either add them to your existing SIEM solution or use [Azure Monitor](#). Archive logs that can be used as part of your incident response plans and investigations.

Logs recommended reading

- [Azure Active Directory audit API reference](#)
- [Azure Active Directory sign-in activity report API reference](#)
- [Get data using the Azure AD Reporting API with certificates](#)
- [Microsoft Graph for Azure Active Directory Identity Protection](#)
- [Office 365 Management Activity API reference](#)
- [How to use the Azure Active Directory Power BI Content Pack](#)

Summary

There are 12 aspects to a secure Identity infrastructure. This list will help you further secure and manage credentials, define authentication experience, delegate assignment, measure usage, and define access policies based on enterprise security posture.

- Assign owners to key tasks.
- Implement solutions to detect weak or leaked passwords, improve password management and protection, and further secure user access to resources.
- Manage the identity of devices to protect your resources at any time and from any location.
- Implement passwordless authentication.
- Provide a standardized single sign-on mechanism across the organization.
- Migrate apps from AD FS to Azure AD to enable better security and more consistent manageability.
- Assign users to applications by using groups to allow greater flexibility and ability to manage at scale.
- Configure risk-based access policies.
- Lock down legacy authentication protocols.
- Detect and remediate illicit consent grants.
- Lock down user and group settings.
- Enable long-term storage of Azure AD logs for troubleshooting, usage analytics, and forensics investigations.

Next steps

Get started with the [Identity governance operational checks and actions](#).

Azure Active Directory governance operations reference guide

4/10/2022 • 7 minutes to read • [Edit Online](#)

This section of the [Azure AD operations reference guide](#) describes the checks and actions you should take to assess and attest the access granted non-privileged and privileged identities, audit, and control changes to the environment.

NOTE

These recommendations are current as of the date of publishing but can change over time. Organizations should continuously evaluate their governance practices as Microsoft products and services evolve over time.

Key operational processes

Assign owners to key tasks

Managing Azure Active Directory requires the continuous execution of key operational tasks and processes, which may not be part of a rollout project. It is still important you set up these tasks to optimize your environment. The key tasks and their recommended owners include:

TASK	OWNER
Archive Azure AD audit logs in SIEM system	InfoSec Operations Team
Discover applications that are managed out of compliance	IAM Operations Team
Regularly review access to applications	InfoSec Architecture Team
Regularly review access to external identities	InfoSec Architecture Team
Regularly review who has privileged roles	InfoSec Architecture Team
Define security gates to activate privileged roles	InfoSec Architecture Team
Regularly review consent grants	InfoSec Architecture Team
Design Catalogs and Access Packages for applications and resources based for employees in the organization	App Owners
Define Security Policies to assign users to access packages	InfoSec team + App Owners
If policies include approval workflows, regularly review workflow approvals	App Owners
Review exceptions in security policies, such as conditional access policies, using access reviews	InfoSec Operations Team

As you review your list, you may find you need to either assign an owner for tasks that are missing an owner or

adjust ownership for tasks with owners that aren't aligned with the recommendations above.

Owner recommended reading

- [Assigning administrator roles in Azure Active Directory](#)
- [Governance in Azure](#)

Configuration changes testing

There are changes that require special considerations when testing, from simple techniques such as rolling out a target subset of users to deploying a change in a parallel test tenant. If you haven't implemented a testing strategy, you should define a test approach based on the guidelines in the table below:

SCENARIO	RECOMMENDATION
Changing the authentication type from federated to PHS/PTA or vice-versa	Use staged rollout to test the impact of changing the authentication type.
Rolling out a new conditional access (CA) policy or Identity Protection Policy	Create a new Conditional Access policy and assign to test users.
Onboarding a test environment of an application	Add the application to a production environment, hide it from the MyApp panel, and assign it to test users during the quality assurance (QA) phase.
Changing of sync rules	Perform the changes in a test Azure AD Connect with the same configuration that is currently in production, also known as staging mode, and analyze CSEport Results. If satisfied, swap to production when ready.
Changing of branding	Test in a separate test tenant.
Rolling out a new feature	If the feature supports roll out to a target set of users, identify pilot users and build out. For example, self-service password reset and multi-factor authentication can target specific users or groups.
Cutover an application from an on-premises Identity provider (IdP), for example, Active Directory, to Azure AD	If the application supports multiple IdP configurations, for example, Salesforce, configure both and test Azure AD during a change window (in case the application introduces HRD page). If the application does not support multiple IdPs, schedule the testing during a change control window and program downtime.
Update dynamic group rules	Create a parallel dynamic group with the new rule. Compare against the calculated outcome, for example, run PowerShell with the same condition. If test pass, swap the places where the old group was used (if feasible).
Migrate product licenses	Refer to Change the license for a single user in a licensed group in Azure Active Directory .
Change AD FS rules such as Authorization, Issuance, MFA	Use group claim to target subset of users.
Change AD FS authentication experience or similar farm-wide changes	Create a parallel farm with same host name, implement config changes, test from clients using HOSTS file, NLB routing rules, or similar routing. If the target platform does not support HOSTS files (for example mobile devices), control change.

Access reviews

Access reviews to applications

Over time, users may accumulate access to resources as they move throughout different teams and positions. It is important that resource owners review the access to applications on a regular basis and remove privileges that are no longer needed throughout the lifecycle of users. Azure AD [access reviews](#) enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. Resource owners should review users' access on a regular basis to make sure only the right people have continued access. Ideally, you should consider using Azure AD access reviews for this task.

Manage user's access with Azure AD Access Reviews

Recently group memberships, access to enterprise applications, and privileged role assignments with Azure Active Directory (Azure AD) Access Reviews.

Getting started is fast and easy. You can start your access review within minutes.

1. Onboard with one-click
2. Create your first access review

Use Azure AD Access Reviews to:

- ✓ Recertify employee and guest's group memberships, access to applications, and role assignments on a recurring basis
- ✓ Automate access removal with custom settings
- ✓ Make informed decisions with the help of smart recommendations
- ✓ Organize and track reviews for compliance and risk management initiatives

[Onboard now](#)

NOTE

Each user who interacts with access reviews must have a paid Azure AD Premium P2 license.

Access reviews to external identities

It is crucial to keep access to external identities constrained only to resources that are needed, during the time that is needed. Establish a regular automated access review process for all external identities and application access using Azure AD [access reviews](#). If a process already exists on-premises, consider using Azure AD access reviews. Once an application is retired or no longer used, remove all the external identities that had access to the application.

NOTE

Each user who interacts with access reviews must have a paid Azure AD Premium P2 license.

Privileged account management

Privileged account usage

Hackers often target admin accounts and other elements of privileged access to rapidly gain access to sensitive data and systems. Since users with privileged roles tend to accumulate over time, it is important to review and manage admin access on a regular basis and provide just-in-time privileged access to Azure AD and Azure resources.

If no process exists in your organization to manage privileged accounts, or you currently have admins who use their regular user accounts to manage services and resources, you should immediately begin using separate accounts, for example one for regular day-to-day activities; the other for privileged access and configured with MFA. Better yet, if your organization has an Azure AD Premium P2 subscription, then you should immediately deploy [Azure AD Privileged Identity Management \(PIM\)](#). In the same token, you should also review those privileged accounts and [assign less privileged roles](#) if applicable.

Another aspect of privileged account management that should be implemented is in defining [access reviews](#) for those accounts, either manually or [automated through PIM](#).

Privileged account management recommended reading

- [Roles in Azure AD Privileged Identity Management](#)

Emergency access accounts

Organizations must create [emergency accounts](#) to be prepared to manage Azure AD for cases such as authentication outages like:

- Outage components of authentication infrastructures (AD FS, On-premises AD, MFA service)
- Administrative staff turnover

To prevent being inadvertently locked out of your tenant because you can't sign in or activate an existing individual user's account as an administrator, you should create two or more emergency accounts and ensure they are implemented and aligned with [Microsoft's best practices](#) and [break glass procedures](#).

Privileged access to Azure EA portal

The [Azure Enterprise Agreement \(Azure EA\) portal](#) enables you to create Azure subscriptions against a master Enterprise Agreement, which is a powerful role within the enterprise. It is common to bootstrap the creation of this portal before even getting Azure AD in place, so it is necessary to use Azure AD identities to lock it down, remove personal accounts from the portal, ensure that proper delegation is in place, and mitigate the risk of lockout.

To be clear, if the EA portal authorization level is currently set to "mixed mode", you must remove any [Microsoft accounts](#) from all privileged access in the EA portal and configure the EA portal to use Azure AD accounts only. If the EA portal delegated roles aren't configured, you should also find and implement delegated roles for departments and accounts.

Privileged access recommended reading

- [Administrator role permissions in Azure Active Directory](#)

Entitlement management

[Entitlement management \(EM\)](#) allows app owners to bundle resources and assign them to specific personas in the organization (both internal and external). EM allows self-service sign up and delegation to business owners while keeping governance policies to grant access, set access durations, and allow approval workflows.

NOTE

Azure AD Entitlement Management requires Azure AD Premium P2 licenses.

Summary

There are eight aspects to a secure Identity governance. This list will help you identify the actions you should take to assess and attest the access granted to non-privileged and privileged identities, audit, and control changes to the environment.

- Assign owners to key tasks.
- Implement a testing strategy.
- Use Azure AD Access Reviews to efficiently manage group memberships, access to enterprise applications, and role assignments.
- Establish a regular, automated access review process for all types of external identities and application access.
- Establish an access review process to review and manage admin access on a regular basis and provide just-in-time privileged access to Azure AD and Azure resources.
- Provision emergency accounts to be prepared to manage Azure AD for unexpected outages.
- Lock down access to the Azure EA portal.
- Implement Entitlement Management to provide governed access to a collection of resources.

Next steps

Get started with the [Azure AD operational checks and actions](#).

Azure Active Directory general operations guide reference

4/10/2022 • 8 minutes to read • [Edit Online](#)

This section of the [Azure AD operations reference guide](#) describes the checks and actions you should take to optimize the general operations of Azure Active Directory (Azure AD).

NOTE

These recommendations are current as of the date of publishing but can change over time. Organizations should continuously evaluate their operational practices as Microsoft products and services evolve over time.

Key operational processes

Assign owners to key tasks

Managing Azure Active Directory requires the continuous execution of key operational tasks and processes, which may not be part of a rollout project. It is still important you set up these tasks to optimize your environment. The key tasks and their recommended owners include:

TASK	OWNER
Drive Improvements on Identity Secure Score	InfoSec Operations Team
Maintain Azure AD Connect Servers	IAM Operations Team
Regularly execute and triage IdFix Reports	IAM Operations Team
Triage Azure AD Connect Health Alerts for Sync and AD FS	IAM Operations Team
If not using Azure AD Connect Health, then customer has equivalent process and tools to monitor custom infrastructure	IAM Operations Team
If not using AD FS, then customer has equivalent process and tools to monitor custom infrastructure	IAM Operations Team
Monitor Hybrid Logs: Azure AD App Proxy Connectors	IAM Operations Team
Monitor Hybrid Logs: Passthrough Authentication Agents	IAM Operations Team
Monitor Hybrid Logs: Password Writeback Service	IAM Operations Team
Monitor Hybrid Logs: On-premises password protection gateway	IAM Operations Team
Monitor Hybrid Logs: Azure AD MFA NPS Extension (if applicable)	IAM Operations Team

As you review your list, you may find you need to either assign an owner for tasks that are missing an owner or

adjust ownership for tasks with owners that aren't aligned with the recommendations above.

Owners recommended reading

- [Assigning administrator roles in Azure Active Directory](#)
- [Governance in Azure](#)

Hybrid management

Recent versions of on-premises components

Having the most up-to-date versions of on-premises components provides the customer all the latest security updates, performance improvements as well as functionality that could help to further simplify the environment. Most components have an automatic upgrade setting, which will automate the upgrade process.

These components include:

- Azure AD Connect
- Azure AD Application Proxy Connectors
- Azure AD Pass-through authentication agents
- Azure AD Connect Health Agents

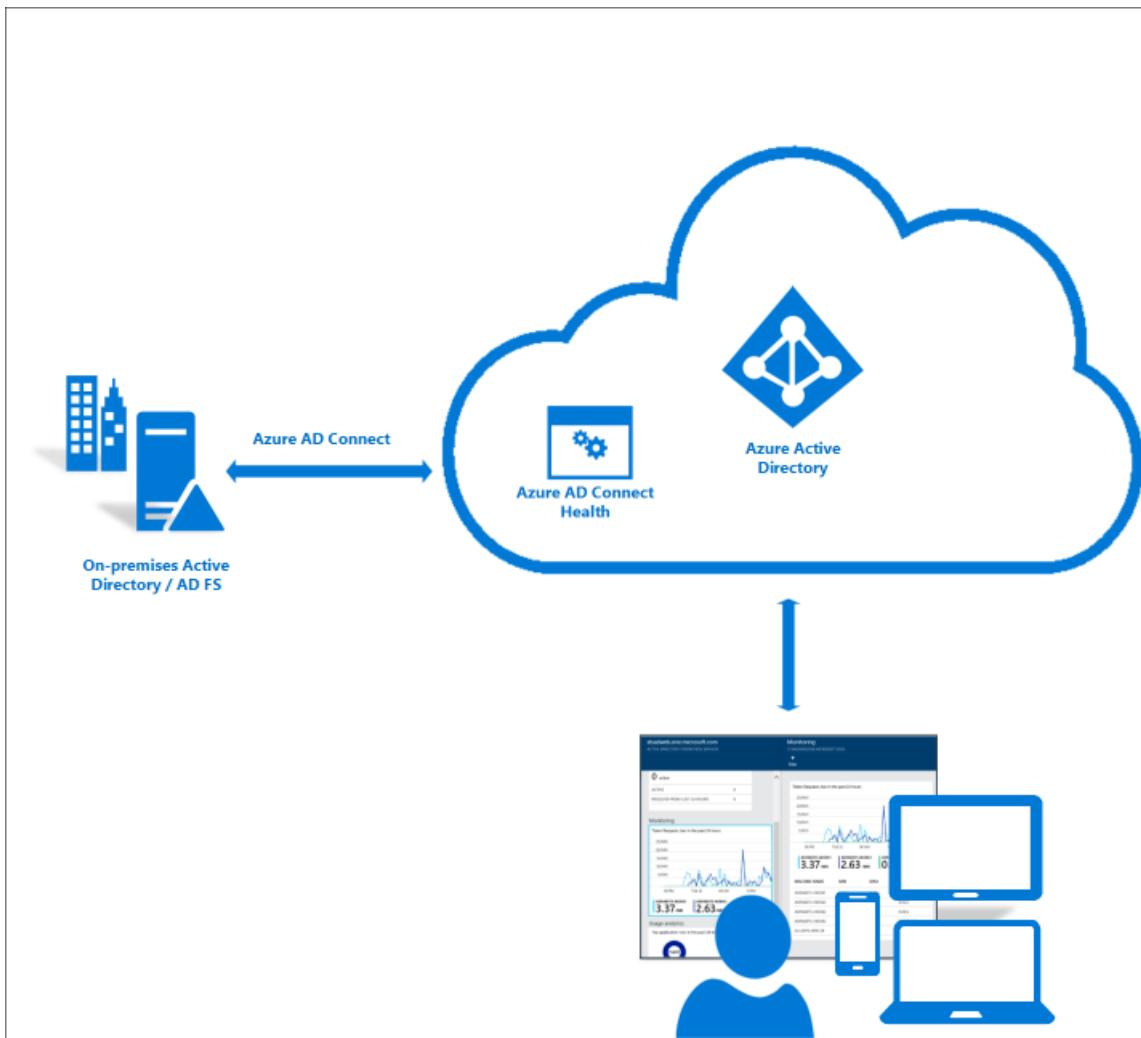
Unless one has been established, you should define a process to upgrade these components and rely on the automatic upgrade feature whenever possible. If you find components that are six or more months behind, you should upgrade as soon as possible.

Hybrid management recommended reading

- [Azure AD Connect: Automatic upgrade](#)
- [Understand Azure AD Application Proxy connectors | Automatic updates](#)

Azure AD Connect Health alert baseline

Organizations should deploy [Azure AD Connect Health](#) for monitoring and reporting of Azure AD Connect and AD FS. Azure AD Connect and AD FS are critical components that can break lifecycle management and authentication and therefore lead to outages. Azure AD Connect Health helps monitor and gain insights into your on-premises identity infrastructure thus ensuring the reliability of your environment.



As you monitor the health of your environment, you must immediately address any high severity alerts, followed by lower severity alerts.

Azure AD Connect Health recommended reading

- [Azure AD Connect Health Agent Installation](#)

On-premises agents logs

Some identity and access management services require on-premises agents to enable hybrid scenarios. Examples include password reset, pass-through authentication (PTA), Azure AD Application Proxy, and Azure AD MFA NPS extension. It is key that the operations team baseline and monitor the health of these components by archiving and analyzing the component agent logs using solutions such as System Center Operations Manager or SIEM. It is equally important your Infosec Operations team or help desk understand how to troubleshoot patterns of errors.

On-premises agents logs recommended reading

- [Troubleshoot Application Proxy](#)
- [Self-service password reset troubleshooting- Azure Active Directory](#)
- [Understand Azure AD Application Proxy connectors](#)
- [Azure AD Connect: Troubleshoot Pass-through Authentication](#)
- [Troubleshoot error codes for the Azure AD MFA NPS extension](#)

On-premises agents management

Adopting best practices can help the optimal operation of on-premises agents. Consider the following best practices:

- Multiple Azure AD Application proxy connectors per connector group are recommended to provide seamless load balancing and high availability by avoiding single points of failure when accessing the proxy

applications. If you presently have only one connector in a connector group that handles applications in production, you should deploy at least two connectors for redundancy.

- Creating and using an app proxy connector group for debugging purposes can be useful for troubleshooting scenarios and when onboarding new on-premises applications. We also recommend installing networking tools such as Message Analyzer and Fiddler in the connector machines.
- Multiple pass-through authentication agents are recommended to provide seamless load balancing and high availability by avoiding single point of failure during the authentication flow. Be sure to deploy at least two pass-through authentication agents for redundancy.

On-premises agents management recommended reading

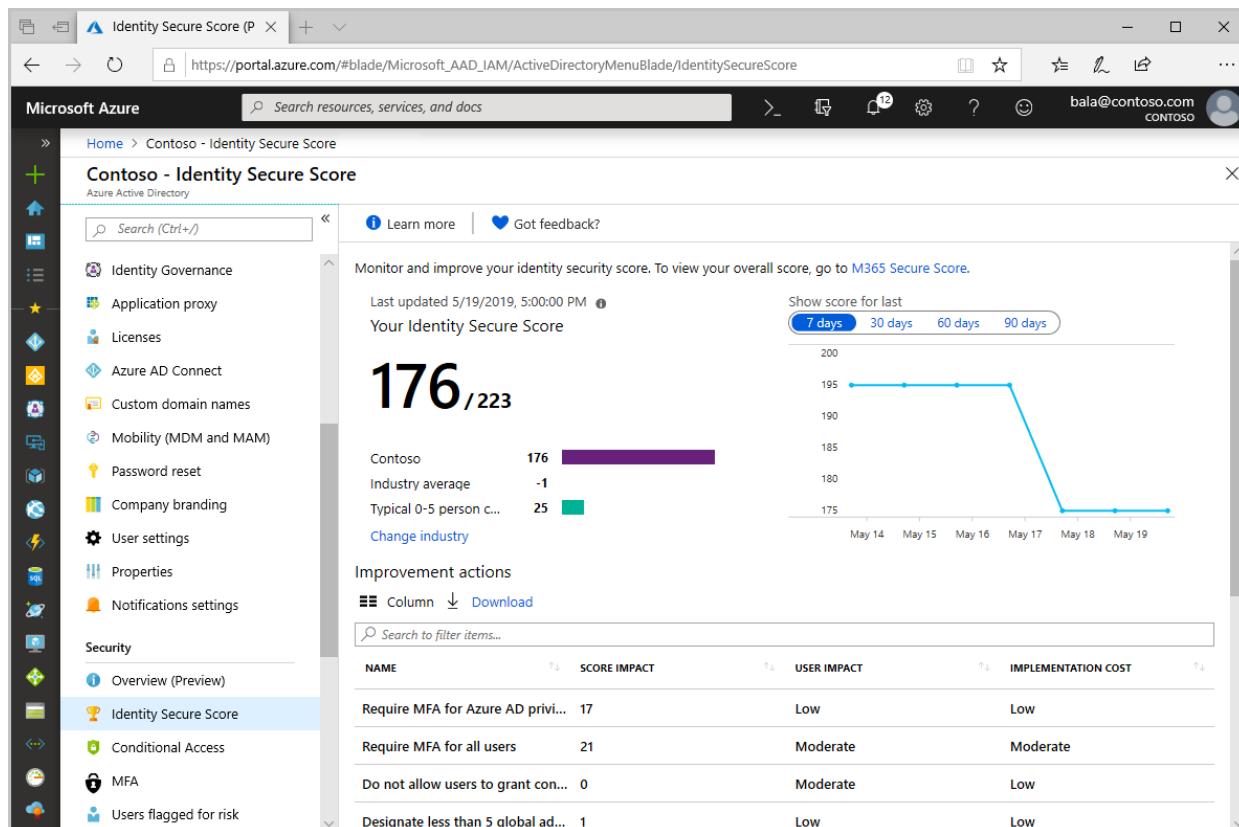
- [Understand Azure AD Application Proxy connectors](#)
- [Azure AD Pass-through Authentication - quickstart](#)

Management at scale

Identity secure score

The [identity secure score](#) provides a quantifiable measure of the security posture of your organization. It is key to constantly review and address findings reported and strive to have the highest score possible. The score helps you to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements



If your organization currently has no program in place to monitor changes in Identity Secure Score, it is recommended you implement a plan and assign owners to monitor and drive improvement actions. Organizations should remediate improvement actions with a score impact higher than 30 as soon as possible.

Notifications

Microsoft sends email communications to administrators to notify various changes in the service, configuration updates that are needed, and errors that require admin intervention. It is important that customers set the

notification email addresses so that notifications are sent to the proper team members who can acknowledge and act upon all notifications. We recommend you add multiple recipients to the [Message Center](#) and request that notifications (including Azure AD Connect Health notifications) be sent to a distribution list or shared mailbox. If you only have one global admin account with an email address, be sure to configure at least two email-capable accounts.

There are two "From" addresses used by Azure AD: o365mc@email2.microsoft.com, which sends Message Center notifications; and azure-noreply@microsoft.com, which sends notifications related to:

- [Azure AD Access Reviews](#)
- [Azure AD Connect Health](#)
- [Azure AD Identity Protection](#)
- [Azure AD Privileged Identity Management](#)
- [Enterprise App Expiring Certificate Notifications](#)
- Enterprise App Provisioning Service Notifications

Refer to the following table to learn the type of notifications that are sent and where to check for them:

NOTIFICATION SOURCE	WHAT IS SENT	WHERE TO CHECK
Technical contact	Sync errors	Azure portal - properties blade
Message Center	Incident and degradation notices of Identity Services and Microsoft 365 backend services	Office Portal
Identity Protection Weekly Digest	Identity Protection Digest	Azure AD Identity Protection blade
Azure AD Connect Health	Alert notifications	Azure portal - Azure AD Connect Health blade
Enterprise Applications Notifications	Notifications when certificates are about to expire and provisioning errors	Azure portal - Enterprise Application blade (each app has its own email address setting)

Notifications recommended reading

- [Change your organization's address, technical contact, and more](#)

Operational surface area

AD FS lockdown

Organizations, which configure applications to authenticate directly to Azure AD benefit from [Azure AD smart lockout](#). If you use AD FS in Windows Server 2012 R2, implement AD FS [extranet lockout protection](#). If you use AD FS on Windows Server 2016 or later, implement [extranet smart lockout](#). At a minimum, we recommend you enable extranet lockout to contain the risk of brute force attacks against on-premises Active Directory. However, if you have AD FS in Windows 2016 or higher, you should also enable extranet smart lockout that will help to mitigate [password spray](#) attacks.

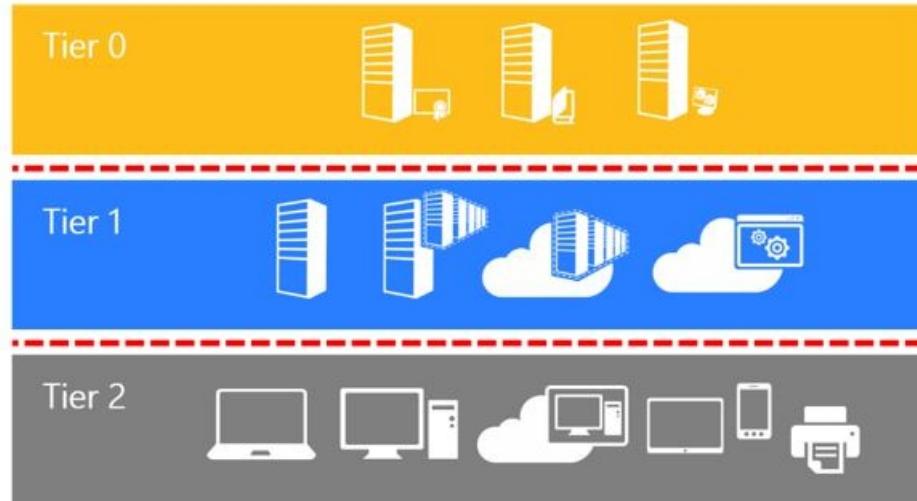
If AD FS is only used for Azure AD federation, there are some endpoints that can be turned off to minimize the attack surface area. For example, if AD FS is only used for Azure AD, you should disable WS-Trust endpoints other than the endpoints enabled for **usernamemixed** and **windowstransport**.

Access to machines with on-premises identity components

Organizations should lock down access to the machines with on-premises hybrid components in the same way as your on-premises domain. For example, a backup operator or Hyper-V administrator should not be able to

log in to the Azure AD Connect Server to change rules.

The Active Directory administrative tier model was designed to protect identity systems using a set of buffer zones between full control of the Environment (Tier 0) and the high-risk workstation assets that attackers



frequently compromise.

The [tier model](#) is composed of three levels and only includes administrative accounts, not standard user accounts.

- **Tier 0** - Direct Control of enterprise identities in the environment. Tier 0 includes accounts, groups, and other assets that have direct or indirect administrative control of the Active Directory forest, domains, or domain controllers, and all the assets in it. The security sensitivity of all Tier 0 assets is equivalent as they are all effectively in control of each other.
- **Tier 1** - Control of enterprise servers and applications. Tier 1 assets include server operating systems, cloud services, and enterprise applications. Tier 1 administrator accounts have administrative control of a significant amount of business value that is hosted on these assets. A common example role is server administrators who maintain these operating systems with the ability to impact all enterprise services.
- **Tier 2** - Control of user workstations and devices. Tier 2 administrator accounts have administrative control of a significant amount of business value that is hosted on user workstations and devices. Examples include Help Desk and computer support administrators because they can impact the integrity of almost any user data.

Lock down access to on-premises identity components such as Azure AD Connect, AD FS, and SQL services the same way as you do for domain controllers.

Summary

There are seven aspects to a secure Identity infrastructure. This list will help you find the actions you should take to optimize the operations for Azure Active Directory (Azure AD).

- Assign owners to key tasks.
- Automate the upgrade process for on-premises hybrid components.
- Deploy Azure AD Connect Health for monitoring and reporting of Azure AD Connect and AD FS.
- Monitor the health of on-premises hybrid components by archiving and analyzing the component agent logs using System Center Operations Manager or a SIEM solution.
- Implement security improvements by measuring your security posture with Identity Secure Score.
- Lock down AD FS.
- Lock down access to machines with on-premises identity components.

Next steps

Refer to the [Azure AD deployment plans](#) for implementation details on any capabilities you haven't deployed.

Azure Active Directory security operations guide

4/10/2022 • 12 minutes to read • [Edit Online](#)

Microsoft has a successful and proven approach to [Zero Trust security](#) using [Defense in Depth](#) principles that leverage identity as a control plane. As organizations continue to embrace a hybrid workload world for scale, cost savings, and security, Azure Active Directory (Azure AD) plays a pivotal role in your strategy for identity management. Recently, news surrounding identity and security compromise has increasingly prompted enterprise IT to consider their identity security posture as a measurement of defensive security success.

Increasingly, organizations must embrace a mixture of on-premises and cloud applications, which users access with both on-premises and cloud-only accounts. Managing users, applications, and devices both on-premises and in the cloud poses challenging scenarios.

Azure Active Directory creates a common user identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.

To achieve hybrid identity with Azure AD, one of three authentication methods can be used, depending on your scenarios. The three methods are:

- [Password hash synchronization \(PHS\)](#)
- [Pass-through authentication \(PTA\)](#)
- [Federation \(AD FS\)](#)

As you audit your current security operations or establish security operations for your Azure environment, we recommend you:

- Read specific portions of the Microsoft security guidance to establish a baseline of knowledge about securing your cloud-based or hybrid Azure environment.
- Audit your account and password strategy and authentication methods to help deter the most common attack vectors.
- Create a strategy for continuous monitoring and alerting on activities that might indicate a security threat.

Audience

The Azure AD SecOps Guide is intended for enterprise IT identity and security operations teams and managed service providers that need to counter threats through better identity security configuration and monitoring profiles. This guide is especially relevant for IT administrators and identity architects advising Security Operations Center (SOC) defensive and penetration testing teams to improve and maintain their identity security posture.

Scope

This introduction provides the suggested prereading and password audit and strategy recommendations. This article also provides an overview of the tools available for hybrid Azure environments as well as fully cloud-based Azure environments. Finally, we provide a list of data sources you can use for monitoring and alerting and configuring your security information and event management (SIEM) strategy and environment. The rest of the guidance presents monitoring and alerting strategies in the following areas:

- [User accounts](#) – Guidance specific to non-privileged user accounts without administrative privilege,

including anomalous account creation and usage, and unusual sign-ins.

- [Privileged accounts](#) – Guidance specific to privileged user accounts that have elevated permissions to perform administrative tasks, including Azure AD role assignments, Azure resource role assignments, and access management for Azure resources and subscriptions.
- [Privileged Identity Management \(PIM\)](#) – guidance specific to using PIM to manage, control, and monitor access to resources.
- [Applications](#) – Guidance specific to accounts used to provide authentication for applications.
- [Devices](#) – Guidance specific to monitoring and alerting for devices registered or joined outside of policies, non-compliant usage, managing device administration roles, and sign-ins to virtual machines.
- [Infrastructure](#)– Guidance specific to monitoring and alerting on threats to your hybrid and purely cloud-based environments.

Important reference content

Microsoft has many products and services that enable you to customize your IT environment to fit your needs. We recommend as part of your monitoring and alerting strategy you review the following guidance that is relevant to your operating environment:

- Windows operating systems
 - [Windows 10 and Windows Server 2016 security auditing and monitoring reference](#)
 - [Security baseline \(FINAL\) for Windows 10 v1909 and Windows Server v1909](#)
 - [Security baseline for Windows 11](#)
 - [Security baseline for Windows Server 2022](#)
- On-premises environments
 - [Microsoft Defender for Identity architecture](#)
 - [Connect Microsoft Defender for Identity to Active Directory quickstart](#)
 - [Azure security baseline for Microsoft Defender for Identity](#)
 - [Monitoring Active Directory for Signs of Compromise](#)
- Cloud-based Azure environments
 - [Monitor sign-ins with the Azure AD sign-in log](#)
 - [Audit activity reports in the Azure Active Directory portal](#)
 - [Investigate risk with Azure Active Directory Identity Protection](#)
 - [Connect Azure AD Identity Protection data to Microsoft Sentinel](#)
- Active Directory Domain Services (AD DS)
 - [Audit Policy Recommendations](#)
- Active Directory Federation Services (AD FS)
 - [AD FS Troubleshooting - Auditing Events and Logging](#)

Data sources

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Sign-in logs](#)
- [Microsoft 365 Audit logs](#)
- [Azure Key Vault logs](#)

From the Azure portal you can view the Azure AD Audit logs and download as comma separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- **Microsoft Sentinel** – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- **Azure Monitor** – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- **Azure Event Hubs integrated with a SIEM** - [Azure AD logs can be integrated to other SIEMs](#) such as Splunk, ArcSight, QRadar and Sumo Logic via the Azure Event Hub integration.
- **Microsoft Defender for Cloud Apps** – enables you to discover and manage apps, govern across apps and resources, and check the compliance of your cloud apps.

Much of what you will monitor and alert on are the effects of your Conditional Access policies. You can use the [Conditional Access insights and reporting workbook](#) to examine the effects of one or more Conditional Access policies on your sign-ins, as well as the results of policies, including device state. This workbook enables you to view an impact summary, and identify the impact over a specific time period. You can also use the workbook to investigate the sign-ins of a specific user.

The remainder of this article describes what we recommend you monitor and alert on, and is organized by the type of threat. Where there are specific pre-built solutions we link to them or provide samples following the table. Otherwise, you can build alerts using the preceding tools.

- **Identity Protection** -- generates three key reports that you can use to help with your investigation:
 - **Risky users** – contains information about which users are at risk, details about detections, history of all risky sign-ins, and risk history.
 - **Risky sign-ins** – contains information surrounding the circumstance of a sign-in that might indicate suspicious circumstances. For additional information on investigating information from this report, visit [How To: Investigate risk](#).
 - **Risk detections** - contains information on risk signals detected by Azure AD Identity Protection that informs sign-in and user risk. For more information, see the [Azure AD security operations guide for user accounts](#).

Data sources for domain controller monitoring

For the best results, we recommend that you monitor your domain controllers using Microsoft Defender for Identity. This will enable you for the best detection and automation capabilities. Please follow the guidance from:

- [Microsoft Defender for Identity architecture](#)
- [Connect Microsoft Defender for Identity to Active Directory quickstart](#)

If you do not plan to use Microsoft Defender for identity, you can [monitor your domain controllers either by event log messages](#) or by [running PowerShell cmdlets](#).

Components of hybrid authentication

As part of an Azure hybrid environment, the following should be baselined and included in your monitoring and alerting strategy.

- **PTA Agent** – The Pass-through authentication agent is used to enable pass-through authentication and is installed on-premises. See [Azure AD Pass-through Authentication agent: Version release history](#) for information on verifying your agent version and next steps.
- **AD FS/WAP** – Azure Active Directory Federation Services (Azure AD FS) and Web Application Proxy (WAP) enable secure sharing of digital identity and entitlement rights across your security and enterprise boundaries. For information on security best practices, see [Best practices for securing Active Directory Federation Services](#).
- **Azure AD Connect Health Agent** – The agent used to provide a communications link for Azure AD Connect Health. For information on installing the agent, see [Azure AD Connect Health agent installation](#).
- **Azure AD Connect Sync Engine** - The on-premises component, also called the sync engine. For information on the feature, see [Azure AD Connect sync service features](#).
- **Password Protection DC agent** – Azure password protection DC agent is used to help with monitoring and reporting event log messages. For information, see [Enforce on-premises Azure AD Password Protection for Active Directory Domain Services](#).
- **Password Filter DLL** – The password filter DLL of the DC Agent receives user password-validation requests from the operating system. The filter forwards them to the DC Agent service that's running locally on the DC. For information on using the DLL, see [Enforce on-premises Azure AD Password Protection for Active Directory Domain Services](#).
- **Password writeback Agent** – Password writeback is a feature enabled with [Azure AD Connect](#) that allows password changes in the cloud to be written back to an existing on-premises directory in real time. For more information on this feature, see [How does self-service password reset writeback work in Azure Active Directory?](#)
- **Azure AD Application Proxy Connector** – Lightweight agents that sit on-premises and facilitate the outbound connection to the Application Proxy service. For more information, see [Understand Azure ADF Application Proxy connectors](#).

Components of cloud-based authentication

As part of an Azure cloud-based environment, the following should be baselined and included in your monitoring and alerting strategy.

- **Azure AD Application Proxy** – This cloud service provides secure remote access to on-premises web applications. For more information, see [Remote access to on-premises applications through Azure AD Application Proxy](#).
- **Azure AD Connect** – Services used for an Azure AD Connect solution. For more information, see [What is Azure AD Connect](#).
- **Azure AD Connect Health** – Service Health provides you with a customizable dashboard which tracks the health of your Azure services in the regions where you use them. For more information, see [Azure AD Connect Health](#).
- **Azure MFA** – Azure AD Multi-Factor Authentication requires a user to provide more than one form of proof for authentication. This can provide a proactive first step to securing your environment. For more information, see [How it works: Azure AD Multi-Factor Authentication](#).

- **Dynamic Groups** – Dynamic configuration of security group membership for Azure Active Directory (Azure AD) Administrators can set rules to populate groups that are created in Azure AD based on user attributes. For more information, see [Dynamic groups and Azure Active Directory B2B collaboration](#).
- **Conditional Access** – Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane. For more information, see [What is Conditional Access](#).
- **Identity Protection** – A tool that enables organizations to automate the detection and remediation of identity-based risks, investigate risks using data in the portal, and export risk detection data to your SIEM. For more information, see [What is Identity Protection?](#)
- **Group-based licensing** – Licenses can be assigned to groups rather than directly to users. Azure AD stores information about license assignment states for users.
- **Provisioning Service** – Provisioning refers to creating user identities and roles in the cloud applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change. For more information, see [How Application Provisioning works in Azure Active Directory](#).
- **Graph API** – The Microsoft Graph API is a RESTful web API that enables you to access Microsoft Cloud service resources. After you register your app and get authentication tokens for a user or service, you can make requests to the Microsoft Graph API. For more information, see [Overview of Microsoft Graph](#).
- **Domain Service** – Azure Active Directory Domain Services (AD DS) provides managed domain services such as domain join, group policy. For more information, see [What is Azure Active Directory Domain Services?](#)
- **Azure Resource Manager** – Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. For more information, see [What is Azure Resource Manager](#)?
- **Managed Identity** – Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. For more information, see [What are managed identities for Azure resources?](#)
- **Privileged Identity Management** – Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. For more information, see [What is Azure AD Privileged Identity Management](#).
- **Access Reviews** – Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access. For more information, see [What are Azure AD access reviews?](#)
- **Entitlement Management** – Azure Active Directory (Azure AD) entitlement management is an [identity governance](#) feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration. For more information, see [What is Azure AD entitlement management](#)?
- **Activity Logs** – The Activity log is a [platform log](#) in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started. For more information, see [Azure Activity log](#).
- **Self-service Password reset service** – Azure Active Directory (Azure AD) self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. For more information, see [How it works: Azure AD self-service password reset](#).

- **Device Services** – Device identity management is the foundation for [device-based Conditional Access](#). With device-based Conditional Access policies, you can ensure that access to resources in your environment is only possible with managed devices. For more information, see [What is a device identity?](#)
- **Self-Service Group Management** – You can enable users to create and manage their own security groups or Microsoft 365 groups in Azure Active Directory (Azure AD). The owner of the group can approve or deny membership requests and can delegate control of group membership. Self-service group management features are not available for mail-enabled security groups or distribution lists. For more information, see [Set up self-service group management in Azure Active Directory](#).
- **Risk detections** – contains information about other risks triggered when a risk is detected and other pertinent information such as sign-in location and any details from Microsoft Defender for Cloud Apps.

Next steps

See these security operations guide articles:

[Azure AD security operations overview](#)

[Security operations for user accounts](#)

[Security operations for privileged accounts](#)

[Security operations for Privileged Identity Management](#)

[Security operations for applications](#)

[Security operations for devices](#)

[Security operations for infrastructure](#)

Azure Active Directory security operations for user accounts

4/10/2022 • 23 minutes to read • [Edit Online](#)

User identity is one of the most important aspects of protecting your organization and data. This article provides guidance for monitoring account creation, deletion, and account usage. The first portion covers how to monitor for unusual account creation and deletion. The second portion covers how to monitor for unusual account usage.

If you have not yet read the [Azure Active Directory \(Azure AD\) security operations overview](#), we recommend you do so before proceeding.

This article covers general user accounts. For privileged accounts, see [Security operations – privileged accounts](#).

Define a baseline

To discover anomalous behavior, you first must define what normal and expected behavior is. Defining what expected behavior for your organization is, helps you determine when unexpected behavior occurs. The definition also helps to reduce the noise level of false positives when monitoring and alerting.

Once you define what you expect, you perform baseline monitoring to validate your expectations. With that information, you can monitor the logs for anything that falls outside of tolerances you define.

Use the Azure AD Audit Logs, Azure AD Sign-in Logs, and directory attributes as your data sources for accounts created outside of normal processes. The following are suggestions to help you think about and define what normal is for your organization.

- **Users account creation** – evaluate the following:
 - Strategy and principles for tools and processes used for creating and managing user accounts. For example, are there standard attributes, formats that are applied to user account attributes.
 - Approved sources for account creation. For example, originating in Active Directory (AD), Azure Active Directory or HR systems like Workday.
 - Alert strategy for accounts created outside of approved sources. Is there a controlled list of organizations your organization collaborates with?
 - Provisioning of guest accounts and alert parameters for accounts created outside of entitlement management or other normal processes.
 - Strategy and alert parameters for accounts created, modified, or disabled by an account that is not an approved user administrator.
 - Monitoring and alert strategy for accounts missing standard attributes, such as employee ID or not following organizational naming conventions.
 - Strategy, principles, and process for account deletion and retention.
- **On-premises user accounts** – evaluate the following for accounts synced with Azure AD Connect:
 - The forests, domains, and organizational units (OUs) in scope for synchronization. Who are the approved administrators who can change these settings and how often is the scope checked?

- The types of accounts that are synchronized. For example, user accounts and or service accounts.
- The process for creating privileged on-premises accounts and how the synchronization of this type of account is controlled.
- The process for creating on-premises user accounts and how the synchronization of this type of account is managed.

For more information for securing and monitoring on-premises accounts, see [Protecting Microsoft 365 from on-premises attacks](#).

- **Cloud user accounts** – evaluate the following:

- The process to provision and manage cloud accounts directly in Azure AD.
- The process to determine the types of users provisioned as Azure AD cloud accounts. For example, do you only allow privileged accounts or do you also allow user accounts?
- The process to create and maintain a list of trusted individuals and or processes expected to create and manage cloud user accounts.
- The process to create and maintained an alert strategy for non-approved cloud-based accounts.

Where to look

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Sign-in logs](#)
- [Microsoft 365 Audit logs](#)
- [Azure Key Vault logs](#)
- [Risky Users log](#)
- [UserRiskEvents log](#)

From the Azure portal you can view the Azure AD Audit logs and download as comma separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- **Microsoft Sentinel** – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- **Azure Monitor** – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- **Azure Event Hubs integrated with a SIEM** - [Azure AD logs can be integrated to other SIEMs](#) such as Splunk, ArcSight, QRadar and Sumo Logic via the Azure Event Hub integration.
- **Microsoft Defender for Cloud Apps** – enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.

Much of what you will monitor and alert on are the effects of your Conditional Access policies. You can use the [Conditional Access insights and reporting workbook](#) to examine the effects of one or more Conditional Access policies on your sign-ins, as well as the results of policies, including device state. This workbook enables you to view an impact summary, and identify the impact over a specific time period. You can also use the workbook to investigate the sign-ins of a specific user.

The remainder of this article describes what we recommend you monitor and alert on, and is organized by the type of threat. Where there are specific pre-built solutions we link to them or provide samples following the table. Otherwise, you can build alerts using the preceding tools.

Account creation

Anomalous account creation can indicate a security issue. Short lived accounts, accounts not following naming standards, and accounts created outside of normal processes should be investigated.

Short-lived accounts

Account creation and deletion outside of normal identity management processes should be monitored in Azure AD. Short-lived accounts are accounts created and deleted in a short time span. This type of account creation and quick deletion could mean a bad actor is trying to avoid detection by creating accounts, using them, and then deleting the account.

Short-lived account patterns might indicate non-approved people or processes might have the right to create and delete accounts that fall outside of established processes and policies. This type of behavior removes visible markers from the directory.

If the data trail for account creation and deletion is not discovered quickly, the information required to investigate an incident may no longer exist. For example, accounts might be deleted and then purged from the recycle bin. Audit logs are retained for 30 days. However, you can export your logs to Azure Monitor or a security information and event management (SIEM) solution for longer term retention.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Account creation and deletion events within a close time frame.	High	Azure AD Audit logs	Activity: Add user Status = success -and- Activity: Delete user Status = success	Search for user principal name (UPN) events. Look for accounts created and then deleted in under 24 hours. Microsoft Sentinel template
Accounts created and deleted by non-approved users or processes.	Medium	Azure AD Audit logs	Initiated by (actor) – USER PRINCIPAL NAME -and- Activity: Add user Status = success and-or Activity: Delete user Status = success	If the actor are non-approved users, configure to send an alert. Microsoft Sentinel template
Accounts from non-approved sources.	Medium	Azure AD Audit logs	Activity: Add user Status = success Target(s) = USER PRINCIPAL NAME	If the entry is not from an approved domain or is a known blocked domain, configure to send an alert.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Accounts assigned to a privileged role.	High	Azure AD Audit logs	Activity: Add user Status = success -and- Activity: Delete user Status = success -and- Activity: Add member to role Status = success	If the account is assigned to an Azure AD role, Azure role, or privileged group membership, alert and prioritize the investigation. Microsoft Sentinel template

Both privileged and non-privileged accounts should be monitored and alerted. However, since privileged accounts have administrative permissions, they should have higher priority in your monitor, alert, and respond processes.

Accounts not following naming policies

User accounts not following naming policies might have been created outside of organizational policies.

A best practice is to have a naming policy for user objects. Having a naming policy makes management easier and helps provide consistency. The policy can also help discover when users have been created outside of approved processes. A bad actor might not be aware of your naming standards and might make it easier to detect an account provisioned outside of your organizational processes.

Organizations tend to have specific formats and attributes that are used for creating user and or privileged accounts. For example:

- Admin account UPN = ADM_firstname.lastname@tenant.onmicrosoft.com
- User account UPN = Firstname.Lastname@contoso.com

User accounts also frequently have an attribute that identifies a real user. For example, EMPID = XXXNNNN. The following are suggestions to help you think about and define what normal is for your organization, as well as thing to consider when defining your baseline for log entries where accounts don't follow your organization's naming convention:

- Accounts that don't follow the naming convention. For example, `nnnnnnn@contoso.com` versus `firstname.lastname@contoso.com`.
- Accounts that don't have the standard attributes populated or are not in the correct format. For example, not having a valid employee ID.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
User accounts that do not have expected attributes defined.	Low	Azure AD Audit logs	Activity: Add user Status = success	Look for accounts with your standard attributes either null or in the wrong format. For example, EmployeeID
User accounts created using incorrect naming format.	Low	Azure AD Audit logs	Activity: Add user Status = success	Look for accounts with a UPN that does not follow your naming policy.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Privileged accounts that do not follow naming policy.	High	Azure Subscription	List Azure role assignments using the Azure portal - Azure RBAC	List role assignments for subscriptions and alert where sign in name does not match your organizations format. For example, ADM_ as a prefix.
Privileged accounts that do not follow naming policy.	High	Azure AD directory	List Azure AD role assignments	List roles assignments for Azure AD roles alert where UPN does not match your organizations format. For example, ADM_ as a prefix.

For more information on parsing, see:

- For Azure AD Audit logs - [Parse text data in Azure Monitor Logs](#)
- For Azure Subscriptions - [List Azure role assignments using Azure PowerShell](#)
- For Azure Active Directory - [List Azure AD role assignments](#)

Accounts created outside normal processes

Having standard processes to create users and privileged accounts is important so that you can securely control the lifecycle of identities. If users are provisioned and deprovisioned outside of established processes, it can introduce security risks. Operating outside of established processes can also introduce identity management problems. Potential risks include:

- User and privileged accounts might not be governed to adhere to organizational policies. This can lead to a wider attack surface on accounts that are not managed correctly.
- It becomes harder to detect when bad actors create accounts for malicious purposes. By having valid accounts created outside of established procedures, it becomes harder to detect when accounts are created, or permissions modified for malicious purposes.

We recommend that user and privileged accounts only be created following your organization policies. For example, an account should be created with the correct naming standards, organizational information and under scope of the appropriate identity governance. Organizations should have rigorous controls for who has the rights to create, manage, and delete identities. Roles to create these accounts should be tightly managed and the rights only available after following an established workflow to approve and obtain these permissions.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
User accounts created or deleted by non-approved users or processes.	Medium	Azure AD Audit logs	Activity: Add user Status = success and-or- Activity: Delete user Status = success -and- Initiated by (actor) = USER PRINCIPAL NAME	Alert on accounts created by non-approved users or processes. Prioritize accounts created with heightened privileges. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
User accounts created or deleted from non-approved sources.	Medium	Azure AD Audit logs	Activity: Add user Status = success -or- Activity: Delete user Status = success -and- Target(s) = USER PRINCIPAL NAME	Alert when the domain is non-approved or known blocked domain.

Unusual sign ins

Seeing failures for user authentication is normal. But seeing patterns or blocks of failures can be an indicator that something is happening with a user's Identity. For example, in the case of Password spray or Brute Force attacks, or when a user account is compromised. It is critical that you monitor and alert when patterns emerge. This helps ensure you can protect the user and your organization's data.

Success appears to say all is well. But it can mean that a bad actor has successfully accessed a service. Monitoring successful logins helps you detect user accounts that are gaining access but are not user accounts that should have access. User authentication successes are normal entries in Azure AD Sign-Ins logs. We recommend you monitor and alert to detect when patterns emerge. This helps ensure you can protect user accounts and your organization's data.

As you design and operationalize a log monitoring and alerting strategy, consider the tools available to you through the Azure portal. Identity Protection enables you to automate the detection, protection, and remediation of identity-based risks. Identity protection uses intelligence-fed machine learning and heuristic systems to detect risk and assign a risk score for users and sign ins. Customers can configure policies based on a risk level for when to allow or deny access or allow the user to securely self-remediate from a risk. The following Identity Protection risk detections inform risk levels today:

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Leaked credentials user risk detection	High	Azure AD Risk Detection logs	UX: Leaked credentials API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Azure AD Threat Intelligence user risk detection	High	Azure AD Risk Detection logs	UX: Azure AD threat intelligence API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Anonymous IP address sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Anonymous IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Atypical travel sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Atypical travel API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Anomalous Token	Varies	Azure AD Risk Detection logs	UX: Anomalous Token API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Malware linked IP address sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Malware linked IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Suspicious browser sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Suspicious browser API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Unfamiliar sign-in properties sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Unfamiliar sign-in properties API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Malicious IP address sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Malicious IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Suspicious inbox manipulation rules sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Suspicious inbox manipulation rules API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Password Spray sign-in risk detection	High	Azure AD Risk Detection logs	UX: Password spray API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Impossible travel sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Impossible travel API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
New country sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: New country API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Activity from anonymous IP address sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Activity from Anonymous IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Suspicious inbox forwarding sign-in risk detection	Varies	Azure AD Risk Detection logs	UX: Suspicious inbox forwarding API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection
Azure AD threat intelligence sign-in risk detection	High	Azure AD Risk Detection logs	UX: Azure AD threat intelligence API: See riskDetection resource type - Microsoft Graph	See What is risk? Azure AD Identity Protection

For more information, visit [What is Identity Protection](#).

What to look for

Configure monitoring on the data within the Azure AD Sign-ins Logs to ensure that alerting occurs and adheres to your organization's security policies. Some examples of this are:

- **Failed Authentications:** As humans we all get our passwords wrong from time to time. However, many failed authentications can indicate that a bad actor is trying to obtain access. Attacks differ in ferocity but can range from a few attempts per hour to a much higher rate. For example, Password Spray normally preys on easier passwords against many accounts, while Brute Force attempts many passwords against targeted accounts.
- **Interrupted Authentications:** An interrupt in Azure AD represents an injection of an additional process

to satisfy authentication, such as when enforcing a control in a CA policy. This is a normal event and can happen when applications are not configured correctly. But when you see many interrupts for a user account it could indicate something is happening with that account.

- For example, if you filtered on a user in Sign-in logs and see a large volume of sign in status = Interrupted and Conditional Access = Failure. Digging deeper it may show in authentication details that the password is correct, but that strong authentication is required. This could mean the user is not completing multi-factor authentication (MFA) which could indicate the user's password is compromised and the bad actor is unable to fulfill MFA.
- **Smart lock out:** Azure AD provides a smart lockout service which introduces the concept of familiar and non-familiar locations to the authentication process. A user account visiting a familiar location might authenticate successfully while a bad actor unfamiliar with the same location is blocked after several attempts. Look for accounts that have been locked out and investigate further.
- **IP Changes:** It is normal to see users originating from different IP addresses. However, Zero Trust states never trust and always verify. Seeing a large volume of IP addresses and failed sign ins can be an indicator of intrusion. Look for a pattern of many failed authentications taking place from multiple IP addresses. Note, virtual private network (VPN) connections can cause false positives. Regardless of the challenges, we recommend you monitor for IP address changes and if possible, use Azure AD Identity Protection to automatically detect and mitigate these risks.
- **Locations:** Generally, you expect a user account to be in the same geographical location. You also expect sign ins from locations where you have employees or business relations. When the user account comes from a different international location in less time than it would take to travel there, it can indicate the user account is being abused. Note, VPNs can cause false positives, we recommend you monitor for user accounts signing in from geographically distant locations and if possible, use Azure AD Identity Protection to automatically detect and mitigate these risks.

For this risk area we recommend you monitor both standard user accounts and privileged accounts but prioritize investigations of privileged accounts. Privileged accounts are the most important accounts in any Azure AD tenant. For specific guidance for privileged accounts, see Security operations – privileged accounts.

How to detect

You use Azure Identity Protection and the Azure AD sign-in logs to help discover threats indicated by unusual sign-in characteristics. Information about Identity Protection is available at [What is Identity Protection](#). You can also replicate the data to Azure Monitor or a SIEM for monitoring and alerting purposes. To define normal for your environment and to set a baseline, determine the following:

- the parameters that you consider normal for your user base.
- the average number of tries of a password over a time before the user calls the service desk or performs a self-service password reset.
- how many failed attempts you want to allow before alerting, and if it will be different for user accounts and privileged accounts.
- how many MFA attempts you want to allow before alerting, and if it will be different for user accounts and privileged accounts.
- if legacy authentication is enabled and your roadmap for discontinuing usage.
- the known egress IP addresses are for your organization.
- the countries your users operate from.
- whether there are groups of users that remain stationary within a network location or country.
- Identify any other indicators for unusual sign ins that are specific to your organization. For example days

or times of the week or year that your organization does not operate.

Once you have scoped what normal is for the types of accounts in your environment, consider the following to help determine which scenarios you want to monitor for and alert on, and to fine-tune your alerting.

- Do you need to monitor and alert if Identity Protection is configured?
- Are there stricter conditions applied to privileged accounts that you can use to monitor and alert on? For example, requiring privileged accounts only be used from trusted IP addresses.
- Are the baselines you set too aggressive? Having too many alerts might result in alerts being ignored or missed.

Configure Identity Protection to help ensure protection is in place that supports your security baseline policies. For example, blocking users if risk = high. This risk level indicates with a high degree of confidence that a user account is compromised. For more information on setting up sign in risk policies and user risk policies, visit [Identity Protection policies](#). For more information on setting up conditional access, visit [Conditional Access: Sign-in risk-based Conditional Access](#).

The following are listed in order of importance based on the impact and severity of the entries.

Monitoring for failed unusual sign ins

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Failed sign-in attempts.	Medium - if Isolated Incident High - if a number of accounts are experiencing the same pattern or a VIP.	Azure AD Sign-ins log	Status = failed -and- Sign-in error code 50126 - Error validating credentials due to invalid username or password.	Define a baseline threshold, and then monitor and adjust to suite your organizational behaviors and limit false alerts from being generated. Azure Sentinel template
Smart lock-out events.	Medium - if Isolated Incident High - if a number of accounts are experiencing the same pattern or a VIP.	Azure AD Sign-ins log	Status = failed -and- Sign-in error code = 50053 – IdsLocked	Define a baseline threshold, and then monitor and adjust to suite your organizational behaviors and limit false alerts from being generated. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Interruptions	Medium - if Isolated Incident High - if a number of accounts are experiencing the same pattern or a VIP.	Azure AD Sign-ins log	500121, Authentication failed during strong authentication request. -or- 50097, Device authentication is required or 50074, Strong Authentication is required. -or- 50155, DeviceAuthentication Failed -or- 50158, ExternalSecurityChallenge - External security challenge was not satisfied -or- 53003 and Failure reason = blocked by CA	Monitor and alert on interruptions. Define a baseline threshold, and then monitor and adjust to suite your organizational behaviors and limit false alerts from being generated. Azure Sentinel template

The following are listed in order of importance based on the impact and severity of the entries.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Multi-factor authentication (MFA) fraud alerts.	High	Azure AD Sign-ins log	Status = failed -and- Details = MFA Denied	Monitor and alert on any entry. Azure Sentinel template
Failed authentications from countries you do not operate out of.	Medium	Azure AD Sign-ins log	Location = <unapproved location>	Monitor and alert on any entries.
Failed authentications for legacy protocols or protocols that are not used .	Medium	Azure AD Sign-ins log	Status = failure -and- Client app = Other Clients, POP, IMAP, MAPI, SMTP, ActiveSync	Monitor and alert on any entries. Azure Sentinel template
Failures blocked by CA.	Medium	Azure AD Sign-ins log	Error code = 53003 -and- Failure reason = blocked by CA	Monitor and alert on any entries. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Increased failed authentications of any type.	Medium	Azure AD Sign-ins log	Capture increases in failures across the board. I.e., total failures for today is >10 % on the same day the previous week.	If you don't have a set threshold, monitor and alert if failures increase by 10% or greater. Azure Sentinel template
Authentication occurring at times and days of the week when countries do not conduct normal business operations.	Low	Azure AD Sign-ins log	Capture interactive authentication occurring outside of normal operating days\time. Status = success -and- Location = <location> -and- Day\Time = <not normal working hours>	Monitor and alert on any entries. Azure Sentinel template
Account disabled/blocked for sign-ins	Low	Azure AD Sign-ins log	Status = Failure -and- error code = 50057, The user account is disabled.	This could indicate someone is trying to gain access to an account once they have left an organization. Although the account is blocked it is still important to log and alert on this activity. Azure Sentinel template

Monitoring for successful unusual sign ins

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Authentications of privileged accounts outside of expected controls.	High	Azure AD Sign-ins log	Status = success -and- UserPrincipalName = <Admin account> -and- Location = <unapproved location> -and- IP Address = <unapproved IP> Device Info= <unapproved Browser, Operating System>	Monitor and alert on successful authentication for privileged accounts outside of expected controls. Three common controls are listed.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
When only single-factor authentication is required.	Low	Azure AD Sign-ins log	Status = success Authentication requirement = Single-factor authentication	Monitor this periodically and ensure this is the expected behavior. Azure Sentinel template
Discover privileged accounts not registered for MFA.	High	Azure Graph API	Query for IsMFARegistered eq false for administrator accounts. List credentialUserRegistrationDetails - Microsoft Graph beta	Audit and investigate to determine if intentional or an oversight.
Successful authentications from countries your organization does not operate out of.	Medium	Azure AD Sign-ins log	Status = success Location = <unapproved country>	Monitor and alert on any entries not equal to the city names you provide.
Successful authentication, session blocked by CA.	Medium	Azure AD Sign-ins log	Status = success -and- error code = 53003 – Failure reason, blocked by CA	Monitor and investigate when authentication is successful, but session is blocked by CA. Azure Sentinel template
Successful authentication after you have disabled legacy authentication.	Medium	Azure AD Sign-ins log	status = success -and- Client app = Other Clients, POP, IMAP, MAPI, SMTP, ActiveSync	If your organization has disabled legacy authentication, monitor and alert when successful legacy authentication has taken place. Azure Sentinel template

On periodic basis, we recommend you review authentications to medium business impact (MBI) and high business impact (HBI) applications where only single-factor authentication is required. For each, you want to determine if single-factor authentication was expected or not. Additionally, review for successful authentication increases or at unexpected times based on the location.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Authentications to MBI and HBI application using single-factor authentication.	Low	Azure AD Sign-ins log	status = success -and- Application ID = <HBI app> -and- Authentication requirement = single-factor authentication.	Review and validate this configuration is intentional. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
-----------------	------------	-------	-------------------	-------

Authentications at days and times of the week or year that countries do not conduct normal business operations.	Low	Azure AD Sign-ins log	Capture interactive authentication occurring outside of normal operating days\time. Status = success Location = <location> Date\Time = <not normal working hours>	Monitor and alert on authentications days and times of the week or year that countries do not conduct normal business operations. Azure Sentinel template
Measurable increase of successful sign ins.	Low	Azure AD Sign-ins log	Capture increases in successful authentication across the board. I.e., total successes for today is >10 % on the same day the previous week.	If you don't have a set threshold, monitor and alert if successful authentications increase by 10% or greater. Azure Sentinel template

Next steps

See these security operations guide articles:

[Azure AD security operations overview](#)

[Security operations for user accounts](#)

[Security operations for privileged accounts](#)

[Security operations for Privileged Identity Management](#)

[Security operations for applications](#)

[Security operations for devices](#)

[Security operations for infrastructure](#)

Security operations for privileged accounts

4/10/2022 • 17 minutes to read • [Edit Online](#)

The security of business assets depends on the integrity of the privileged accounts that administer your IT systems. Cyber attackers use credential theft attacks and other means to target privileged accounts and gain access to sensitive data.

Traditionally, organizational security has focused on the entry and exit points of a network as the security perimeter. However, software as a service (SaaS) applications and personal devices on the internet have made this approach less effective.

Azure Active Directory (Azure AD) uses identity and access management (IAM) as the control plane. In your organization's identity layer, users assigned to privileged administrative roles are in control. The accounts used for access must be protected, whether the environment is on-premises, in the cloud, or a hybrid environment.

You're entirely responsible for all layers of security for your on-premises IT environment. When you use Azure services, prevention and response are the joint responsibilities of Microsoft as the cloud service provider and you as the customer.

- For more information on the shared responsibility model, see [Shared responsibility in the cloud](#).
- For more information on securing access for privileged users, see [Securing privileged access for hybrid and cloud deployments in Azure AD](#).
- For a wide range of videos, how-to guides, and content of key concepts for privileged identity, see [Privileged Identity Management documentation](#).

Where to look

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Microsoft 365 Audit logs](#)
- [Azure Key Vault insights](#)

From the Azure portal, you can view the Azure AD Audit logs and download as comma-separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- [Microsoft Sentinel](#): Enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- [Azure Monitor](#): Enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- [Azure Event Hubs](#) integrated with a SIEM: Enables [Azure AD logs to be pushed to other SIEMs](#) such as Splunk, ArcSight, QRadar, and Sumo Logic via the Azure Event Hubs integration.
- [Microsoft Defender for Cloud Apps](#): Enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.
- [Microsoft Graph](#): Enables you to export data and use Microsoft Graph to do more analysis. For more information on Microsoft Graph, see [Microsoft Graph PowerShell SDK](#) and [Azure Active Directory Identity Protection](#).

- **Identity Protection:** Generates three key reports you can use to help with your investigation:
 - **Risky users:** Contains information about which users are at risk, details about detections, history of all risky sign-ins, and risk history.
 - **Risky sign-ins:** Contains information about a sign-in that might indicate suspicious circumstances. For more information on investigating information from this report, see [Investigate risk](#).
 - **Risk detections:** Contains information about other risks triggered when a risk is detected and other pertinent information such as sign-in location and any details from Microsoft Defender for Cloud Apps.

Although we discourage the practice, privileged accounts can have standing administration rights. If you choose to use standing privileges, and the account is compromised, it can have a strongly negative effect. We recommend you prioritize monitoring privileged accounts and include the accounts in your Privileged Identity Management (PIM) configuration. For more information on PIM, see [Start using Privileged Identity Management](#). Also, we recommend you validate that admin accounts:

- Are required.
- Have the least privilege to execute the required activities.
- Are protected with multifactor authentication (MFA) at a minimum.
- Are run from privileged access workstation (PAW) or secure admin workstation (SAW) devices.

The rest of this article describes what we recommend you monitor and alert on. The article is organized by the type of threat. Where there are specific prebuilt solutions, we link to them following the table. Otherwise, you can build alerts by using the preceding tools.

Specifically, this article provides details on setting baselines and auditing sign-in and usage of privileged accounts. It also discusses tools and resources you can use to help maintain the integrity of your privileged accounts. The content is organized into the following subjects:

- Emergency "break-glass" accounts
- Privileged account sign-in
- Privileged account changes
- Privileged groups
- Privilege assignment and elevation

Emergency access accounts

It's important that you prevent being accidentally locked out of your Azure AD tenant. You can mitigate the effect of an accidental lockout by creating emergency access accounts in your organization. Emergency access accounts are also known as break-glass accounts, as in "break glass in case of emergency" messages found on physical security equipment like fire alarms.

Emergency access accounts are highly privileged, and they aren't assigned to specific individuals. Emergency access accounts are limited to emergency or break-glass scenarios where normal privileged accounts can't be used. An example is when a Conditional Access policy is misconfigured and locks out all normal administrative accounts. Restrict emergency account use to only the times when it's absolutely necessary.

For guidance on what to do in an emergency, see [Secure access practices for administrators in Azure AD](#).

Send a high-priority alert every time an emergency access account is used.

Discovery

Because break-glass accounts are only used if there's an emergency, your monitoring should discover no account activity. Send a high-priority alert every time an emergency access account is used or changed. Any of the following events might indicate a bad actor is trying to compromise your environments:

- **Account used:** Monitor and alert on any activity by using this type of account, such as:
 - Sign-in.
 - Account password change.
 - Account permission or roles changed.
 - Credential or auth method added or changed.

For more information on managing emergency access accounts, see [Manage emergency access admin accounts in Azure AD](#). For detailed information on creating an alert for an emergency account, see [Create an alert rule](#).

Privileged account sign-in

Monitor all privileged account sign-in activity by using the Azure AD Sign-in logs as the data source. In addition to sign-in success and failure information, the logs contain the following details:

- Interrupts
- Device
- Location
- Risk
- Application
- Date and time
- Is the account disabled
- Lockout
- MFA fraud
- Conditional Access failure

Things to monitor

You can monitor privileged account sign-in events in the Azure AD Sign-in logs. Alert on and investigate the following events for privileged accounts.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Sign-in failure, bad password threshold	High	Azure AD Sign-ins log	Status = Failure -and- error code = 50126	Define a baseline threshold and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated. Azure Sentinel template
Failure because of Conditional Access requirement	High	Azure AD Sign-ins log	Status = Failure -and- error code = 53003 -and- Failure reason = Blocked by Conditional Access	This event can be an indication an attacker is trying to get into the account. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Privileged accounts that don't follow naming policy		Azure subscription	List Azure role assignments using the Azure portal - Azure RBAC	List role assignments for subscriptions and alert where the sign-in name doesn't match your organization's format. An example is the use of ADM_ as a prefix.
Interrupt	High, medium	Azure AD Sign-ins	Status = Interrupted -and- error code = 50074 -and- Failure reason = Strong auth required Status = Interrupted -and- Error code = 500121 Failure reason = Authentication failed during strong authentication request	This event can be an indication an attacker has the password for the account but can't pass the MFA challenge. Azure Sentinel template
Privileged accounts that don't follow naming policy	High	Azure AD directory	List Azure AD role assignments	List role assignments for Azure AD roles and alert where the UPN doesn't match your organization's format. An example is the use of ADM_ as a prefix.
Discover privileged accounts not registered for MFA	High	Microsoft Graph API	Query for IsMFARegistered eq false for admin accounts. List credentialUserRegistrationDetails - Microsoft Graph beta	Audit and investigate to determine if the event is intentional or an oversight.
Account lockout	High	Azure AD Sign-ins log	Status = Failure -and- error code = 50053	Define a baseline threshold, and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Account disabled or blocked for sign-ins	Low	Azure AD Sign-ins log	Status = Failure -and- Target = User UPN -and- error code = 50057	This event could indicate someone is trying to gain access to an account after they've left the organization. Although the account is blocked, it's still important to log and alert on this activity. Azure Sentinel template
MFA fraud alert or block	High	Azure AD Sign-ins log/Azure Log Analytics	Sign-ins>Authentication details Result details = MFA denied, fraud code entered	Privileged user has indicated they haven't instigated the MFA prompt, which could indicate an attacker has the password for the account. Azure Sentinel template
MFA fraud alert or block	High	Azure AD Audit log log/Azure Log Analytics	Activity type = Fraud reported - User is blocked for MFA or fraud reported - No action taken (based on tenant-level settings for fraud report)	Privileged user has indicated they haven't instigated the MFA prompt, which could indicate an attacker has the password for the account. Azure Sentinel template
Privileged account sign-ins outside of expected controls		Azure AD Sign-ins log	Status = Failure UserPrincipalName = <Admin account> Location = <unapproved location> IP address = <unapproved IP> Device info = <unapproved Browser, Operating System>	Monitor and alert on any entries that you've defined as unapproved. Azure Sentinel template

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Outside of normal sign-in times	High	Azure AD Sign-ins log	Status = Success -and- Location = -and- Time = Outside of working hours	Monitor and alert if sign-ins occur outside of expected times. It's important to find the normal working pattern for each privileged account and to alert if there are unplanned changes outside of normal working times. Sign-ins outside of normal working hours could indicate compromise or possible insider threats. Azure Sentinel template
Identity protection risk	High	Identity Protection logs	Risk state = At risk -and- Risk level = Low, medium, high -and- Activity = Unfamiliar sign-in/TOR, and so on	This event indicates there's some abnormality detected with the sign-in for the account and should be alerted on.
Password change	High	Azure AD Audit logs	Activity actor = Admin/self-service -and- Target = User -and- Status = Success or failure	Alert on any admin account password changes, especially for global admins, user admins, subscription admins, and emergency access accounts. Write a query targeted at all privileged accounts. Azure Sentinel template
Change in legacy authentication protocol	High	Azure AD Sign-ins log	Client App = Other client, IMAP, POP3, MAPI, SMTP, and so on -and- Username = UPN -and- Application = Exchange (example)	Many attacks use legacy authentication, so if there's a change in auth protocol for the user, it could be an indication of an attack.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
New device or location	High	Azure AD Sign-ins log	Device info = Device ID -and- Browser -and- OS -and- Compliant/Managed -and- Target = User -and- Location	Most admin activity should be from privileged access devices , from a limited number of locations. For this reason, alert on new devices or locations. Azure Sentinel template
Audit alert setting is changed	High	Azure AD Audit logs	Service = PIM -and- Category = Role management -and- Activity = Disable PIM alert -and- Status = Success	Changes to a core alert should be alerted if unexpected.

Changes by privileged accounts

Monitor all completed and attempted changes by a privileged account. This data enables you to establish what's normal activity for each privileged account and alert on activity that deviates from the expected. The Azure AD Audit logs are used to record this type of event. For more information on Azure AD Audit logs, see [Audit logs in Azure Active Directory](#).

Azure Active Directory Domain Services

Privileged accounts that have been assigned permissions in Azure AD Domain Services can perform tasks for Azure AD Domain Services that affect the security posture of your Azure-hosted virtual machines (VMs) that use Azure AD Domain Services. Enable security audits on VMs and monitor the logs. For more information on enabling Azure AD Domain Services audits and for a list of sensitive privileges, see the following resources:

- [Enable security audits for Azure Active Directory Domain Services](#)
- [Audit Sensitive Privilege Use](#)

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Attempted and completed changes	High	Azure AD Audit logs	Date and time -and- Service -and- Category and name of the activity (what) -and- Status = Success or failure -and- Target -and- Initiator or actor (who)	Any unplanned changes should be alerted on immediately. These logs should be retained to assist in any investigation. Any tenant-level changes should be investigated immediately (link out to Infra doc) that would lower the security posture of your tenant. An example is excluding accounts from MFA or Conditional Access. Alert on any additions or changes to applications .
EXAMPLE Attempted or completed change to high-value apps or services	High	Audit log	Service -and- Category and name of the activity	<ul style="list-style-type: none"> • Date and time • Service • Category and name of the activity • Status = Success or failure • Target • Initiator or actor (who)
Privileged changes in Azure AD Domain Services	High	Azure AD Domain Services	Look for event 4673	Enable security audits for Azure Active Directory Domain Services Audit Sensitive Privilege use . See the article for a list of all privileged events.

Changes to privileged accounts

Investigate changes to privileged accounts' authentication rules and privileges, especially if the change provides greater privilege or the ability to perform tasks in your Azure AD environment.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Privileged account creation	Medium	Azure AD Audit logs	Service = Core Directory -and- Category = User management -and- Activity type = Add user -correlate with- Category type = Role management -and- Activity type = Add member to role -and- Modified properties = Role.DisplayName	Monitor creation of any privileged accounts. Look for correlation that's of a short time span between creation and deletion of accounts. Azure Sentinel template
Changes to authentication methods	High	Azure AD Audit logs	Service = Authentication Method -and- Activity type = User registered security information -and- Category = User management	This change could be an indication of an attacker adding an auth method to the account so they can have continued access. Azure Sentinel template
Alert on changes to privileged account permissions	High	Azure AD Audit logs	Category = Role management -and- Activity type = Add eligible member (permanent) -and- Activity type = Add eligible member (eligible) -and- Status = Success or failure -and- Modified properties = Role.DisplayName	This alert is especially for accounts being assigned roles that aren't known or are outside of their normal responsibilities.
Unused privileged accounts	Medium	Azure AD Access Reviews		Perform a monthly review for inactive privileged user accounts.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Accounts exempt from Conditional Access	High	Azure Monitor Logs -or- Access Reviews	Conditional Access = Insights and reporting	Any account exempt from Conditional Access is most likely bypassing security controls and is more vulnerable to compromise. Break-glass accounts are exempt. See information on how to monitor break-glass accounts in a subsequent section of this article.

For more information on how to monitor for exceptions to Conditional Access policies, see [Conditional Access insights and reporting](#).

For more information on discovering unused privileged accounts, see [Create an access review of Azure AD roles in Privileged Identity Management](#).

Assignment and elevation

Having privileged accounts that are permanently provisioned with elevated abilities can increase the attack surface and risk to your security boundary. Instead, employ just-in-time access by using an elevation procedure. This type of system allows you to assign eligibility for privileged roles. Admins elevate their privileges to those roles only when they perform tasks that need those privileges. Using an elevation process enables you to monitor elevations and non-use of privileged accounts.

Establish a baseline

To monitor for exceptions, you must first create a baseline. Determine the following information for:

- **Admin accounts:**
 - Your privileged account strategy
 - Use of on-premises accounts to administer on-premises resources
 - Use of cloud-based accounts to administer cloud-based resources
 - Approach to separating and monitoring administrative permissions for on-premises and cloud-based resources
- **Privileged role protection:**
 - Protection strategy for roles that have administrative privileges
 - Organizational policy for using privileged accounts
 - Strategy and principles for maintaining permanent privilege versus providing time-bound and approved access

The following concepts and information will help you determine policies:

- **Just-in-time admin principles:** Use the Azure AD logs to capture information for performing administrative tasks that are common in your environment. Determine the typical amount of time needed to complete the tasks.
- **Just-enough admin principles:** [Determine the least-privileged role](#), which might be a custom role, that's needed for administrative tasks.
- **Establish an elevation policy:** After you have insight into the type of elevated privilege needed and how

long is needed for each task, create policies that reflect elevated privileged usage for your environment. As an example, define a policy to limit Global admin access to one hour.

After you establish your baseline and set policy, you can configure monitoring to detect and alert usage outside of policy.

Discovery

Pay particular attention to and investigate changes in assignment and elevation of privilege.

Things to monitor

You can monitor privileged account changes by using Azure AD Audit logs and Azure Monitor logs. Specifically, include the following changes in your monitoring process.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Added to eligible privileged role	High	Azure AD Audit Logs	Service = PIM -and- Category = Role management -and- Activity type = Add member to role completed (eligible) -and- Status = Success or failure -and- Modified properties = Role.DisplayName	Any account eligible for a role is now being given privileged access. If the assignment is unexpected or into a role that isn't the responsibility of the account holder, investigate. Azure Sentinel template
Roles assigned out of PIM	High	Azure AD Audit Logs	Service = PIM -and- Category = Role management -and- Activity type = Add member to role (permanent) -and- Status = Success or failure -and- Modified properties = Role.DisplayName	These roles should be closely monitored and alerted. Users shouldn't be assigned roles outside of PIM where possible. Azure Sentinel template
Elevations	Medium	Azure AD Audit Logs	Service = PIM -and- Category = Role management -and- Activity type = Add member to role completed (PIM activation) -and- Status = Success or failure -and- Modified properties = Role.DisplayName	After a privileged account is elevated, it can now make changes that could affect the security of your tenant. All elevations should be logged and, if happening outside of the standard pattern for that user, should be alerted and investigated if not planned.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Approvals and deny elevation	Low	Azure AD Audit Logs	Service = Access Review -and- Category = UserManagement -and- Activity type = Request approved or denied -and- Initiated actor = UPN	Monitor all elevations because it could give a clear indication of the timeline for an attack. Azure Sentinel template
Changes to PIM settings	High	Azure AD Audit Logs	Service = PIM -and- Category = Role management -and- Activity type = Update role setting in PIM -and- Status reason = MFA on activation disabled (example)	One of these actions could reduce the security of the PIM elevation and make it easier for attackers to acquire a privileged account.
Elevation not occurring on SAW/PAW	High	Azure AD Sign In logs	Device ID -and- Browser -and- OS -and- Compliant/Managed Correlate with: Service = PIM -and- Category = Role management -and- Activity type = Add member to role completed (PIM activation) -and- Status = Success or failure -and- Modified properties = Role.DisplayName	If this change is configured, any attempt to elevate on a non-PAW/SAW device should be investigated immediately because it could indicate an attacker is trying to use the account.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUBFILTER	NOTES
Elevation to manage all Azure subscriptions	High	Azure Monitor	Activity Log tab Directory Activity tab Operations Name = Assigns the caller to user access admin -and- Event category = Administrative -and- Status = Succeeded, start, fail -and- Event initiated by	This change should be investigated immediately if it isn't planned. This setting could allow an attacker access to Azure subscriptions in your environment.

For more information about managing elevation, see [Elevate access to manage all Azure subscriptions and management groups](#). For information on monitoring elevations by using information available in the Azure AD logs, see [Azure Activity log](#), which is part of the Azure Monitor documentation.

For information about configuring alerts for Azure roles, see [Configure security alerts for Azure resource roles in Privileged Identity Management](#).

Next steps

See these security operations guide articles:

- [Azure AD security operations overview](#)
- [Security operations for user accounts](#)
- [Security operations for privileged accounts](#)
- [Security operations for Privileged Identity Management](#)
- [Security operations for applications](#)
- [Security operations for devices](#)
- [Security operations for infrastructure](#)

Azure Active Directory security operations for Privileged Identity Management (PIM)

4/10/2022 • 8 minutes to read • [Edit Online](#)

The security of business assets depends on the integrity of the privileged accounts that administer your IT systems. Cyber-attackers use credential theft attacks to target admin accounts and other privileged access accounts to try gaining access to sensitive data.

For cloud services, prevention and response are the joint responsibilities of the cloud service provider and the customer.

Traditionally, organizational security has focused on the entry and exit points of a network as the security perimeter. However, SaaS apps and personal devices have made this approach less effective. In Azure Active Directory (Azure AD), we replace the network security perimeter with authentication in your organization's identity layer. As users are assigned to privileged administrative roles, their access must be protected in on-premises, cloud, and hybrid environments.

You're entirely responsible for all layers of security for your on-premises IT environment. When you use Azure cloud services, prevention and response are joint responsibilities of Microsoft as the cloud service provider and you as the customer.

- For more information on the shared responsibility model, see [Shared responsibility in the cloud](#).
- For more information on securing access for privileged users, see [Securing Privileged access for hybrid and cloud deployments in Azure AD](#).
- For a wide range of videos, how-to guides, and content of key concepts for privileged identity, visit [Privileged Identity Management documentation](#).

Privileged Identity Management (PIM) is an Azure AD service that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. You can use PIM to help mitigate the following risks:

- Identify and minimize the number of people who have access to secure information and resources.
- Detect excessive, unnecessary, or misused access permissions on sensitive resources.
- Reduce the chances of a malicious actor getting access to secured information or resources.
- Reduce the possibility of an unauthorized user inadvertently impacting sensitive resources.

This article provides guidance on setting baselines, auditing sign-ins and usage of privileged accounts, and the source of audit logs you can use to help maintain the integrity of your privilege accounts.

Where to look

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Sign-in logs](#)
- [Microsoft 365 Audit logs](#)

- [Azure Key Vault logs](#)

In the Azure portal you can view the Azure AD Audit logs and download them as comma-separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- **Microsoft Sentinel** – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- **Azure Monitor** – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- **Azure Event Hubs integrated with a SIEM**- [Azure AD logs can be integrated to other SIEMs](#) such as Splunk, ArcSight, QRadar, and Sumo Logic via the Azure Event Hub integration.
- **Microsoft Defender for Cloud Apps** – enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.

The rest of this article provides recommendations for setting a baseline to monitor and alert on, organized using a tier model. Links to pre-built solutions are listed following the table. You can also build alerts using the preceding tools. The content is organized into the following topic areas of PIM:

- Baselines
- Azure AD role assignment
- Azure AD role alert settings
- Azure resource role assignment
- Access management for Azure resources
- Elevated access to manage Azure subscriptions

Baselines

The following are recommended baseline settings:

WHAT TO MONITOR	RISK LEVEL	RECOMMENDATION	ROLES	NOTES
Azure AD roles assignment	High	<ul style="list-style-type: none"> • Require justification for activation. • Require approval to activate. • Set two-level approver process. • On activation, require Azure Active Directory Multi-Factor Authentication (MFA). • Set maximum elevation duration to 8 hrs. 	<ul style="list-style-type: none"> • Privileged Role Administration • Global Administrator 	A privileged role administrator can customize PIM in their Azure AD organization, including changing the experience for users activating an eligible role assignment.

WHAT TO MONITOR	RISK LEVEL	RECOMMENDATION	ROLES	NOTES
Azure Resource Role Configuration	High	<ul style="list-style-type: none"> • Require justification for activation. • Require approval to activate. • Set two-level approver process. • On activation, require Azure MFA. • Set maximum elevation duration to 8 hrs. 	<ul style="list-style-type: none"> • Owner • Resource Administrator • User Access Administrator • Administrator • Global Administrator • Security Administrator 	Investigate immediately if not a planned change. This setting could enable an attacker access to Azure subscriptions in your environment.

Azure AD roles assignment

A privileged role administrator can customize PIM in their Azure AD organization. This includes changing the experience for a user who is activating an eligible role assignment as follows:

- Prevent bad actor to remove Azure MFA requirements to activate privileged access.
- Prevent malicious users bypass justification and approval of activating privileged access.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Alert on Add changes to privileged account permissions	High	Azure AD Audit logs	Category = Role Management -and- Activity Type – Add eligible member (permanent) -and- Activity Type – Add eligible member (eligible) -and- Status = Success/failure -and- Modified properties = Role.DisplayName	Monitor and always alert for any changes to privileged role administrator and global administrator. <ul style="list-style-type: none"> • This can be an indication an attacker is trying to gain privilege to modify role assignment settings • If you don't have a defined threshold, alert on 4 in 60 minutes for users and 2 in 60 minutes for privileged accounts.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Alert on bulk deletion changes to privileged account permissions	High	Azure AD Audit logs	Category = Role Management -and- Activity Type – Remove eligible member (permanent) -and- Activity Type – Remove eligible member (eligible) -and- Status = Success/failure -and- Modified properties = Role.DisplayName	Investigate immediately if not a planned change. This setting could enable an attacker access to Azure subscriptions in your environment. Azure Sentinel template
Changes to PIM settings	High	Azure AD Audit Log	Service = PIM -and- Category = Role Management -and- Activity Type = Update role setting in PIM -and- Status Reason = MFA on activation disabled (example)	Monitor and always alert for any changes to Privileged Role Administrator and Global Administrator. <ul style="list-style-type: none">• This can be an indication an attacker already gained access able to modify to modify role assignment settings• One of these actions could reduce the security of the PIM elevation and make it easier for attackers to acquire a privileged account.
Approvals and deny elevation	High	Azure AD Audit Log	Service = Access Review -and- Category = UserManagement -and- Activity Type = Request Approved/Denied -and- Initiated actor = UPN	All elevations should be monitored. Log all elevations as this could give a clear indication of timeline for an attack.
Alert setting changes to disabled.	High	Azure AD Audit logs	Service =PIM -and- Category = Role Management -and- Activity Type = Disable PIM Alert -and- Status = Success /Failure	Always alert. <ul style="list-style-type: none">• Helps detect bad actor removing alerts associated with Azure MFA requirements to activate privileged access.• Helps detect suspicious or unsafe activity. Azure Sentinel template

For more information on identifying role setting changes in the Azure AD Audit log, see [View audit history for Azure AD roles in Privileged Identity Management](#).

Azure resource role assignment

Monitoring Azure resource role assignments provides visibility into activity and activations for resources roles. These might be misused to create an attack surface to a resource. As you monitor for this type of activity, you are trying to detect:

- Query role assignments at specific resources
- Role assignments for all child resources
- All active and eligible role assignment changes

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Audit Alert Resource Audit log for Privileged account activities	High	In PIM, under Azure Resources, Resource Audit	Action : Add eligible member to role in PIM completed (time bound) -and- Primary Target -and- Type User -and- Status = Succeeded	Always alert. Helps detect bad actor adding eligible roles to manage all resources in Azure.
Audit Alert Resource Audit for Disable Alert	Medium	In PIM, under Azure Resources, Resource Audit	Action : Disable Alert -and- Primary Target : Too many owners assigned to a resource -and- Status = Succeeded	Helps detect bad actor disabling alerts from Alerts pane which can bypass malicious activity being investigated
Audit Alert Resource Audit for Disable Alert	Medium	In PIM, under Azure Resources, Resource Audit	Action : Disable Alert -and- Primary Target : Too many permanent owners assigned to a resource -and- Status = Succeeded	Prevent bad actor from disable alerts from Alerts pane which can bypass malicious activity being investigated
Audit Alert Resource Audit for Disable Alert	Medium	In PIM, under Azure Resources, Resource Audit	Action : Disable Alert -and- Primary Target Duplicate role created -and- Status = Succeeded	Prevent bad actor from disable alerts from Alerts pane which can bypass malicious activity being investigated

For more information on configuring alerts and auditing Azure resource roles, see:

- [Configure security alerts for Azure resource roles in Privileged Identity Management](#)
- [View audit report for Azure resource roles in Privileged Identity Management \(PIM\)](#)

Access management for Azure resources and subscriptions

Users or members of a group assigned to the Owner or User Access Administrator subscriptions roles, and Azure AD Global administrators that enabled subscription management in Azure AD have Resource administrator permissions by default. These administrators can assign roles, configure role settings, and review access using Privileged Identity Management (PIM) for Azure resources.

A user who has Resource administrator permissions can manage PIM for Resources. The risk this introduces that you must monitor for and mitigate, is that the capability can be used to allow bad actors to have privileged access to Azure subscription resources, such as virtual machines or storage accounts.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Elevations	High	Azure AD, under Manage, Properties	Periodically review setting. Access management for Azure resources	Global administrators can elevate by enabling Access management for Azure resources. Verify bad actors have not gained permissions to assign roles in all Azure subscriptions and management groups associated with Active Directory.

For more information see [Assign Azure resource roles in Privileged Identity Management](#)

Next steps

See these security operations guide articles:

[Azure AD security operations overview](#)

[Security operations for user accounts](#)

[Security operations for privileged accounts](#)

[Security operations for Privileged Identity Management](#)

[Security operations for applications](#)

[Security operations for devices](#)

[Security operations for infrastructure](#)

Azure Active Directory security operations guide for Applications

4/10/2022 • 10 minutes to read • [Edit Online](#)

Applications provide an attack surface for security breaches and must be monitored. While not targeted as often as user accounts, breaches can occur. Since applications often run without human intervention, the attacks may be harder to detect.

This article provides guidance to monitor and alert on application events. It's regularly updated to help ensure that you:

- Prevent malicious applications from getting unwarranted access to data.
- Prevent existing applications from being compromised by bad actors.
- Gather insights that enable you to build and configure new applications more securely.

If you're unfamiliar with how applications work in Azure Active Directory (Azure AD), see [Apps and service principals in Azure AD](#).

NOTE

If you have not yet reviewed the [Azure Active Directory security operations overview](#), consider doing so now.

What to look for

As you monitor your application logs for security incidents, review the following to help differentiate normal activity from malicious activity. The following events may indicate security concerns and each are covered in the rest of the article.

- Any changes occurring outside of normal business processes and schedules.
- Application credentials changes
- Application permissions
 - Service principal assigned to an Azure AD or Azure RBAC role.
 - Applications that are granted highly privileged permissions.
 - Azure Key Vault changes.
 - End user granting applications consent.
 - Stopped end user consent based on level of risk.
- Application configuration changes
 - Universal resource identifier (URI) changed or non-standard.
 - Changes to application owners.
 - Logout URLs modified.

Where to look

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Sign-in logs](#)
- [Microsoft 365 Audit logs](#)
- [Azure Key Vault logs](#)

From the Azure portal, you can view the Azure AD Audit logs and download as comma-separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- **Microsoft Sentinel** – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- **Azure Monitor** – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- **Azure Event Hubs integrated with a SIEM**- [Azure AD logs can be integrated to other SIEMs](#) such as Splunk, ArcSight, QRadar, and Sumo Logic via the Azure Event Hub integration.
- **Microsoft Defender for Cloud Apps** – enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.

Much of what you will monitor and alert on are the effects of your Conditional Access policies. You can use the [Conditional Access insights and reporting workbook](#) to examine the effects of one or more Conditional Access policies on your sign-ins, as well as the results of policies, including device state. This workbook enables you to view an impact summary, and identify the impact over a specific time period. You can also use the workbook to investigate the sign-ins of a specific user.

The remainder of this article describes what we recommend you monitor and alert on, and is organized by the type of threat. Where there are specific pre-built solutions we link to them or provide samples following the table. Otherwise, you can build alerts using the preceding tools.

Application credentials

Many applications use credentials to authenticate in Azure AD. Any additional credentials added outside of expected processes could be a malicious actor using those credentials. We strongly recommend using X509 certificates issued by trusted authorities or Managed Identities instead of using client secrets. However, if you need to use client secrets, follow good hygiene practices to keep applications safe. Note, application and service principal updates are logged as two entries in the audit log.

- Monitor applications to identify those with long credential expiration times.
- Replace long-lived credentials with credentials that have a short life span. Take steps to ensure that credentials don't get committed in code repositories and are stored securely.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Added credentials to existing applications	High	Azure AD Audit logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application-Certificates and secrets management -and- Activity: Update Service principal/Update Application	Alert when credentials are: <ul style="list-style-type: none">• added outside of normal business hours or workflows.• of types not used in your environment.• added to a non-SAML flow supporting service principal.
Credentials with a lifetime longer than your policies allow.	Medium	Microsoft Graph	State and end date of Application Key credentials -and- Application password credentials	You can use MS Graph API to find the start and end date of credentials, and evaluate those with a longer than allowed lifetime. See PowerShell script following this table.

The following pre-built monitoring and alerts are available.

- Microsoft Sentinel – [Alert when new app or service principle credentials added](#)
- Azure Monitor – [Azure AD workbook to help you assess Solorigate risk - Microsoft Tech Community](#)
- Defender for Cloud Apps – [Defender for Cloud Apps anomaly detection alerts investigation guide](#)
- PowerShell - [Sample PowerShell script to find credential lifetime.](#)

Application permissions

Like an administrator account, applications can be assigned privileged roles. Apps can be assigned Azure AD roles, such as global administrator, or Azure RBAC roles such as subscription owner. Because they can run without a user present and as a background service, closely monitor anytime an application is granted a highly privileged role or permission.

Service principal assigned to a role

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
App assigned to Azure RBAC role, or Azure AD Role	High to Medium	Azure AD Audit logs	Type: service principal Activity: "Add member to role" or "Add eligible member to role" -or- "Add scoped member to role."	For highly privileged roles such as Global Administrator, risk is high. For lower privileged roles risk is medium. Alert anytime an application is assigned to an Azure role or Azure AD role outside of normal change management or configuration procedures.

Application granted highly privileged permissions

Applications should also follow the principle of least privilege. Investigate application permissions to ensure they're truly needed. You can create an [app consent grant report](#) to help identify existing applications and highlight privileged permissions.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
App granted highly privileged permissions, such as permissions with ".All" <i>(Directory.ReadWrite.All) or wide ranging permissions (Mail.)</i>	High	Azure AD Audit logs	"Add app role assignment to service principal", - where- Target(s) identifies an API with sensitive data (such as Microsoft Graph) -and- AppRole.Value identifies a highly privileged application permission (app role).	Apps granted broad permissions such as ".All" <i>(Directory.ReadWrite.All) or wide ranging permissions (Mail.)</i>
Administrator granting either application permissions (app roles) or highly privileged delegated permissions	High	Microsoft 365 portal	"Add app role assignment to service principal", -where- Target(s) identifies an API with sensitive data (such as Microsoft Graph) "Add delegated permission grant", -where- Target(s) identifies an API with sensitive data (such as Microsoft Graph) -and- DelegatedPermissionGrant.Scope includes high-privilege permissions.	Alert when a global administrator, application administrator, or cloud application administrator consents to an application. Especially look for consent outside of normal activity and change procedures.
Application is granted permissions for Microsoft Graph, Exchange, SharePoint, or Azure AD.	High	Azure AD Audit logs	"Add delegated permission grant" -or- "Add app role assignment to service principal", -where- Target(s) identifies an API with sensitive data (such as Microsoft Graph, Exchange Online, and so on)	Alert as in the preceding row.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Application permissions (app roles) for other APIs are granted	Medium	Azure AD Audit logs	"Add app role assignment to service principal", -where- Target(s) identifies any other API.	Alert as in the preceding row.
Highly privileged delegated permissions are granted on behalf of all users	High	Azure AD Audit logs	"Add delegated permission grant", where Target(s) identifies an API with sensitive data (such as Microsoft Graph), DelegatedPermission Grant.Scope includes high-privilege permissions, -and- DelegatedPermission Grant.ConsentType is "AllPrincipals".	Alert as in the preceding row.

For more information on monitoring app permissions, see this tutorial: [Investigate and remediate risky OAuth apps](#).

Azure Key Vault

Azure Key Vault can be used to store your tenant's secrets. We recommend you pay particular attention to any changes to Key Vault configuration and activities.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
How and when your Key Vaults are accessed and by whom	Medium	Azure Key Vault logs	Resource type: Key Vaults	<p>Look for</p> <ul style="list-style-type: none"> • any access to Key Vault outside of regular processes and hours. • any changes to Key Vault ACL.

After setting up Azure Key Vault, be sure to [enable logging](#), which shows [how and when your Key Vaults are accessed](#), and [configure alerts](#) on Key Vault to notify assigned users or distribution lists via email, phone call, text message, or [event grid](#) notification if health is impacted. Additionally, setting up [monitoring](#) with Key Vault insights will give you a snapshot of Key Vault requests, performance, failures, and latency. [Log Analytics](#) also has some [example queries](#) for Azure Key Vault that can be accessed after selecting your Key Vault and then under "Monitoring" selecting "Logs".

End-user consent

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
End-user consent to application	Low	Azure AD Audit logs	Activity: Consent to application / ConsentContext.IsAdminConsent = false	<p>Look for:</p> <ul style="list-style-type: none"> • high profile or highly privileged accounts. • app requests high-risk permissions • apps with suspicious names, for example generic, misspelled, etc.

The act of consenting to an application is not in itself malicious. However, investigate new end-user consent grants looking for suspicious applications. You can [restrict user consent operations](#).

For more information on consent operations, see the following resources:

- [Managing consent to applications and evaluating consent requests in Azure Active Directory](#)
- [Detect and Remediate Illicit Consent Grants - Office 365](#)
- [Incident response playbook - App consent grant investigation](#)

End user stopped due to risk-based consent

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
End-user consent stopped due to risk-based consent	Medium	Azure AD Audit logs	Core Directory / ApplicationManagement / Consent to application Failure status reason = Microsoft.online.Security.userConsent BlockedForRiskyApps Exceptions	<p>Monitor and analyze any time consent is stopped due to risk.</p> <p>Look for:</p> <ul style="list-style-type: none"> • high profile or highly privileged accounts. • app requests high-risk permissions • apps with suspicious names, for example generic, misspelled, etc.

Application configuration changes

Monitor changes to any application's configuration. Specifically, configuration changes to the uniform resource identifier (URI), ownership, and logout URL.

Dangling URI and Redirect URI changes

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Dangling URI	High	Azure AD Logs and Application Registration	Service-Core Directory, Category-ApplicationManagement Activity: Update Application Success – Property Name AppAddress	<p>Look for dangling URLs, for example, that point to a domain name that no longer exists or one that you don't explicitly own.</p>

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Redirect URI configuration changes	High	Azure AD logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application Success – Property Name AppAddress	Look for URIs not using HTTPS*, URIs with wildcards at the end or the domain of the URL, URIs that are NOT unique to the application, URIs that point to a domain you do not control.

Alert anytime these changes are detected.

AppID URI added, modified, or removed

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Changes to AppID URI	High	Azure AD logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application Activity: Update Service principal	Look for any AppID URI modifications, such as adding, modifying, or removing the URI.

Alert any time these changes are detected outside of approved change management procedures.

New Owner

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Changes to application ownership	Medium	Azure AD logs	Service-Core Directory, Category-ApplicationManagement Activity: Add owner to application	Look for any instance of a user being added as an application owner outside of normal change management activities.

Logout URL modified or removed

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Changes to logout URL	Low	Azure AD logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application -and- Activity: Update service principle	Look for any modifications to a sign out URL. Blank entries or entries to non-existent locations would stop a user from terminating a session.

Additional Resources

The following are links to useful resources:

- GitHub Azure AD toolkit - <https://github.com/microsoft/AzureADToolkit>
- Azure Key Vault security overview and security guidance - [Azure Key Vault security overview](#)
- Solorgate risk information and tools - [Azure AD workbook to help you access Solorigate risk](#)
- OAuth attack detection guidance - [Unusual addition of credentials to an OAuth app](#)

Azure AD monitoring configuration information for SIEMs - [Partner tools with Azure Monitor integration](#)

Next steps

See these security operations guide articles:

[Azure AD security operations overview](#)

[Security operations for user accounts](#)

[Security operations for privileged accounts](#)

[Security operations for Privileged Identity Management](#)

[Security operations for applications](#)

[Security operations for devices](#)

[Security operations for infrastructure](#)

Azure Active Directory security operations for devices

4/10/2022 • 7 minutes to read • [Edit Online](#)

Devices aren't commonly targeted in identity-based attacks, but *can* be used to satisfy and trick security controls, or to impersonate users. Devices can have one of four relationships with Azure AD:

- Unregistered
- [Azure Active Directory \(Azure AD\) registered](#)
- [Azure AD joined](#)
- [Hybrid Azure AD joined](#)

Registered and joined devices are issued a [Primary Refresh Token \(PRT\)](#), which can be used as a primary authentication artifact, and in some cases as a multifactor authentication artifact. Attackers may try to register their own devices, use PRTs on legitimate devices to access business data, steal PRT-based tokens from legitimate user devices, or find misconfigurations in device-based controls in Azure Active Directory. With Hybrid Azure AD joined devices, the join process is initiated and controlled by administrators, reducing the available attack methods.

For more information on device integration methods, see [Choose your integration methods](#) in the article [Plan your Azure AD device deployment](#).

To reduce the risk of bad actors attacking your infrastructure through devices, monitor

- Device registration and Azure AD join
- Non-compliant devices accessing applications
- BitLocker key retrieval
- Device administrator roles
- Sign-ins to virtual machines

Where to look

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Sign-in logs](#)
- [Microsoft 365 Audit logs](#)
- [Azure Key Vault logs](#)

From the Azure portal, you can view the Azure AD Audit logs and download as comma-separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- [Microsoft Sentinel](#) – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.

- **Azure Monitor** – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- **Azure Event Hubs** -integrated with a SIEM- [Azure AD logs can be integrated to other SIEMs](#) such as Splunk, ArcSight, QRadar, and Sumo Logic via the Azure Event Hub integration.
- **Microsoft Defender for Cloud Apps** – enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.

Much of what you'll monitor and alert on are the effects of your Conditional Access policies. You can use the [Conditional Access insights and reporting workbook](#) to examine the effects of one or more Conditional Access policies on your sign-ins, and the results of policies including device state. This workbook enables you to view an impact summary, and identify the impact over a specific time period. You can also use the workbook to investigate the sign-ins of a specific user.

The rest of this article describes what we recommend you monitor and alert on, and is organized by the type of threat. Where there are specific pre-built solutions we link to them or provide samples following the table. Otherwise, you can build alerts using the preceding tools.

Device registrations and joins outside policy

Azure AD registered and Azure AD joined devices possess primary refresh tokens (PRTs), which are the equivalent of a single authentication factor. These devices can at times contain strong authentication claims. For more information on when PRTs contain strong authentication claims, see [When does a PRT get an MFA claim?](#) To keep bad actors from registering or joining devices, require multifactor authentication (MFA) to register or join devices. Then monitor for any devices registered or joined without MFA. You'll also need to watch for changes to MFA settings and policies, and device compliance policies.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Device registration or join completed without MFA	Medium	Sign-in logs	Activity: successful authentication to Device Registration Service. And No MFA required	Alert when: Any device registered or joined without MFA Azure Sentinel template
Changes to the Device Registration MFA toggle in Azure AD	High	Audit log	Activity: Set device registration policies	Look for: The toggle being set to off. There isn't audit log entry. Schedule periodic checks.
Changes to Conditional Access policies requiring domain joined or compliant device.	High	Audit log	Changes to CA policies	Alert when: <ul style="list-style-type: none"> • Change to any policy requiring domain joined or compliant. • Changes to trusted locations. • Accounts or devices added to MFA policy exceptions.

You can create an alert that notifies appropriate administrators when a device is registered or joined without MFA by using Microsoft Sentinel.

```

Sign-in logs

| where ResourceDisplayName == "Device Registration Service"
| where conditionalAccessStatus == "success"
| where AuthenticationRequirement <> "multiFactorAuthentication"

```

You can also use [Microsoft Intune](#) to set and monitor device compliance policies.

Non-compliant device sign in

It might not be possible to block access to all cloud and software-as-a-service applications with Conditional Access policies requiring compliant devices.

[Mobile device management](#) (MDM) helps you keep Windows 10 devices compliant. With Windows version 1809, we released a [security baseline](#) of policies. Azure Active Directory can [integrate with MDM](#) to enforce device compliance with corporate policies, and can report a device's compliance status.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Sign-ins by non-compliant devices	High	Sign-in logs	DeviceDetail.isCompliant == false	If requiring sign-in from compliant devices, alert when: <ul style="list-style-type: none"> any sign in by non-compliant devices. any access without MFA or a trusted location. If working toward requiring devices, monitor for suspicious sign-ins. Azure Sentinel template
Sign-ins by unknown devices	Low	Sign-in logs	<ul style="list-style-type: none"> DeviceDetail is empty Single factor authentication From a non-trusted location 	Look for: <ul style="list-style-type: none"> any access from out of compliance devices. any access without MFA or trusted location

Use LogAnalytics to query

Sign-ins by non-compliant devices

```

SigninLogs

| where DeviceDetail.isCompliant == false
| where conditionalAccessStatus == "success"

```

Sign-ins by unknown devices

```

SigninLogs
| where isempty(DeviceDetail.deviceId)

| where AuthenticationRequirement == "singleFactorAuthentication"

| where ResultType == "0"

| where NetworkLocationDetails == "[]"

```

Stale devices

Stale devices include devices that haven't signed in for a specified time period. Devices can become stale when a user gets a new device or loses a device, or when an Azure AD joined device is wiped or reprovisioned. Devices may also remain registered or joined when the user is no longer associated with the tenant. Stale devices should be removed so that their primary refresh tokens (PRTs) cannot be used.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Last sign-in date	Low	Graph API	approximateLastSignInDateTime	Use Graph API or PowerShell to identify and remove stale devices.

BitLocker key retrieval

Attackers who have compromised a user's device may retrieve the [BitLocker](#) keys in Azure AD. It's uncommon for users to retrieve keys, and should be monitored and investigated.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Key retrieval	Medium	Audit logs	OperationName == "Read BitLocker key"	Look for <ul style="list-style-type: none"> key retrieval other anomalous behavior by users retrieving keys.

In LogAnalytics create a query such as

```

AuditLogs
| where OperationName == "Read BitLocker key"

```

Device administrator roles

Global administrators and cloud Device Administrators automatically get local administrator rights on all Azure AD joined devices. It's important to monitor who has these rights to keep your environment safe.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Users added to global or device admin roles	High	Audit logs	Activity type = Add member to role.	<p>Look for:</p> <ul style="list-style-type: none"> • new users added to these Azure AD roles. • Subsequent anomalous behavior by machines or users.

Non-Azure AD sign-ins to virtual machines

Sign-ins to Windows or LINUX virtual machines (VMs) should be monitored for sign-ins by accounts other than Azure AD accounts.

Azure AD sign-in for LINUX

Azure AD sign-in for LINUX allows organizations to sign in to their Azure LINUX VMs using Azure AD accounts over secure shell protocol (SSH).

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Non-Azure AD account signing in, especially over SSH	High	Local authentication logs	Ubuntu: monitor /var/log/auth.log for SSH use RedHat: monitor /var/log/sssd/ for SSH use	<p>Look for:</p> <ul style="list-style-type: none"> • entries where non-Azure AD accounts are successfully connecting to VMs. • See following example.

Ubuntu example:

May 9 23:49:39 ubuntu1804 aad_certhandler[3915]: Version: 1.0.015570001; user: localusertest01

May 9 23:49:39 ubuntu1804 aad_certhandler[3915]: User 'localusertest01' is not an AAD user; returning empty result.

May 9 23:49:43 ubuntu1804 aad_certhandler[3916]: Version: 1.0.015570001; user: localusertest01

May 9 23:49:43 ubuntu1804 aad_certhandler[3916]: User 'localusertest01' is not an AAD user; returning empty result.

May 9 23:49:43 ubuntu1804 sshd[3909]: Accepted publicly for localusertest01 from 192.168.0.15 port 53582
ssh2: RSA SHA256:MiROf6f9u1w8J+46AXR1WmPjDhNWJEoXp4HMm9lvJAQ

May 9 23:49:43 ubuntu1804 sshd[3909]: pam_unix(sshd:session): session opened for user localusertest01 by (uid=0).

You can set policy for LINUX VM sign-ins, and detect and flag Linux VMs that have non-approved local accounts added. To learn more, see using [Azure Policy to ensure standards and assess compliance](#).

Azure AD sign-ins for Windows Server

Azure AD sign-in for Windows allows your organization to sign in to your Azure Windows 2019+ VMs using Azure AD accounts over remote desktop protocol (RDP).

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Non-Azure AD account signing in, especially over RDP	High	Windows Server event logs	Interactive Login to Windows VM	Event 528, logon type 10 (RemoteInteractive). Shows when a user signs in over Terminal Services or Remote Desktop.

Next Steps

See these additional security operations guide articles:

[Azure AD security operations overview](#)

[Security operations for user accounts](#)

[Security operations for privileged accounts](#)

[Security operations for Privileged Identity Management](#)

[Security operations for applications](#)

[Security operations for devices](#)

[Security operations for infrastructure](#)

Security operations for infrastructure

4/10/2022 • 13 minutes to read • [Edit Online](#)

Infrastructure has many components where vulnerabilities can occur if not properly configured. As part of your monitoring and alerting strategy for infrastructure, monitor and alert events in the following areas:

- Authentication and Authorization
- Hybrid Authentication components incl. Federation Servers
- Policies
- Subscriptions

Monitoring and alerting the components of your authentication infrastructure is critical. Any compromise can lead to a full compromise of the whole environment. Many enterprises that use Azure AD operate in a hybrid authentication environment. This means both cloud and on-premises components should be included in your monitoring and alerting strategy. Having a hybrid authentication environment also introduces another attack vector to your environment.

We recommend all the components be considered Control Plane / Tier 0 assets, as well as the accounts used to manage them. Refer to [Securing privileged assets](#) (SPA) for guidance on designing and implementing your environment. This guidance includes recommendations for each of the hybrid authentication components that could potentially be used for an Azure AD tenant.

A first step in being able to detect unexpected events and potential attacks is to establish a baseline. For all on-premises components listed in this article, see [Privileged access deployment](#), which is part of the Securing privileged assets (SPA) guide.

Where to look

The log files you use for investigation and monitoring are:

- [Azure AD Audit logs](#)
- [Sign-in logs](#)
- [Microsoft 365 Audit logs](#)
- [Azure Key Vault logs](#)

From the Azure portal you can view the Azure AD Audit logs and download as comma separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Azure AD logs with other tools that allow for greater automation of monitoring and alerting:

- [Microsoft Sentinel](#) – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- [Azure Monitor](#) – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- [Azure Event Hubs](#) integrated with a SIEM- [Azure AD logs can be integrated to other SIEMs](#) such as Splunk, ArcSight, QRadar and Sumo Logic via the Azure Event Hub integration.
- [Microsoft Defender for Cloud Apps](#) – enables you to discover and manage apps, govern across apps and

resources, and check your cloud apps' compliance.

The remainder of this article describes what you should monitor and alert on and is organized by the type of threat. Where there are specific pre-built solutions, you will find links to them following the table. Otherwise, you can build alerts using the preceding tools.

Authentication infrastructure

In hybrid environments that contain both on-premises and cloud-based resources and accounts, the Active Directory infrastructure is a key part of the authentication stack. The stack is also a target for attacks so must be configured to maintain a secure environment and must be monitored properly. Examples of current types of attacks used against your authentication infrastructure use Password Spray and Solorigate techniques. The following are links to articles we recommend:

- [Securing privileged access overview](#) – This article provides an overview of current techniques using Zero Trust techniques to create and maintain secure privileged access.
- [Microsoft Defender for Identity monitored domain activities](#) - This article provides a comprehensive list of activities to monitor and set alerts for.
- [Microsoft Defender for Identity security alert tutorial](#) - This article provides guidance on creating and implementing a security alert strategy.

The following are links to specific articles that focus on monitoring and alerting your authentication infrastructure:

- [Understand and use Lateral Movement Paths with Microsoft Defender for Identity](#) - This article describes detection techniques you can use to help identify when non-sensitive accounts are used to gain access to sensitive accounts throughout your network.
- [Working with security alerts in Microsoft Defender for Identity](#) - This article describes how to review and manage alerts once they are logged.

The following are specific things to look for:

WHAT TO MONITOR	RISK LEVEL	WHERE	NOTES
Extranet lockout trends	High	Azure AD Connect Health	Use information at Monitor AD FS using Azure AD Connect Health for tools and techniques to help detect extranet lockout trends.
Failed sign-ins	High	Connect Health Portal	Export or download the Risky IP report and follow the guidance at Risky IP report (public preview) for next steps.
In privacy compliant	Low	Azure AD Connect Health	Configure Azure AD Connect Health to be disable data collections and monitoring using the User privacy and Azure AD Connect Health article.

WHAT TO MONITOR	RISK LEVEL	WHERE	NOTES
Potential brute force attack on LDAP	Medium	Microsoft Defender for Identity	Use sensor to help detect potential brute force attacks against LDAP.
Account enumeration reconnaissance	Medium	Microsoft Defender for Identity	Use sensor to help perform account enumeration reconnaissance.
General correlation between Azure AD and Azure AD FS	Medium	Microsoft Defender for Identity	Use capabilities to correlate activities between your Azure AD and Azure AD FS environments.

Pass-through authentication monitoring

Azure Active Directory (Azure AD) Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

The following are specific things to look for:

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Azure AD pass-through authentication errors	Medium	Application and Service Logs\Microsoft\Azure AdConnect\AuthenticationAgent\Admin	AADSTS80001 – Unable to connect to Active Directory	Ensure that agent servers are members of the same AD forest as the users whose passwords need to be validated and they can connect to Active Directory.
Azure AD pass-through authentication errors	Medium	Application and Service Logs\Microsoft\Azure AdConnect\AuthenticationAgent\Admin	AADSTS8002 - A timeout occurred connecting to Active Directory	Check to ensure that Active Directory is available and is responding to requests from the agents.
Azure AD pass-through authentication errors	Medium	Application and Service Logs\Microsoft\Azure AdConnect\AuthenticationAgent\Admin	AADSTS80004 - The username passed to the agent was not valid	Ensure the user is attempting to sign in with the right username.
Azure AD pass-through authentication errors	Medium	Application and Service Logs\Microsoft\Azure AdConnect\AuthenticationAgent\Admin	AADSTS80005 - Validation encountered unpredictable WebException	A transient error. Retry the request. If it continues to fail, contact Microsoft support.
Azure AD pass-through authentication errors	Medium	Application and Service Logs\Microsoft\Azure AdConnect\AuthenticationAgent\Admin	AADSTS80007 - An error occurred communicating with Active Directory	Check the agent logs for more information and verify that Active Directory is operating as expected.

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Azure AD pass-through authentication errors	High	Win32 LogonUserA function API	Logon events 4624(s): An account was successfully logged on - correlate with – 4625(F): An account failed to log on	Use with the suspected usernames on the domain controller that is authenticating requests. Guidance at LogonUserA function (winbase.h)
Azure AD pass-through authentication errors	Medium	PowerShell script of domain controller	see query following table.	Use the information at Azure AD Connect: Troubleshoot Pass-through Authentication for additional guidance.

```

<QueryList>

<Query Id="0" Path="Security">

<Select Path="Security">*[EventData[Data[@Name='ProcessName'] and (Data='C:\Program Files\Microsoft Azure AD Connect Authentication Agent\AzureADConnectAuthenticationService.exe')]]</Select>

</Query>

</QueryList>

```

AppProxy Connector

Azure AD and Azure AD Application Proxy give remote users a single sign-on (SSO) experience. Users securely connect to on-premises apps without a virtual private network (VPN) or dual-homed servers and firewall rules. If your Azure AD Application Proxy connector server is compromised, attackers could alter the SSO experience or change access to published applications.

To configuring monitoring for Application Proxy, see [Troubleshoot Application Proxy problems and error messages](#). The data file that logs information can be found in Applications and Services Logs\Microsoft\AadApplicationProxy\Connector\Admin. For a complete reference guide to audit activity, see [Azure AD audit activity reference](#). Specific things to monitor:

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Kerberos errors	Medium	Various tools	Medium	Kerberos authentication error guidance under Kerberos errors on Troubleshoot Application Proxy problems and error messages .

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
DC security issues	High	DC Security Audit logs	Event ID 4742(S): A computer account was changed -and- Flag – Trusted for Delegation -or- Flag – Trusted to Authenticate for Delegation	Investigate any flag change.
Pass-the-ticket like attacks	High			Follow guidance in: <ul style="list-style-type: none"> • Security principal reconnaissance (LDAP) (external ID 2038) • Tutorial: Compromised credential alerts • Understand and use Lateral Movement Paths with Microsoft Defender for Identity • Understanding entity profiles

Legacy authentication settings

For multifactor authentication (MFA) to be effective, you also need to block legacy authentication. You then need to monitor your environment and alert on any use of legacy authentication. This is because legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA. This makes these protocols preferred entry points for attackers of your organization. For more information on tools that you can use to block legacy authentication, see [New tools to block legacy authentication in your organization](#).

Legacy authentication is captured in the Azure AD Sign-ins log as part of the detail of the event. You can use the Azure Monitor workbook to help with identifying legacy authentication usage. For more information, see [Sign-ins using legacy authentication](#), which is part of [How to use Azure Monitor Workbooks for Azure Active Directory reports](#). You can also use the Insecure protocols workbook for Microsoft Sentinel. For more information, see [Microsoft Sentinel Insecure Protocols Workbook Implementation Guide](#). Specific activities to monitor include:

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Legacy authentications	High	Azure AD Sign-ins log	ClientApp : POP ClientApp : IMAP ClientApp : MAPI ClientApp: SMTP ClientApp : ActiveSync go to EXO Other Clients = SharePoint and EWS	In federated domain environments, failed authentications are not recorded so will not appear in the log.

Azure AD Connect

Azure AD Connect provides a centralized location that enables account and attribute synchronization between your on-premises and cloud-based Azure AD environment. Azure AD Connect is the Microsoft tool designed to

meet and accomplish your hybrid identity goals. It provides the following features:

- **Password hash synchronization** - A sign-in method that synchronizes a hash of a user's on-premises AD password with Azure AD.
- **Synchronization** - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
- **Health Monitoring** - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Synchronizing identity between your on-premises environment and your cloud environment introduces a new attack surface for your on-premises and cloud-based environment. We recommend:

- You treat your Azure AD Connect primary and staging servers as Tier 0 Systems in your control plane.
- You follow a standard set of policies that govern each type of account and its usage in your environment.
- You install Azure AD Connect and Connect Health. These primarily provide operational data for the environment.

Logging of Azure AD Connect operations occurs in different ways:

- The Azure AD Connect wizard logs data to \ProgramData\AADConnect . Each time the wizard is invoked, a timestamped trace log file is created. The trace log can be imported into Sentinel or other 3rd party security information and event management (SIEM) tools for analysis.
- Some operations initiate a PowerShell script to capture logging information. To collect this data, you must make sure script block logging is enabled.

Monitoring configuration changes

Azure AD uses Microsoft SQL Server Data Engine or SQL to store Azure AD Connect configuration information. Therefore, monitoring and auditing of the log files associated with configuration should be included in your monitoring and auditing strategy. Specifically, include the following tables in your monitoring and alerting strategy.

WHAT TO MONITOR	WHERE	NOTES
mms_management_agent	SQL service audit records	See SQL Server Audit Records
mms_partition	SQL service audit records	See SQL Server Audit Records
mms_run_profile	SQL service audit records	See SQL Server Audit Records
mms_server_configuration	SQL service audit records	See SQL Server Audit Records
mms_synchronization_rule	SQL service audit records	See SQL Server Audit Records

For information on what and how to monitor configuration information refer to:

- For SQL server, see [SQL Server Audit Records](#).
- For Microsoft Sentinel, see [Connect to Windows servers to collect security events](#).
- For information on configuring and using Azure AD Connect, see [What is Azure AD Connect?](#)

Monitoring and troubleshooting synchronization

One function of Azure AD Connect is to synchronize hash synchronization between a user's on-premises password and Azure AD. If passwords are not synchronizing as expected, the synchronization might affect a subset of users or all users. Use the following to help verify proper operation or troubleshoot issues:

- Information for checking and troubleshooting hash synchronization, see [Troubleshoot password hash synchronization with Azure AD Connect sync](#).
- Modifications to the connector spaces, see [Troubleshoot Azure AD Connect objects and attributes](#).

Important resources on monitoring

WHAT TO MONITOR	RESOURCES
Hash synchronization validation	See Troubleshoot password hash synchronization with Azure AD Connect sync
Modifications to the connector spaces	see Troubleshoot Azure AD Connect objects and attributes
Modifications to the rules you configured	Specifically, monitor filtering changes, domain and OU changes, attribute changes, and group-based changes
SQL and MSDE changes	Changes to logging parameters and addition of custom functions

Monitor the following:

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Scheduler changes	High	PowerShell	Set-ADSyncScheduler	Look for modifications to schedule
Changes to scheduled tasks	High	Azure AD Audit logs	Activity = 4699(S): A scheduled task was deleted -or- Activity = 4701(s): A scheduled task was disabled -or- Activity = 4701(s): A scheduled task was updated	Monitor all

- For more information on logging PowerShell script operations, refer to [Enabling Script Block Logging](#), which is part of the PowerShell reference documentation.
- For more information on configuring PowerShell logging for analysis by Splunk, refer to [Get Data into Splunk User Behavior Analytics](#).

Monitoring seamless single sign-on

Azure Active Directory (Azure AD) Seamless Single Sign-On (Seamless SSO) automatically signs in users when they are on their corporate desktops that are connected to your corporate network. Seamless SSO provides your users with easy access to your cloud-based applications without needing any additional on-premises components. SSO uses the pass-through authentication and password hash synchronization capabilities provided by Azure AD Connect.

Monitoring single sign-on and Kerberos activity can help you detect general credential theft attack patterns.

Monitor using the following information:

WHAT TO MONITOR	RISK LEVEL	WHERE	FILTER/SUB-FILTER	NOTES
Errors associated with SSO and Kerberos validation failures	Medium	Azure AD Sign-ins log		Single sign-on list of error codes at Single sign-on .
Query for troubleshooting errors	Medium	PowerShell	See query following table. check in each forest with SSO enabled.	Check in each forest with SSO enabled.
Kerberos-related events	High	Microsoft Defender for Identity monitoring		Review guidance available at Microsoft Defender for Identity Lateral Movement Paths (LMPs)

```
<QueryList>

<Query Id="0" Path="Security">

<Select Path="Security">*[EventData[Data[@Name='ServiceName'] and (Data='AZUREADSSOACC$')]]</Select>

</Query>

</QueryList>
```

Password protection policies

If you deploy Azure AD Password Protection, monitoring and reporting are essential tasks. The following links provide details to help you understand various monitoring techniques, including where each service logs information and how to report on the use of Azure AD Password Protection.

The domain controller (DC) agent and proxy services both log event log messages. All PowerShell cmdlets described below are only available on the proxy server (see the `AzureADPasswordProtection` PowerShell module). The DC agent software does not install a PowerShell module.

Detailed information for planning and implementing on-premises password protection is available at [Plan and deploy on-premises Azure Active Directory Password Protection](#). For monitoring details, see [Monitor on-premises Azure AD Password Protection](#). On each domain controller, the DC agent service software writes the results of each individual password validation operation (and other status) to the following local event log:

- `\Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Admin`
- `\Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Operational`
- `\Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Trace`

The DC agent Admin log is the primary source of information for how the software is behaving. By default, the Trace log is off and must be enabled before data is logged. To troubleshoot application proxy problems and error messages, detailed information is available at [Troubleshoot Azure Active Directory Application Proxy](#).

Information for these events is logged in:

- `Applications and Services Logs\Microsoft\AadApplicationProxy\Connector\Admin`
- `Azure AD Audit Log, Category Application Proxy`

Complete reference for Azure AD audit activities is available at [Azure Active Directory \(Azure AD\) audit activity reference](#).

Next steps

See these additional security operations guide articles:

[Azure AD security operations overview](#)

[Security operations for user accounts](#)

[Security operations for privileged accounts](#)

[Security operations for Privileged Identity Management](#)

[Security operations for applications](#)

[Security operations for devices](#)

[Security operations for infrastructure](#)

Protecting Microsoft 365 from on-premises attacks

4/10/2022 • 11 minutes to read • [Edit Online](#)

Many customers connect their private corporate networks to Microsoft 365 to benefit their users, devices, and applications. However, these private networks can be compromised in many well-documented ways. Because Microsoft 365 acts as a sort of nervous system for many organizations, it's critical to protect it from compromised on-premises infrastructure.

This article shows you how to configure your systems to protect your Microsoft 365 cloud environment from on-premises compromise. We focus primarily on:

- Azure Active Directory (Azure AD) tenant configuration settings.
- How Azure AD tenants can be safely connected to on-premises systems.
- The tradeoffs required to operate your systems in ways that protect your cloud systems from on-premises compromise.

We strongly recommend you implement this guidance to secure your Microsoft 365 cloud environment.

NOTE

This article was initially published as a blog post. It has been moved to its current location for longevity and maintenance.

To create an offline version of this article, use your browser's print-to-PDF functionality. Check back here frequently for updates.

Primary threat vectors from compromised on-premises environments

Your Microsoft 365 cloud environment benefits from an extensive monitoring and security infrastructure. Using machine learning and human intelligence, Microsoft 365 looks across worldwide traffic. It can rapidly detect attacks and allow you to reconfigure nearly in real time.

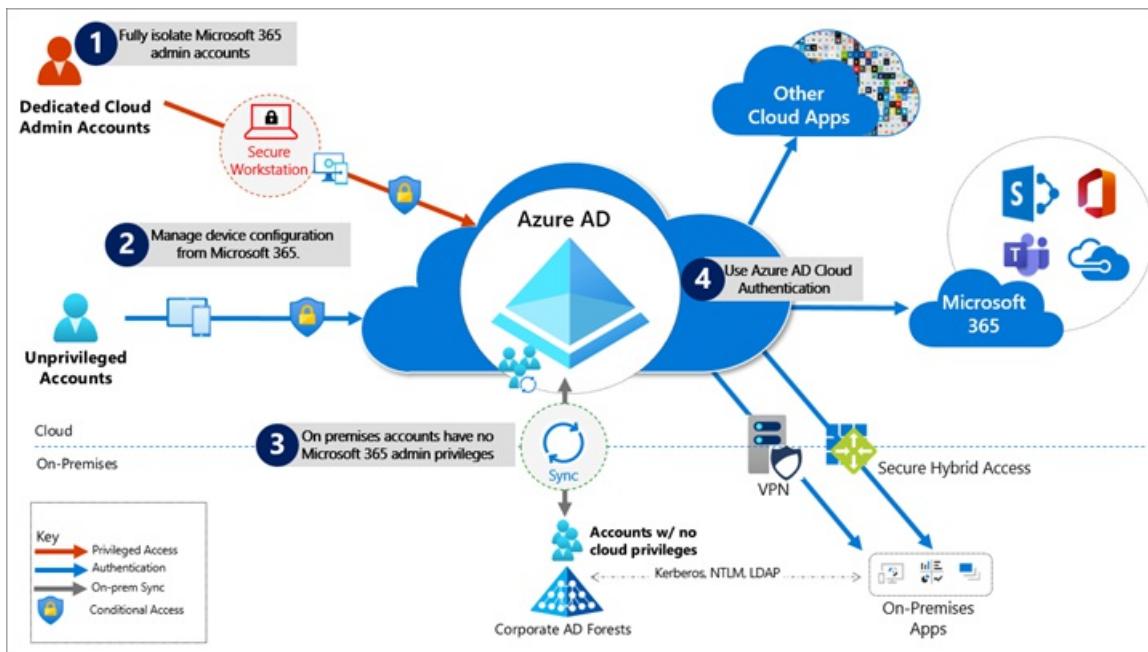
In hybrid deployments that connect on-premises infrastructure to Microsoft 365, many organizations delegate trust to on-premises components for critical authentication and directory object state management decisions. Unfortunately, if the on-premises environment is compromised, these trust relationships become an attacker's opportunities to compromise your Microsoft 365 environment.

The two primary threat vectors are *federation trust relationships* and *account synchronization*. Both vectors can grant an attacker administrative access to your cloud.

- **Federated trust relationships**, such as SAML authentication, are used to authenticate to Microsoft 365 through your on-premises identity infrastructure. If a SAML token-signing certificate is compromised, federation allows anyone who has that certificate to impersonate any user in your cloud. *We recommend you disable federation trust relationships for authentication to Microsoft 365 when possible.*
- **Account synchronization** can be used to modify privileged users (including their credentials) or groups that have administrative privileges in Microsoft 365. *We recommend you ensure that synchronized objects hold no privileges beyond a user in Microsoft 365*, either directly or through inclusion in trusted roles or groups. Ensure these objects have no direct or nested assignment in trusted cloud roles or groups.

Protecting Microsoft 365 from on-premises compromise

To address the threat vectors outlined earlier, we recommend you adhere to the principles illustrated in the following diagram:



1. Fully isolate your Microsoft 365 administrator accounts. They should be:

- Mastered in Azure AD.
- Authenticated by using multifactor authentication.
- Secured by Azure AD Conditional Access.
- Accessed only by using Azure-managed workstations.

These administrator accounts are restricted-use accounts. *No on-premises accounts should have administrative privileges in Microsoft 365.*

For more information, see the [overview of Microsoft 365 administrator roles](#). Also see [Roles for Microsoft 365 in Azure AD](#).

2. Manage devices from Microsoft 365. Use Azure AD join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure. These dependencies can compromise device and security controls.

3. Ensure no on-premises account has elevated privileges to Microsoft 365. Some accounts access on-premises applications that require NTLM, LDAP, or Kerberos authentication. These accounts must be in the organization's on-premises identity infrastructure. Ensure that these accounts, including service accounts, aren't included in privileged cloud roles or groups. Also ensure that changes to these accounts can't affect the integrity of your cloud environment. Privileged on-premises software must not be capable of affecting Microsoft 365 privileged accounts or roles.

4. Use Azure AD cloud authentication to eliminate dependencies on your on-premises credentials. Always use strong authentication, such as Windows Hello, FIDO, Microsoft Authenticator, or Azure AD multifactor authentication.

Specific security recommendations

The following sections provide specific guidance about how to implement the principles described earlier.

Isolate privileged identities

In Azure AD, users who have privileged roles, such as administrators, are the root of trust to build and manage

the rest of the environment. Implement the following practices to minimize the effects of a compromise.

- Use cloud-only accounts for Azure AD and Microsoft 365 privileged roles.
- Deploy [privileged access devices](#) for privileged access to manage Microsoft 365 and Azure AD.
- Deploy [Azure AD Privileged Identity Management](#) (PIM) for just-in-time (JIT) access to all human accounts that have privileged roles. Require strong authentication to activate roles.
- Provide administrative roles that allow the [least privilege necessary to do required tasks](#).
- To enable a rich role assignment experience that includes delegation and multiple roles at the same time, consider using Azure AD security groups or Microsoft 365 Groups. These groups are collectively called *cloud groups*. Also [enable role-based access control](#). You can use [administrative units](#) to restrict the scope of roles to a portion of the organization.
- Deploy [emergency access accounts](#). Do *not* use on-premises password vaults to store credentials.

For more information, see [Securing privileged access](#). Also see [Secure access practices for administrators in Azure AD](#).

Use cloud authentication

Credentials are a primary attack vector. Implement the following practices to make credentials more secure:

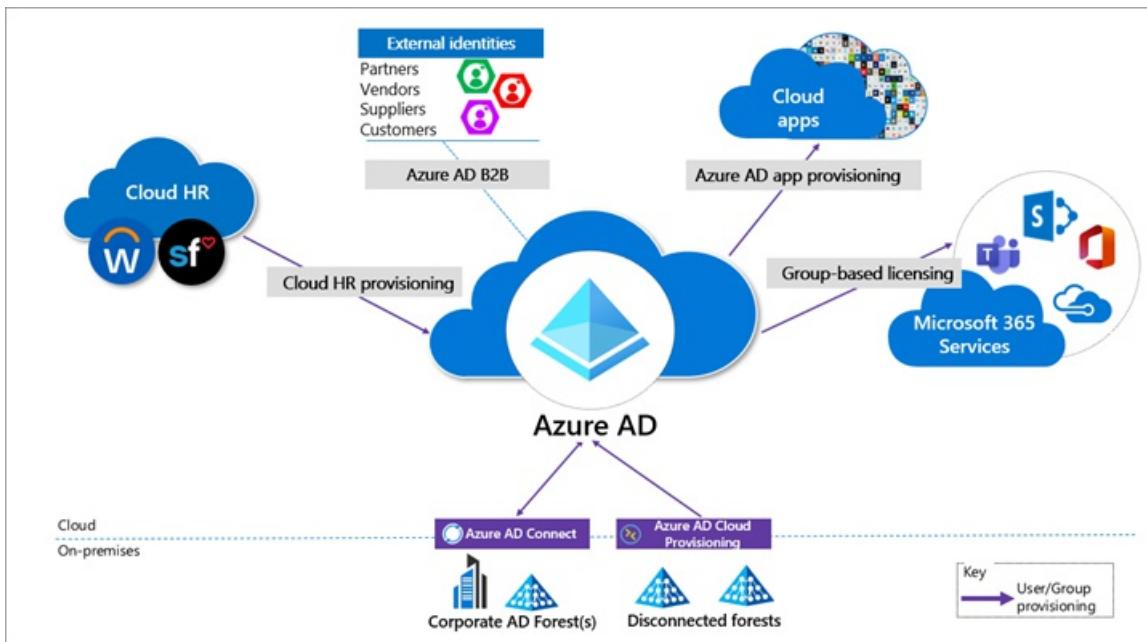
- [Deploy passwordless authentication](#). Reduce the use of passwords as much as possible by deploying passwordless credentials. These credentials are managed and validated natively in the cloud. Choose from these authentication methods:
 - [Windows Hello for business](#)
 - [The Microsoft Authenticator app](#)
 - [FIDO2 security keys](#)
- [Deploy multifactor authentication](#). Provision [multiple strong credentials by using Azure AD multifactor authentication](#). That way, access to cloud resources will require a credential that's managed in Azure AD in addition to an on-premises password that can be manipulated. For more information, see [Create a resilient access control management strategy by using Azure AD](#).

Limitations and tradeoffs

- Hybrid account password management requires hybrid components such as password protection agents and password writeback agents. If your on-premises infrastructure is compromised, attackers can control the machines on which these agents reside. This vulnerability won't compromise your cloud infrastructure. But your cloud accounts won't protect these components from on-premises compromise.
- On-premises accounts synced from Active Directory are marked to never expire in Azure AD. This setting is usually mitigated by on-premises Active Directory password settings. However, if your on-premises instance of Active Directory is compromised and synchronization is disabled, you must set the [EnforceCloudPasswordPolicyForPasswordSyncedUsers](#) option to force password changes.

Provision user access from the cloud

Provisioning refers to the creation of user accounts and groups in applications or identity providers.



We recommend the following provisioning methods:

- **Provision from cloud HR apps to Azure AD:** This provisioning enables an on-premises compromise to be isolated, without disrupting your joiner-mover-leaver cycle from your cloud HR apps to Azure AD.
- **Cloud applications:** Where possible, deploy [Azure AD app provisioning](#) as opposed to on-premises provisioning solutions. This method protects some of your software-as-a-service (SaaS) apps from being affected by malicious hacker profiles in on-premises breaches.
- **External identities:** Use [Azure AD B2B collaboration](#). This method reduces the dependency on on-premises accounts for external collaboration with partners, customers, and suppliers. Carefully evaluate any direct federation with other identity providers. We recommend limiting B2B guest accounts in the following ways:
 - Limit guest access to browsing groups and other properties in the directory. Use the external collaboration settings to restrict guests' ability to read groups they're not members of.
 - Block access to the Azure portal. You can make rare necessary exceptions. Create a Conditional Access policy that includes all guests and external users. Then [implement a policy to block access](#).
- **Disconnected forests:** Use [Azure AD cloud provisioning](#). This method enables you to connect to disconnected forests, eliminating the need to establish cross-forest connectivity or trusts, which can broaden the effect of an on-premises breach.

Limitations and tradeoffs

When used to provision hybrid accounts, the Azure-AD-from-cloud-HR system relies on on-premises synchronization to complete the data flow from Active Directory to Azure AD. If synchronization is interrupted, new employee records won't be available in Azure AD.

Use cloud groups for collaboration and access

Cloud groups allow you to decouple your collaboration and access from your on-premises infrastructure.

- **Collaboration:** Use Microsoft 365 Groups and Microsoft Teams for modern collaboration. Decommission on-premises distribution lists, and [upgrade distribution lists to Microsoft 365 Groups in Outlook](#).
- **Access:** Use Azure AD security groups or Microsoft 365 Groups to authorize access to applications in

Azure AD.

- **Office 365 licensing:** Use group-based licensing to provision to Office 365 by using cloud-only groups. This method decouples control of group membership from on-premises infrastructure.

Owners of groups that are used for access should be considered privileged identities to avoid membership takeover in an on-premises compromise. A takeover would include direct manipulation of group membership on-premises or manipulation of on-premises attributes that can affect dynamic group membership in Microsoft 365.

Manage devices from the cloud

Use Azure AD capabilities to securely manage devices.

- **Use Windows 10 workstations:** [Deploy Azure AD joined](#) devices with MDM policies. Enable [Windows Autopilot](#) for a fully automated provisioning experience.
 - Deprecate machines that run Windows 8.1 and earlier.
 - Don't deploy server OS machines as workstations.
 - Use [Microsoft Intune](#) as the source of authority for all device management workloads.
- **Deploy privileged access devices:** Use privileged access to manage Microsoft 365 and Azure AD as part of a complete approach to [Securing privileged access](#).

Workloads, applications, and resources

- **On-premises single-sign-on (SSO) systems**

Deprecate any on-premises federation and web access management infrastructure. Configure applications to use Azure AD.

- **SaaS and line-of-business (LOB) applications that support modern authentication protocols**

[Use Azure AD for SSO](#). The more apps you configure to use Azure AD for authentication, the less risk in an on-premises compromise.

- **Legacy applications**

- You can enable authentication, authorization, and remote access to legacy applications that don't support modern authentication. Use [Azure AD Application Proxy](#). You can also enable them through a network or application delivery controller solution by using [secure hybrid access partner integrations](#).

- Choose a VPN vendor that supports modern authentication. Integrate its authentication with Azure AD. In an on-premises compromise, you can use Azure AD to disable or block access by disabling the VPN.

- **Application and workload servers**

- Applications or resources that required servers can be migrated to Azure infrastructure as a service (IaaS). Use [Azure AD Domain Services](#) (Azure AD DS) to decouple trust and dependency on on-premises instances of Active Directory. To achieve this decoupling, make sure virtual networks used for Azure AD DS don't have a connection to corporate networks.

- Follow the guidance for [credential tiering](#). Application servers are typically considered tier-1 assets.

Conditional Access policies

Use Azure AD Conditional Access to interpret signals and use them to make authentication decisions. For more information, see the [Conditional Access deployment plan](#).

- Use Conditional Access to [block legacy authentication protocols](#) whenever possible. Additionally, disable legacy authentication protocols at the application level by using an application-specific configuration.

For more information, see [Legacy authentication protocols](#). Or see specific details for [Exchange Online](#) and [SharePoint Online](#).

- Implement the recommended [identity and device access configurations](#).
- If you're using a version of Azure AD that doesn't include Conditional Access, ensure that you're using the [Azure AD security defaults](#).

For more information about Azure AD feature licensing, see the [Azure AD pricing guide](#).

Monitor

After you configure your environment to protect your Microsoft 365 from an on-premises compromise, [proactively monitor](#) the environment.

Scenarios to monitor

Monitor the following key scenarios, in addition to any scenarios specific to your organization. For example, you should proactively monitor access to your business-critical applications and resources.

- **Suspicious activity**

Monitor all [Azure AD risk events](#) for suspicious activity. [Azure AD Identity Protection](#) is natively integrated with Microsoft Defender for Cloud.

Define the network [named locations](#) to avoid noisy detections on location-based signals.

- **User and Entity Behavioral Analytics (UEBA) alerts**

Use UEBA to get insights on anomaly detection.

- Microsoft Defender for Cloud Apps provides [UEBA in the cloud](#).
- You can [integrate on-premises UEBA from Azure Advanced Threat Protection \(ATP\)](#). Defender for Cloud Apps reads signals from Azure AD Identity Protection.

- **Emergency access accounts activity**

Monitor any access that uses [emergency access accounts](#). Create alerts for investigations. This monitoring must include:

- Sign-ins.
- Credential management.
- Any updates on group memberships.
- Application assignments.

- **Privileged role activity**

Configure and review security [alerts generated by Azure AD Privileged Identity Management \(PIM\)](#).

Monitor direct assignment of privileged roles outside PIM by generating alerts whenever a user is assigned directly.

- **Azure AD tenant-wide configurations**

Any change to tenant-wide configurations should generate alerts in the system. These changes include but aren't limited to:

- Updated custom domains.
- Azure AD B2B changes to allowlists and blocklists.
- Azure AD B2B changes to allowed identity providers (SAML identity providers through direct federation or social sign-ins).
- Conditional Access or Risk policy changes.

- **Application and service principal objects**

- New applications or service principals that might require Conditional Access policies.
- Credentials added to service principals.
- Application consent activity.

- **Custom roles**

- Updates to the custom role definitions.
- Newly created custom roles.

Log management

Define a log storage and retention strategy, design, and implementation to facilitate a consistent tool set. For example, you could consider security information and event management (SIEM) systems like Microsoft Sentinel, common queries, and investigation and forensics playbooks.

- **Azure AD logs:** Ingest generated logs and signals by consistently following best practices for settings such as diagnostics, log retention, and SIEM ingestion.

The log strategy must include the following Azure AD logs:

- Sign-in activity
- Audit logs
- Risk events

Azure AD provides [Azure Monitor integration](#) for the sign-in activity log and audit logs. Risk events can be ingested through the [Microsoft Graph API](#). You can [stream Azure AD logs to Azure Monitor logs](#).

- **Hybrid infrastructure OS security logs:** All hybrid identity infrastructure OS logs should be archived and carefully monitored as a tier-0 system, because of the surface-area implications. Include the following elements:

- Azure AD Connect. [Azure AD Connect Health](#) must be deployed to monitor identity synchronization.
- Application Proxy agents
- Password writeback agents
- Password Protection Gateway machines
- Network policy servers (NPSs) that have the Azure AD multifactor authentication RADIUS extension

Next steps

- Build resilience into identity and access management by using Azure AD
- Secure external access to resources
- Integrate all your apps with Azure AD

Securing external collaboration in Azure Active Directory and Microsoft 365

4/10/2022 • 2 minutes to read • [Edit Online](#)

Secure collaboration with external partners ensures that the right external partners have appropriate access to internal resources for the right length of time. Through a holistic governance approach, you can reduce security risks, meet compliance goals, and ensure that you know who has access.

Ungoverned collaboration leads to a lack of clarity on ownership of access, and the possibility of sensitive resources being exposed. Moving to secure and governed collaboration can ensure that there are clear lines of ownership and accountability for external users' access. This includes:

- Managing the external organizations, and users within them, that have access to resources.
- Ensuring that access is appropriate, reviewed, and time bound where appropriate.
- Empowering business owners to manage collaboration within IT-created guard rails.

If you must meet compliance frameworks, governed collaboration enables you to attest to the appropriateness of access.

Microsoft offers comprehensive suites of tools for secure external access. Azure Active Directory (Azure AD) B2B Collaboration is at the center of any external collaboration plan. Azure AD B2B can integrate with other tools in Azure AD, and tools in Microsoft 365 services, to help secure and manage your external access.

This document set is designed to enable you to move from ad hoc or loosely governed external collaboration to a more secure state.

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Determine your security posture for external access

4/10/2022 • 3 minutes to read • [Edit Online](#)

As you consider governing external access, you'll need to assess the security and collaboration needs for your organization overall, and within each scenario. At the organizational level, consider the amount of control you need your IT team to have over day-to-day collaboration. Organizations in regulated industries may require more IT control. For example, a defense contractor may be required to positively identify and document each external user, their access, and the removal of access. This requirement may be on all access, or on specific scenarios or workloads. On the other end of the spectrum, a consulting firm may generally allow end users to determine the external users they need to collaborate with, within certain IT guard rails.



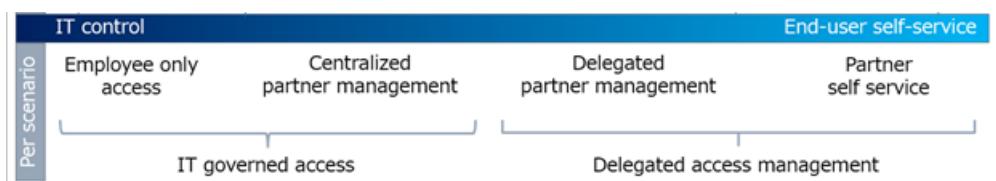
NOTE

Overly tight control on collaboration can lead to higher IT budgets, reduced productivity, and delayed business outcomes. When official collaboration channels are perceived as too onerous, end users tend to go around IT provided systems to get their jobs done, by for example emailing unsecured documents.

Think in terms of scenarios

In many cases IT can delegate partner access, at least in some scenarios, while providing guard rails for security. The IT guard rails can help ensure that intellectual property stays secure, while empowering employees to collaborate with partners to get work done.

As you consider the scenarios within your organization, assess the need for employee versus business partner access to resources. A bank may have compliance needs that restrict access to certain resources, like user account information, to a small group of internal employees. Conversely, the same bank may enable delegated access for partners working on a marketing campaign.



In each scenario, consider

- the sensitivity of the information at risk
- whether you need to restrict what partners can see about other users
- the cost of a breach vs the weight of centralized control and end-user friction

You may also start with centrally managed controls to meet compliance targets and delegate control to end users over time. All access management models may simultaneously coexist within an organization.

The use of **partner managed credentials** provides your organization with an essential signal that terminates

access to your resources once the external user has lost access to the resources of their own company.

Goals of securing external access

The goals of IT-governed and delegated access differ.

The primary goals of IT-governed access are to:

- Meet governance, regulatory, and compliance (GRC) targets.
- Tightly control partner access and what partners can see about member users, groups, and other partners.

The primary goals of delegating access are to:

- Enable business owners to govern who they collaborate with, within IT constraints.
- Enable business partners to request access based on rules defined by business owners.

Whichever you enact for your organization and scenarios you'll need to:

- **Control access to applications, data, and content.** This can be accomplished through a variety of methods, depending on your versions of [Azure AD](#) and [Microsoft 365](#).
- **Reduce the attack surface.** [Privileged identity management](#), [data loss prevention \(DLP\)](#), and [encryption capabilities](#) reduce the attack surface.
- **Regularly review activity and audit log to confirm compliance.** IT can delegate access decisions to business owners through entitlement management while access reviews provide a way to periodically confirm continued access. Automated data classification with sensitivity labels helps to automate encryption of sensitive content making it easy for employee end users to comply.

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#) (You are here.)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Discover the current state of external collaboration in your organization

4/10/2022 • 3 minutes to read • [Edit Online](#)

Before discovering the current state of your external collaboration, you should [determine your desired security posture](#). You'll consider your organization's needs for centralized vs. delegated control, and any relevant governance, regulatory, and compliance targets.

Individuals in your organization are probably already collaborating with users from other organizations. Collaboration can be through features in productivity applications like Microsoft 365, by emailing, or by otherwise sharing resources with external users. The pillars of your governance plan will form as you discover:

- The users who are initiating external collaboration.
- The external users and organizations you're collaborating with.
- The access being granted to external users.

Users initiating external collaboration

The users initiating external collaboration best understand the applications most relevant for external collaboration, and when that access should end. Understanding these users can help you determine who should be delegated permission to inviting external users, create access packages, and complete access reviews.

To find users who are currently collaborating, review the [Microsoft 365 audit log for sharing and access request activities](#). You can also review the [Azure AD audit log for details on who invited B2B users to your directory](#).

Find current collaboration partners

External users may be [Azure AD B2B users](#) (preferable) with partner-managed credentials, or external users with locally provisioned credentials. These users are typically (but not always) marked with a UserType of Guest. You can enumerate guest users through the [Microsoft Graph API](#), [PowerShell](#), or the [Azure portal](#).

Use email domains and companyName property

External organizations can be determined by the domain names of external user email addresses. If consumer identity providers such as Google are supported, this may not be possible. In this case we recommend that you write the companyName attribute to clearly identify the user's external organization.

Use allow or deny lists

Consider whether your organization wants to allow collaboration with only specific organizations. Alternatively, consider if your organization wants to block collaboration with specific organizations. At the tenant level, there is an [allow or deny list](#), which can be used to control overall B2B invitations and redemptions regardless of source (such as Microsoft Teams, Microsoft SharePoint, or the Azure portal).

If you're using entitlement management, you can also scope access packages to a subset of your partners by using the Specific connected organizations setting as shown below.

The screenshot shows the 'New access package' creation interface in Microsoft Azure. The 'Requests' tab is selected. The 'For users in your directory' option is chosen. A note says: 'Allow users and groups in your directory to request this access package'. The 'For users not in your directory' option is also available. The 'None (administrator direct assignments only)' option is shown but not selected. A note for this option says: 'Allow administrators to directly assign specific users to this access package. Users cannot request this access package'. Below this, there's a section for selecting connected organizations, with 'Specific connected organizations' selected. Other options include 'All configured connected organizations' and 'All users (All connected organizations + any new external users)'. A note says: 'Learn more about setting up policies for users not yet in your directory'. At the bottom, there are 'Review + Create', 'Previous', and 'Next: Requestor Information >' buttons.

Find access being granted to external users

Once you have an inventory of external users and organizations, you can determine the access granted to these users using the Microsoft Graph API to determine Azure AD [group membership](#) or [direct application assignment](#) in Azure AD.

Enumerate application-specific permissions

You may also be able to perform application-specific permission enumeration. For example, you can programmatically generate a permission report for SharePoint Online by using [this script](#).

Specifically investigate access to all of your business-sensitive and business-critical apps so that you are fully aware of any external access.

Detect ad hoc sharing

If your email and network plans enable it, you can investigate content being shared through email or through unauthorized software as a service (SaaS) apps. [Microsoft 365 Data Loss Protection](#) helps you identify, prevent, and monitor the accidental sharing of sensitive information across your Microsoft 365 infrastructure. [Microsoft Defender for Cloud Apps](#) can help you identify the use of unauthorized SaaS apps in your environment.

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#)
2. [Discover your current state](#) (You are here.)
3. [Create a governance plan](#)
4. [Use groups for security](#)

5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

3. Create a security plan for external access

4/10/2022 • 8 minutes to read • [Edit Online](#)

Now that you have [determined your desired security posture](#) [security posture for external access](#) and [discovered your current collaboration state](#), you can create an external user security and governance plan.

This plan should document the following:

- The applications and other resources that should be grouped for access.
- The appropriate sign-in conditions for external users. These can include device state, sign-in location, client application requirements, and user risk.
- Business policies on when to review and remove access.
- User populations to be grouped and treated similarly.

Once these areas are documented, you can use identity and access management policies from Microsoft or any other identity provider (IdP) to implement this plan.

Document resources to be grouped for access

There are multiple ways to group resources for access.

- Microsoft Teams groups files, conversation threads, and other resources in one place. You should formulate an external access strategy for Microsoft Teams. See [Secure access to Teams, OneDrive, and SharePoint](#).
- Entitlement Management Access Packages enable you to create a single package of applications and other resources to which you can grant access.
- Conditional Access policies can be applied to up to 250 applications with the same access requirements.

However you will manage access, you must document which applications should be grouped together.

Considerations should include:

- **Risk profile.** What is the risk to your business if a bad actor gained access to an application? Consider coding each application as high, medium, or low risk. Be cautious about grouping high-risk applications with low-risk ones.
 - Document applications that should never be shared with external users as well.
- **Compliance Frameworks.** What if any compliance frameworks must an application meet? What are the access and review requirements?
- **Applications for specific job roles or departments.** Are there applications that should be grouped because all users in a specific job role or department will need access?
- **Collaboration-focused applications.** What collaboration-focused applications should external users be able to access? Microsoft Teams and SharePoint may need to be accessible. For productivity applications within Office 365, like Word and Excel, will external users bring their own licenses, or will you need to license them and provide access?

For each grouping of applications and resources that you want to make accessible to external users , document the following:

- A descriptive name for the group, for example *High_Risk_External_Access_Finance*.
- Complete list of all applications and resources in the group.
- Application and resource owners and contact information.
- Whether the access is controlled by IT, or delegated to the business owner.
- Any prerequisites, for example completing a background check or a training, for access.
- Any compliance requirements for accessing the resources.
- Any additional challenges, for example requiring multi-factor-authentication for specific resources.
- How often access will be reviewed, by whom, and where it will be documented.

This type of governance plan can and should also be completed for internal access as well.

Document sign-in conditions for external users.

As part of your plan you must determine the sign-in requirements for your external users as they access resources. Sign-in requirements are often based on the risk profile of the resources, and the risk assessment of the users' sign-in.

Sign-in conditions are configured in [Azure AD Conditional Access](#) and are made up of a condition and an outcome. For example, when to require multi-factor authentication

Resource risk-based sign-in conditions.

APPLICATION RISK PROFILE	CONSIDER THESE POLICIES FOR TRIGGERING MULTI-FACTOR AUTHENTICATION
Low risk	Require MFA for specific application sets
Med risk	Require MFA when other risks present
High risk	Require MFA always for external users

Today, you can [enforce multi-factor authentication for B2B users in your tenant](#).

User- and device-based sign in conditions.

USER OR SIGN-IN RISK	CONSIDER THESE POLICIES
Device	Require compliant devices
Mobile apps	Require approved apps
Identity protection shows high risk	Require user to change password
Network location	Require sign in from a specific IP address range to highly confidential projects

Today, to use device state as an input to a policy, the device must be registered or joined to your tenant.

[Identity Protection risk-based policies](#) can be used. However, issues must be mitigated in the user's home tenant.

For [network locations](#), you can restrict access to any IP addresses range that you own. You might use this if you only want external partners accessing an application while they are on site at your organization.

[Learn more about conditional access policies.](#)

Document access review policies

Document your business policies for when you need to review access to resources, and when you need to remove account access for external users. Inputs to these decisions may include:

- Requirements detailed in any compliance frameworks.
- Internal business policies and processes
- User behavior

While your policies will be highly customized to your needs, consider the following:

- **Entitlement Management Access Reviews.** Use the functionality in Entitlement Management to
 - [Automatically expire access packages](#), and thus external user access to the included resources.
 - Set a [required review frequency](#) for access reviews.
 - If you are using [connected organizations](#) to group all users from a single partner, schedule regular reviews with the business owner and the partner representative.
- **Microsoft 365 Groups.** Set a [group expiration policy](#) for Microsoft 365 Groups to which external users are invited.
- **Other options.** If external users have access outside of Entitlement Management access packages or Microsoft 365 groups, set up business process to review when accounts should be made inactive or deleted. For example:
 - Remove sign-in ability for any account not signed in to for 90 days.
 - Assess access needs and take action at the end of every project with external users.

Determine your access control methods

Now that you know what you want to control access to, how those assets should be grouped for common access, and required sign-in and access review policies, you can decide on how to accomplish your plan.

Some functionality, for example [Entitlement Management](#), is only available with an Azure AD Premium 2 (P2) licenses. Microsoft 365 E5 and Office 365 E5 licenses include Azure AD P2 licenses.

Other combinations of Microsoft 365, Office 365 and Azure AD also enable some functionality for managing external users. See [Information Protection](#) for more information.

NOTE

Licenses are per user. Therefore, you can have specific users, including administrators and business owners delegated access control, at the Azure AD P2 or Microsoft 365 E5 level without enabling those licenses for all users. Your first 50,000 external users are free. If you do not enable P2 licenses for your other internal users, they will not be able to use entitlement management functionality like Access packages.

Govern access with Azure AD P2 and Microsoft / Office 365 E5

Azure AD P2 and Microsoft 365 E5 have the full suite of security and governance tools.

Provisioning, signing in, reviewing access, and deprovisioning. Bolded entries are preferred methods

FEATURE	PROVISION EXTERNAL USERS	ENFORCE SIGN-IN REQS.	REVIEW ACCESS	DEPROVISION ACCESS
Azure AD B2B Collaboration	Invite via email, OTP, self-service		Periodic review per partner	Remove account Restrict sign in
Entitlement Management	Add user via assignment or self-service access		Access reviews	Expiration of, or removal from, access package
Office 365 Groups			Review group memberships	Expiration or deletion of group Removal from group
Azure AD security groups		Conditional access policies (Add external users to security groups as necessary)		

Access to resources. **Bolded entries are preferred methods**

FEATURE	APP & RESOURCE ACCESS	SHAREPOINT & ONEDRIVE ACCESS	TEAMS ACCESS	EMAIL & DOCUMENT SECURITY
Entitlement Management	Add user via assignment or self-service access	Access packages	Access packages	
Office 365 Group		Access to site(s) (and associated content) included with group	Access to teams (and associated content) included with group	
Sensitivity labels		Manually and automatically classify and restrict access	Manually and automatically classify and restrict access	Manually and automatically classify and restrict access
Azure AD security groups	Conditional Access policies for access not included in access packages			

Entitlement Management

Entitlement management access packages enable provisioning and deprovisioning access to Groups and Teams, Applications, and SharePoint sites. You can define which connected organizations are allowed access, whether self-service requests are allowed, and what approval workflows are required (if any) to grant access. To ensure that access doesn't stay around longer than necessary, you can define expiration policies and access reviews for each access package.

Govern access with Azure AD P1 and Microsoft / Office 365 E3

You can achieve robust governance with Azure AD P1 and Microsoft 365 E3

Provisioning, signing in, reviewing access, and deprovisioning

FEATURE	PROVISION EXTERNAL USERS	ENFORCE SIGN-IN REQUIREMENTS	REVIEW ACCESS	DEPROVISION ACCESS
Azure AD B2B Collaboration	Invite via email, OTP, self-service	Direct B2B federation	Periodic review per partner	Remove account Restrict sign in
Microsoft or Office 365 Groups				Expiration of or deletion of group. Removal from group.
Security groups		Add external users to security groups (org, team, project, etc.)		
Conditional Access policies		Sign-in Conditional Access policies for external users		

Access to resources.

FEATURE	APP & RESOURCE ACCESS	SHAREPOINT & ONEDRIVE ACCESS	TEAMS ACCESS	EMAIL & DOCUMENT SECURITY
Microsoft or Office 365 Groups		Access to site(s) included with group (and associated content)	Access to teams included with Microsoft 365 group (and associated content)	
Sensitivity labels		Manually classify and restrict access	Manually classify and restrict access.	Manually classify to restrict and encrypt
Conditional Access Policies	Conditional Access policies for access control			
Additional methods		Restrict SharePoint site access granularly with security groups. Disallow direct sharing.	Restrict external invitations from within teams	

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#) (You are here.)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)

7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Securing external access with groups

4/10/2022 • 6 minutes to read • [Edit Online](#)

Groups are an essential part of any access control strategy. Azure Active Directory (Azure AD) security groups and Microsoft 365 Groups can be used as the basis for securing access to resources.

Groups are the best option to use as the basis for the following access control mechanisms:

- Conditional Access policies
- Entitlement Management Access Packages
- Access to Microsoft 365 resources, Microsoft Teams, and SharePoint sites

Groups have the following roles:

- Owners – Group owners manage the group settings and its membership.
- Members – Members who inherit the permissions and access assigned to the group.
- Guests – Guests are members from outside of your organization.

Determine your group strategy

As you develop your group strategy to secure external access to your resources, consider [your desired security posture](#) to determine the following choices.

- **Who should be able to create groups?** Do you want only administrators to create groups, or do you want employees and or external users to also create these groups.
 - *By default any tenant member can create Azure AD security groups.*
 - You can [restrict access to the portal for non-administrators](#) and disable group creation ability in [PowerShell](#).
 - You can also [set up self-service group management in Azure Active Directory](#).
 - *By default all users can create Microsoft 365 Groups and groups are open for all (internal and external) users in your tenant to join.*
 - [You can restrict Microsoft 365 Group creation](#) to the members of a particular security group. Use Windows PowerShell to configure this setting.
- **Who should be able to invite people to groups?** Can all group members be able to add other members, or can only group owners add members?
- **Who can be invited to groups?** By default, external users can be added to groups.

Assign users to groups

Users can be assigned to groups both manually based on the user attributes in their user object, or on other criteria. Users can only be assigned to groups dynamically based on their attributes.

For example, you can assign users to groups based on their:

- specific job title or department
- partner organization to which they belong (manually, or through Connected organizations)

- user type (Member or Guest)
- participation in a specific project (manually)
- location

Dynamic groups can contain either users or devices, but not both. You add queries based on user attributes to assign users into the dynamic group. The below example shows queries that add users to the group if they are members (not guests) and in the finance department.

The screenshot shows the 'Dynamic membership rules' section in the Azure Active Directory portal. It displays a table with two rows of conditions. The first row has 'userType' as the property, 'Equals' as the operator, and 'member' as the value. The second row has 'department' as the property, 'Equals' as the operator, and 'finance' as the value. There are buttons for 'Add expression' and 'Get custom extension properties' at the bottom.

And/Or	Property	Operator	Value
And	userType	Equals	member
	department	Equals	finance

For more information on dynamic groups, see [Create or update a dynamic group in Azure Active Directory](#).

Do not use groups for multiple purposes

When using groups for security or resource access purposes, it's important that they have a single function. If a group is used to grant access to resources, it shouldn't be used for any other purpose. If a group is used for generic purposes such as to define location or team membership, it shouldn't also be used to secure access.

We recommend a naming convention for security groups that makes the purpose clear. For example:

- *Secure_access_finance_apps*
- *Team_membership_finance_team*
- *Location_finance_building*

Types of groups

Both Azure AD security groups and Microsoft 365 groups can be created from the Azure AD portal or the Microsoft 365 admin portal. Both types can be used as the basis for securing external access:

CONSIDERATIONS	AZURE AD SECURITY GROUPS (MANUAL AND DYNAMIC)	MICROSOFT 365 GROUPS
What can the group contain?	Users Groups Service principals Devices	Users only
Where is the group created?	Azure AD portal Microsoft 365 portal (if to be mail enabled) PowerShell Microsoft Graph End user portal	Microsoft 365 portal Azure AD portal PowerShell Microsoft Graph In Microsoft 365 applications
Who creates by default?	Administrators Users	Administrators Users

CONSIDERATIONS	AZURE AD SECURITY GROUPS (MANUAL AND DYNAMIC)	MICROSOFT 365 GROUPS
Who can be added by default?	Internal users (tenant members)	Tenant members and guests from any organization
What does it grant access to?	Only resources to which it's assigned.	All group-related resources: (Group mailbox, site, team, chats, and other included Microsoft 365 resources) Any other resources to which group is added
Can be used with	Conditional Access Entitlement Management Group licensing	Conditional Access Entitlement Management Sensitivity labels

Use Microsoft 365 groups to create and manage a set of Microsoft 365 resources, such as a Team and its associated sites and content. They're a great choice for a project-based effort.

Azure AD security groups

[Azure AD security groups](#) can contain users or devices and can be used to manage access to

- Azure resources such as Microsoft 365 apps, custom apps, and Software as a Service (SaaS) apps such as ServiceNow or Dropbox.
- Azure data and subscriptions.
- Azure services.

Azure AD security groups can also be used to:

- assign licenses for services such as Microsoft 365, Dynamics 365, and Enterprise Mobility and Security. For more information, see [group-based licensing](#).
- assign elevated permissions. For more information, see [Use Azure AD groups to manage role assignments](#).

To create a group [in the Azure portal](#) navigate to Azure Active Directory, then to Groups. You can also create Azure AD security groups by using [PowerShell cmdlets](#).

NOTE

A security group can be used for assignment of up to 1500 applications, but not more.

New Group

Group type *

Security

Microsoft 365

Group name * ⓘ

Finance App - Access Control

Group description ⓘ

used to grant access to tier 1 finance apps

Azure AD roles can be assigned to the group ⓘ

Yes No

Membership type * ⓘ

Assigned

Assigned

Dynamic User

Dynamic Device

Owners

1 owner selected

Members

No members selected

Create

IMPORTANT

To create a mail-enabled security group, go to the [Microsoft 365 Admin center](#). You cannot create it in the Azure AD portal.

You must enable a security group for mail at the time of creation. You can't enable it later.

Hybrid organizations and Azure AD security groups

Hybrid organizations have both an on-premises infrastructure and an Azure AD cloud infrastructure. Many hybrid organizations that use Active Directory create their security groups on-premises and sync them to the cloud. By using this method, only users in the on-premises environment can be added to the security groups.

Protect your on-premises infrastructure from compromise, as a breach on-premises can be used to gain access to your Microsoft 365 tenant. See [Protecting Microsoft 365 from on-premises attacks](#) for guidance.

Microsoft 365 Groups

[Microsoft 365 Groups](#) are the foundational membership service that drives all access across Microsoft 365. They can be created from the [Azure portal](#), or the [Microsoft 365 portal](#). When a Microsoft 365 group is created, you grant access to a group of resources used to collaborate. See [Overview of Microsoft 365 Groups for administrators](#) for a complete listing of these resources.

Microsoft 365 Groups have the following nuances for their roles:

- **Owners** - Group owners can add or remove members and have unique administrative permissions in the group, such as the ability to delete conversations from the shared inbox or change group settings. Group owners can rename the group, update the description or picture and more.
- **Members** - Group members can access everything in the group but can't change group settings. By default, group members can invite guests to join your group. You can [control that setting](#).

- **Guests** - Group guests are members who are from outside your organization. Guests by default have some limits to functionality in Teams.

Microsoft 365 Group settings

You select email alias, privacy, and whether to enable the group for teams at the time of set-up.

Edit settings

Microsoft 365 group
Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars.

Group email address *

Please provide a group email address.

Privacy

Public - Anyone can see group content
 Private - Only members can see group content

Add Microsoft Teams to your group

Create a team for this group

① Some settings like Allow External Senders, or Send Copies of Group Conversations to Members' Inboxes can only be set after the group is created. [Learn more about this setting](#)

After setup, you add members, and configure settings for email usage, etc.

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your desired security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security \(You are here.\)](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Transition to governed collaboration with Azure Active Directory B2B collaboration

4/10/2022 • 9 minutes to read • [Edit Online](#)

Getting your collaboration under control is key to securing external access to your resources. Before going forward with this article, be sure that you have:

- [Determined your security posture](#)
- [Discovered your current state](#)
- [Created a security plan](#)
- [Understood how groups and security work together](#)

Once you've done those things, you're ready to move into controlled collaboration. This article will guide you to move all your external collaboration into [Azure Active Directory B2B collaboration](#) (Azure AD B2B). Azure AD B2B is a feature of [Azure AD External Identities](#).

Control who your organization collaborates with

You must decide whether to limit which organizations your users can collaborate with, and who within your organization can initiate collaboration. Most organizations take the approach of permitting business units to decide with whom they collaborate, and delegating the approval and oversight as needed. For example, some government, education, and financial services organizations don't permit open collaboration. You may wish to use the Azure AD features to scope collaboration, as discussed in the rest of this section.

Determine collaboration partners

First, ensure you've documented the organizations you're currently collaborating with, and the domains for those organizations' users. One collaboration partner may have multiple domains. For example, a partner may have multiple business units with separate domains.

Next, determine if you want to enable future collaboration with

- any domain (most inclusive)
- all domains except those explicitly denied
- only specific domains (most restrictive)

NOTE

The more restrictive your collaboration settings, the more likely that your users will go outside of your approved collaboration framework. We recommend enabling the broadest collaboration your security needs will allow, and closely reviewing that collaboration rather than being overly restrictive.

Also note that limiting to a single domain may inadvertently prevent authorized collaboration with organizations, which have other unrelated domains for their users. For example, if doing business with an organization Contoso, the initial point of contact with Contoso might be one of their US-based employees who has an email with a ".com" domain. However if you only allow the ".com" domain you may inadvertently omit their Canadian employees who have ".ca" domain.

There are circumstances in which you would want to only allow specific collaboration partners. For example, a university system may only want to allow their own faculty access to a resource tenant. Or a conglomerate may only want to allow specific subsidiaries to collaborate with each other to achieve compliance with a required framework.

Using allow and deny lists

You can use an allow list or deny list to [restrict invitations to B2B users](#) from specific organizations. You can use only an allow or a deny list, not both.

- An [allow list](#) limits collaboration to only those domains listed; all other domains are effectively on the deny list.
- A [deny list](#) allows collaboration with any domain not on the deny list.

IMPORTANT

These lists do not apply to users who are already in your directory. They also do not apply to OneDrive for Business and SharePoint allow/deny lists which are separate.

Some organizations use a list of known ‘bad actor’ domains provided by their managed security provider for their deny list. For example, if the organization is legitimately doing business with Contoso and using a .com domain, there may be an unrelated organization that has been using the Contoso .org domain and attempting a phishing attack to impersonate Contoso employees.

Control how external users gain access

There are many ways to collaborate with external partners using Azure AD B2B. To begin collaboration, you invite or otherwise enable your partner to access your resources. Users can gain access by responding to :

- Redeeming [an invitation sent via an email](#), or [a direct link to share](#) a resource.
- Requesting access [through an application](#) you create
- Requesting access through the [My Access](#) portal

When you enable Azure AD B2B, you enable the ability to invite guest users via direct links and email invitations by default. Invitations via Email OTP and a self-service portal are currently in preview and must be enabled within the External Identities | External collaboration settings in the Azure AD portal.

Control who can invite guest users

Determine who can invite guest users to access resources.

- The most restrictive setting is to allow only administrators and those users granted the [guest inviter role](#) to invite guests.
- If your security requirements allow it, we recommend allowing all users with a userType of Member to invite guests.
- Determine if you want users with a userType of Guest, which is the default account type for Azure AD B2B users, to be able to invite other guests.

Guest invite settings

Admins and users in the guest inviter role can invite ⓘ

Yes No

Members can invite ⓘ

Yes No

Guests can invite ⓘ

Yes No

Enable Email One-Time Passcode for guests (Preview) ⓘ

Learn more

Yes No

Enable guest self-service sign up via user flows (Preview) ⓘ

Learn more

Yes No

Collect additional information about external users

If you use Azure AD entitlement management, you can configure questions for external users to answer. The questions will then be shown to approvers to help them make a decision. You can configure different sets of questions for each [access package policy](#) so that approvers can have relevant information for the access they're approving. For example, if one access package is intended for vendor access, then the requestor may be asked for their vendor contract number. A different access package intended for suppliers, may ask for their country of origin.

If you use a self-service portal, you can use [API connectors](#) to collect additional attributes about users as they sign up. You can then potentially use those attributes to assign access. For example, if during the sign-up process you collect their supplier ID, you could use that attribute to dynamically assign them to a group or access package for that supplier. You can create custom attributes in the Azure portal and use them in your self-service sign-up user flows. You can also read and write these attributes by using the [Microsoft Graph API](#).

Troubleshoot invitation redemption to Azure AD users

There are three instances when invited guest users from a collaboration partner using Azure AD will have trouble redeeming an invitation.

- If using an allow list and the user's domain isn't included in an allow list.
- If the collaboration partner's home tenant has tenant restrictions that prevent collaboration with external users..
- If the user isn't part of the partner's Azure AD tenant. For example, there are users at contoso.com who are only in Active Directory (or another on-premises IdP), they'll only be able to redeem invitations via the email OTP process. for more information, see the [invitation redemption flow](#).

Control what external users can access

Most organizations aren't monolithic. That is, there are some resources that are fine to share with external users, and some you will not want external users to access. Therefore, you must control what external users access. Consider using [Entitlement management and access packages to control access](#) to specific resources.

By default, guest users can see information and attributes about tenant members and other partners, including group memberships. Consider if your security requirements call for limiting external user access to this information.

External collaboration settings

 Save  Discard

Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

We recommend the following restrictions for guest users.

- **Limit guest access to browsing groups and other properties in the directory**
 - Use the external collaboration settings to restrict guest ability to read groups they aren't members of.
- **Block access to employee-only apps.**
 - Create a Conditional Access policy to block access to Azure AD-integrated applications that are only appropriate for non-guest users.
- **Block access to the Azure portal. You can make rare necessary exceptions.**
 - Create a Conditional Access policy that includes either All guest and external users and then [implement a policy to block access](#).

Remove users who no longer need access

Evaluate current access so that you can [review and remove users who no longer need access](#). Include external users in your tenant as guests, and those with member accounts.

Some organizations added external users such as vendors, partners, and contractors as members. These members may have a specific attribute, or usernames that begin with, for example

- v- for vendors
- p- for partners
- c- for contractors

Evaluate any external users with member accounts to determine if they still need access. If so, transition these users to Azure AD B2B as described in the next section.

You may also have guest users who weren't invited through Entitlement Management or Azure AD B2B

To find these users, you can:

- [Find guest users not invited through Entitlement Management](#).
 - We provide a [SAMPLE PowerShell script](#).

Transition these users to Azure AD B2B users as described in the following section.

Transition your current external users to B2B

If you haven't been using Azure AD B2B, you likely have non-employee users in your tenant. We recommend you transition these accounts to Azure AD B2B external user accounts and then change their UserType to Guest. This enables you to take advantage of the many ways Azure AD and Microsoft 365 allow you to treat external

users differently. Some of these ways include:

- Easily including or excluding guest users in Conditional Access policies
- Easily including or excluding guest users in Access Packages and Access Reviews
- Easily including or excluding external access to Teams, SharePoint, and other resources.

To transition these internal users while maintaining their current access, UPN, and group memberships, see [Invite external users to B2B collaboration](#).

Decommission undesired collaboration methods

To complete your transition to governed collaboration, you should decommission undesired collaboration methods. Which you decommission is based on the degree of control you wish IT to exert over collaboration, and your security posture. For information about IT versus end-user control, see [Determine your security posture for external access](#).

The following are collaboration vehicles you may wish to evaluate.

Direct invitation through Microsoft Teams

By default Teams allows external access, which means that organization can communicate with all external domains. If you want to restrict or allow specific domains just for Teams, you can do so in the [Teams Admin portal](#).

Direct sharing through SharePoint and OneDrive

Direct sharing through SharePoint and OneDrive can add users outside of the Entitlement Management process. For an in-depth look at these configurations see [Manage Access with Microsoft Teams, SharePoint, and OneDrive for business](#). You can also [block the use of user's personal OneDrive](#) if desired.

Sending documents through email

Your users will send documents through email to external users. Consider how you want to restrict and encrypt access to these documents by using sensitivity labels. For more information, see [Manage access with Sensitivity labels](#).

Unsanctioned collaboration tools

The landscape of collaboration tools is vast. Your users likely use many outside of their official duties, including platforms like Google Docs, DropBox, Slack, or Zoom. It's possible to block the use of such tools from a corporate network at the Firewall level and with mobile application management for organization-managed devices. However, this will also block any sanctioned instances of these platforms and wouldn't block access from unmanaged devices. Block platforms you don't want any use of if necessary, and create business policies for no unsanctioned usage for the platforms you need to use.

For more information on managing unsanctioned applications, see:

- [Governing connected apps](#)
- [Sanctioning and unsanctioning an application](#).

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)

4. [Use groups for security](#)
5. [Transition to Azure AD B2B \(You are here.\)](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Manage external access with Entitlement Management

4/10/2022 • 4 minutes to read • [Edit Online](#)

Entitlement management is an identity governance capability that enables organizations to manage identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration. Entitlement management allows delegated non-admins to create [access packages](#) that external users from other organizations can request access to. One and multi-stage approval workflows can be configured to evaluate requests, and [provision](#) users for time-limited access with recurring reviews. Entitlement management enables policy-based provisioning and deprovisioning of external accounts.

Key concepts for enabling Entitlement Management

The following key concepts are important to understand for entitlement management.

Access Packages

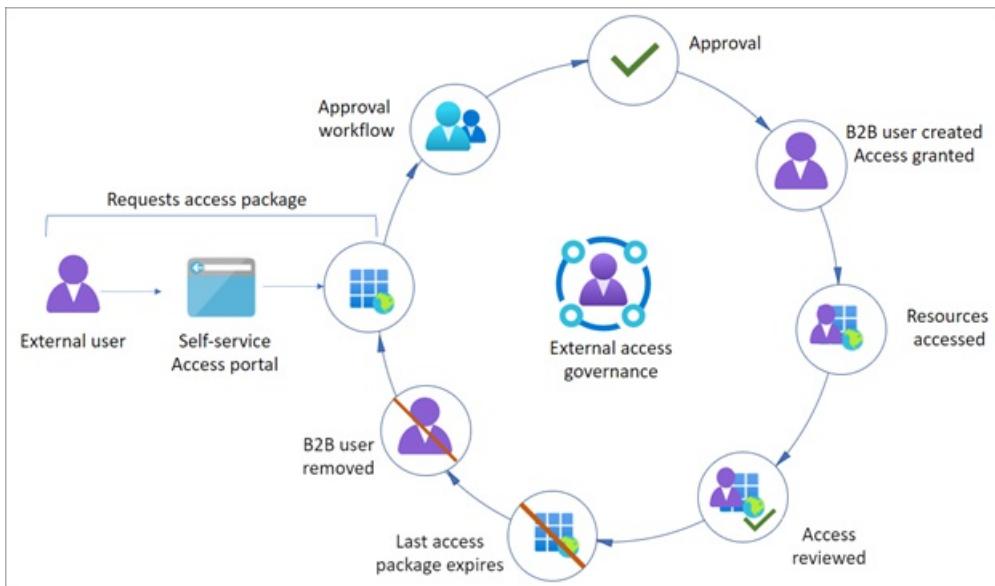
An [access package](#) is the foundation of entitlement management. Access packages are groupings of policy-governed resources a user needs to collaborate on a project or do other tasks. For example, an access package might include:

- access to specific SharePoint sites.
- enterprise applications including your custom in-house and SaaS apps like Salesforce.
- Microsoft Teams.
- Microsoft 365 Groups.

Catalogs

Access packages reside in [catalogs](#). You create a catalog when you want to group related resources and access packages and delegate the ability to manage them. First you add resources to a catalog, and then you can add those resources to access packages. For example, you might want to create a "Finance" catalog, and [delegate its management](#) to a member of the finance team. That person can then [add resources](#), create access packages, and manage access approval to those packages.

The following diagram shows a typical governance lifecycle for an external user gaining access to an access package that has an expiration.



Self-service external access

You can surface access packages through the [Azure AD My Access Portal](#) to enable external users to request access. Policies determine who can request an access package. You specify who is allowed to request the access package:

- Specific [connected organizations](#)
- All configured connected organizations
- All users from any organization
- Member or guest users already in your tenant

Approvals

Access packages can include mandatory approval for access. **Always implement approval processes for external users.** Approvals can be a single or multi-stage approval. Approvals are determined by policies. If both internal and external users need to access the same package, you'll likely set up different access policies for different categories of connected organizations, and for internal users.

Expiration

Access packages can include an expiration date. Expiration can be set to a specific day or give the user a specific number of days for access. When the access package expires, and the user has no other access, the B2B guest user object representing the user can be deleted or blocked from signing in. We recommend that you enforce expiration on access packages for external users. Not all access packages have expirations. For those that don't, ensure that you perform access reviews.

Access reviews

Access packages can require periodic [access reviews](#), which require the package owner or a designee to attest to the continued need for users' access.

Before you set up your review, determine the following.

- Who
 - What are the criteria for continued access?
 - Who are the specified reviewers?
- How often should scheduled reviews occur?
 - Built in options include monthly, quarterly, bi-annually or annually.

- We recommend quarterly or more frequently for packages that support external access.

IMPORTANT

Access reviews of access packages only review access granted through Entitlement Management. You must therefore set up other processes to review any access provided to external users outside of Entitlement Management.

For more information about access reviews, see [Planning an Azure AD Access Reviews deployment](#).

Using automation in Entitlement Management

You can perform [Entitlement Management functions by using Microsoft Graph](#), including

- [Manage access packages](#)
- [Manage access reviews](#)
- [Manage connected organizations](#)
- [Manage Entitlement Management settings](#)

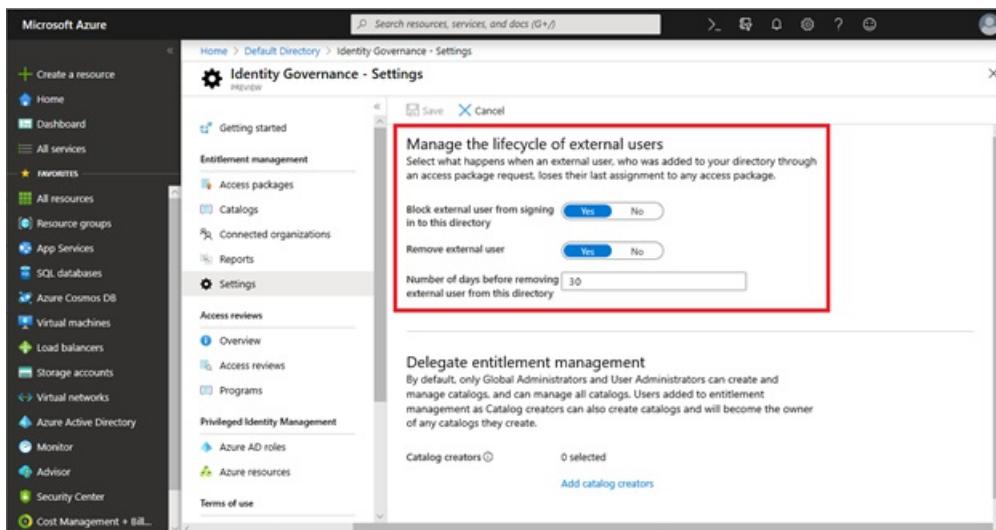
Recommendations

We recommend the practices to govern external access with Entitlement Management.

For projects with one or more business partners, [Create and use access packages](#) to onboard and provision those partner's users access to resources.

- If you already have B2B users in your directory, you can also directly assign them to the appropriate access packages.
- You can assign access in the [Azure portal](#), or via [Microsoft Graph](#).

Use your Identity Governance settings to remove users from your directory when their access packages expire.



These settings only apply to users who were onboarded through Entitlement Management.

Delegate management of catalogs and access packages to business owners, who have more information on who should access.

Finance Team Catalog | Roles and administrators

Catalog

Overview

Add owner Add reader Add access package manager Add access package assignment manager Column Remove Refresh

Manage

Resources Access packages Roles and administrators

Type All Role All

Search by name

Name	UPN	Type	Role	Added by
Finance Team	FinanceTeam@Contoso.com	Group	Access package man...	...

Enforce expiration of access packages to which external users have access.

Expiration

Access package assignments expire ⓘ On date Number of days Never

Assignments expire after 365

[Hide advanced expiration settings](#)

Allow users to extend access * ⓘ Yes No

Require approval to grant extension * ⓘ Yes No

- If you know the end date of a project-based access package, use the On Date to set the specific date.
- Otherwise we recommend the expiration be no longer 365 days, unless it is known to be a multi-year engagement.
- Allow users to extend access.
- Require approval to grant the extension.

Enforce access reviews of packages to avoid inappropriate access for guests.

New access package

* Basics Resource roles * Requests Requestor information (Preview) * Lifecycle

Expiration

Access package assignments expire ⓘ On date Number of days Never

Assignments expire after

[Show advanced expiration settings](#)

Access Reviews

Require access reviews * Yes No

Starting on ⓘ

Review frequency ⓘ Annually Bi-annually Quarterly Monthly

Duration (in days) ⓘ Maximum 80

Reviewers ⓘ Self-review Specific reviewer(s)

- Enforce reviews quarterly.
- For compliance-sensitive projects, set the reviewers to be specific reviewers, rather than self-review for external users. The users who are access package managers are a good place to start for reviewers.
- For less sensitive projects, having the users self-review will reduce the burden on the organization to remove access from users who are no longer with their home organization.

For more information, see [Govern access for external users in Azure AD Entitlement Management](#)

Next steps

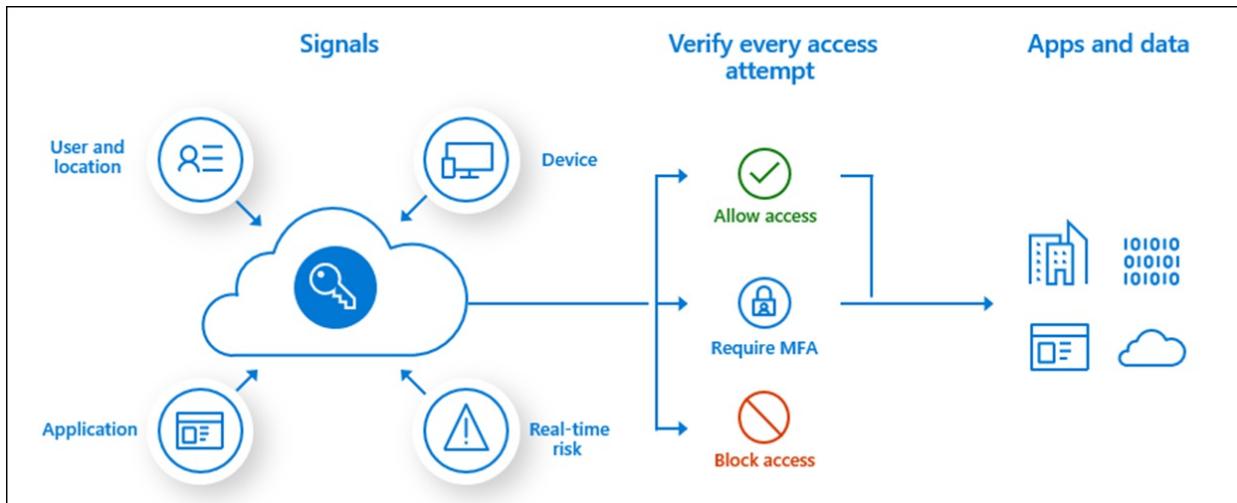
See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#) (You are here.)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Manage external access with Conditional Access policies

4/10/2022 • 4 minutes to read • [Edit Online](#)

Conditional Access is the tool Azure AD uses to bring together signals, enforce policies, and determine whether a user should be allowed access to resources. For detailed information on how to create and use Conditional Access policies (Conditional Access policies), see [Plan a Conditional Access deployment](#).



This article discusses applying Conditional Access policies to external users and assumes you don't have access to [Entitlement Management](#) functionality. Conditional Access policies can be and are used alongside Entitlement Management.

Earlier in this document set, you [created a security plan](#) that outlined:

- Applications and resources have the same security requirements and can be grouped for access.
- Sign-in requirements for external users.

You'll use that plan to create your Conditional Access policies for external access.

IMPORTANT

Create several internal and external user test accounts so that you can test the policies you create before applying them.

Conditional Access policies for external access

The following are best practices related to governing external access with Conditional Access policies.

- If you can't use connected organizations in Entitlement Management, create an Azure AD security group or Microsoft 365 group for each partner organization you work with. Assign all users from that partner to the group. You may then use those groups in Conditional Access policies.
- Create as few Conditional Access policies as possible. For applications that have the same access needs, add them all to the same policy.

NOTE

Conditional Access policies can apply to a maximum of 250 applications. If more than 250 Apps have the same access needs, create duplicate policies. Policy A will apply to apps 1-250, policy B will apply to apps 251-500, etc.

- Clearly name policies specific to external access with a naming convention. One naming convention is *ExternalAccess_actiontaken_AppGroup*. For example a policy for external access that blocks access to finance apps, called ExternalAccess_Block_FinanceApps.

Block all external users from resources

You can block external users from accessing specific sets of resources with Conditional Access policies. Once you've determined the set of resources to which you want to block access, create a policy.

To create a policy that blocks access for external users to a set of applications:

1. Sign in to the **Azure portal** as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to **Azure Active Directory > Security > Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies, for example ExternalAccess_Block_FinanceApps.
5. Under **Assignments**, select **Users and groups**.
 - a. Under **Include**, select **All guests and external users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's [emergency access or break-glass accounts](#).
 - c. Select **Done**.
6. Under **Cloud apps or actions > Include**, select **All cloud apps**.
 - a. Under **Exclude**, select any applications that shouldn't be blocked.
7. Under **Access controls > Grant**, select **Block access**, and choose **Select**.
8. Confirm your settings and set **Enable policy to Report-only**.
9. Select **Create** to create to enable your policy.

After confirming your settings using [report-only mode](#), an administrator can move the **Enable policy** toggle from **Report-only** to **On**.

Block external access to all except specific external users

There may be times you want to block external users except a specific group. For example, you may want to block all external users except those working for the finance team from the finance applications. To do this [Create a security group](#) to contain the external users who should access the finance applications:

1. Sign in to the **Azure portal** as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to **Azure Active Directory > Security > Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies, for example ExternalAccess_Block_AllButFinance.
5. Under **Assignments**, select **Users and groups**.
 - a. Under **Include**, select **All guests and external users**.
 - b. Under **Exclude**, select **Users and groups**,
 - a. Choose your organization's [emergency access or break-glass accounts](#).

- b. Choose the security group of external users you want to exclude from being blocked from specific applications.
 - c. Select **Done**.
6. Under **Cloud apps or actions > Include**, select **All cloud apps**.
 - a. Under **Exclude**, select the finance applications that shouldn't be blocked.
7. Under **Access controls > Grant**, select **Block access**, and choose **Select**.
8. Confirm your settings and set **Enable policy to Report-only**.
9. Select **Create** to create to enable your policy.

After confirming your settings using [report-only mode](#), an administrator can move the **Enable policy** toggle from **Report-only** to **On**.

Implement Conditional Access

Many common Conditional Access policies are documented. See the article [Common Conditional Access policies](#) for other common policies you may want to adapt for external users.

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your desired security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#) (You're here)
8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Control access with sensitivity labels

4/10/2022 • 5 minutes to read • [Edit Online](#)

Sensitivity labels help you control access to your content in Office 365 applications, and in containers like Microsoft Teams, Microsoft 365 Groups, and SharePoint sites. They can protect your content without hindering your users' collaboration and production abilities. Sensitivity labels allow you to send your organization's content across devices, apps, and services, while protecting your data and meeting your compliance and security policies.

With sensitivity labels you can:

- **Classify content without adding any protection settings.** You can assign a classification to content (like a sticker) that persists and roams with your content as it's used and shared. You can use this classification to generate usage reports and see activity data for your sensitive content.
- **Enforce protection settings such as encryption, watermarks, and access restrictions.** For example, users can apply a Confidential label to a document or email, and that label can [encrypt the content](#) and add a "Confidential" watermark. In addition, you can [apply a sensitivity label to a container](#) like a SharePoint site, and enforce whether external users can access the content it contains.

Sensitivity labels on email and other content travel with the content. Sensitivity labels on containers can restrict access to the container, but content in the container doesn't inherit the label. For example, a user could take content from a protected site, download it, and then share it without restrictions unless the content also had a sensitivity label.

NOTE

To apply sensitivity labels users must be signed into their Microsoft work or school account.

Permissions necessary to create and manage sensitivity levels

Members of your compliance team who will create sensitivity labels need permissions to the Microsoft 365 Defender portal, Microsoft 365 Compliance Center, or Office 365 Security & Compliance Center.

By default, global administrators for your tenant have access to these admin centers and can give compliance officers and other people access, without giving them all the permissions of a tenant admin. For this delegated limited admin access, add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group.

Determine your sensitivity label strategy

As you think about governing external access to your content, determine the following:

For all content and containers

- How will you define what is High, Medium, or Low Business Impact (HBI, MBI, LBI)? Consider the impact to your organization if specific types of content are shared inappropriately.
 - Content with specific types of inherently [sensitive content](#), such as credit cards or passport numbers
 - Content created by specific groups or people (for example, compliance officers, financial officers,

or executives)

- Content in specific libraries or sites. For example, containers hosting organizational strategy or private financial data
- Other criteria
- What categories of content (for example HBI content) should be restricted from access by external users?
 - Restrictions can include actions like restricting access to containers, and encrypting content.
- What defaults should be in place for HBI data, sites, or Microsoft 365 Groups?
- Where will you use sensitivity labels to [label and monitor](#), versus to [enforce encryption](#) or to [enforce container access restrictions](#)?

For email and content

- Do you want to [automatically apply sensitivity labels](#) to content, or do so manually?
 - If you choose to do so manually, do you want to [recommend that users apply a label](#)?

For containers

- What criteria will determine if M365 Groups, Teams, or SharePoint sites require access to be restricted by using sensitivity labels?
- Do you want to only label content in these containers moving forward, or do you want to [automatically label](#) existing files in SharePoint and OneDrive?

See these [common scenarios for sensitivity labels](#) for other ideas on how you can use sensitivity labels.

Sensitivity labels on email and content

When you assign a sensitivity label to a document or email, it's like a stamp that's applied to content that is customizable, clear text, and persistent.

- **Customizable** means you can create labels appropriate for your organization and determine what happens when they're applied.
- **Clear text** means it's a part of the item's metadata and is readable by applications and services so that they can apply their own protective actions.
- **Persistent** means the label and any associated protections roam with the content, and become the basis for applying and enforcing policies.

NOTE

Each item of content can have a single sensitivity label applied to it.

Sensitivity labels on containers

You can apply sensitivity labels on containers such as [Microsoft 365 Groups](#), [Microsoft Teams](#), and [SharePoint sites](#). When you apply this sensitivity label to a supported container, the label automatically applies the classification and protection settings to the connected site or group. Sensitivity labels on these containers can control the following aspects of containers:

- **Privacy**. You can choose who can see the site: specific users, all internal users, or anyone.
- **External user access**. Controls whether the group owner can add guests to the group.
- **Access from unmanaged devices**. Determines if and how unmanaged devices can access content.

Edit sensitivity label

The screenshot shows a navigation sidebar on the left with the following items:

- Name & description (checked)
- Encryption (checked)
- Content marking (checked)
- Site and group settings (selected)
- Auto-labeling for Office apps
- Review your settings

The main content area is titled "Site and group settings". It contains the following sections:

- Site and group settings**: A toggle switch is turned on.
- Privacy of Office 365 group-connected team sites**: A dropdown menu set to "Public - anyone in the organization can access the site".
- External users access**: An unchecked checkbox for "Let Office 365 group owners add people outside the organization to the group".
- Unmanaged devices**: Three radio button options:
 - Allow full access from desktop apps, mobile apps, and the web
 - Allow limited, web only access
 - Block access (selected)

When you apply a sensitivity label to a container such as a SharePoint site, it is not applied to content there: sensitivity labels on containers control access to the content within the container.

- If you want to automatically apply labels to the content within the container, see [Apply a sensitivity to content automatically](#).
- If you want users to be able to manually apply labels to this content, be sure that you've [enabled sensitivity labels for Office files in SharePoint and OneDrive](#).

Plan to implement sensitivity labels

Once you have determined how you want to use sensitivity labels, and to what content and sites you want to apply them, see the following documentation to help you perform your implementation.

1. [Get started with sensitivity labels](#)
2. [Create a deployment strategy](#)
3. [Create and publish sensitivity labels](#)
4. [Restrict access to content using sensitivity labels to apply encryption](#)
5. [Use sensitivity labels with teams, groups, and sites](#)
6. [Enable sensitivity labels for Office files in SharePoint and OneDrive](#)

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your desired security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)

6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)
8. [Secure access with Sensitivity labels](#) (You are here.)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#)

Secure external access to Microsoft Teams, SharePoint, and OneDrive for Business

4/10/2022 • 7 minutes to read • [Edit Online](#)

Microsoft Teams, SharePoint, and OneDrive for Business are three of the most used ways to collaborate and share content with external users. If the “approved” methods are too restrictive, users will go outside of approved methods by emailing content or setting up insecure external processes and applications, such as a personal DropBox or OneDrive. Your goal is to balance your security needs with ease of collaboration.

This article guides you to determine and configure external collaboration to meet your business goals using Microsoft Teams and SharePoint.

Governance begins in Azure Active Directory

Sharing in Microsoft 365 is in part governed by the [External Identities | External collaboration settings](#) in Azure Active Directory (Azure AD). If external sharing is disabled or restricted in Azure AD, it overrides any sharing settings configured in Microsoft 365. An exception to this is that if Azure AD B2B integration isn't enabled, SharePoint and OneDrive can be configured to support ad-hoc sharing via one-time passcodes (OTP).

The screenshot shows the Azure Active Directory admin center interface. The left sidebar has a tree view with 'All services > Contoso > External Identities'. The main content area is titled 'External Identities | External collaboration settings' under 'Contoso - Azure Active Directory'. It includes sections for 'Guest user access', 'Guest invite settings', and 'Enable Email One-Time Passcode for guests (Preview)'. Each section has radio button options and 'Yes' or 'No' buttons for configuration.

Guest user access

There are three choices for guest user access, which controls what guest users can see after being invited.

To prevent guest users from seeing details of other guest users, and being able to enumerate group membership, choose Guest users have limited access to properties and memberships of directory objects.

Guest invite settings

These settings determine who can invite guests and how those guests can be invited. These settings are only enabled if the integration with B2B is enabled.

We recommend enabling administrators and users in the guest inviter role can invite. This setting allows

controlled collaboration processes to be set up, as in the following example.

- Team owner submits a ticket to be assigned the Guest inviter role, and
 - Becomes responsible for all guest invitations.
 - Agrees not to directly add users to the underlying SharePoint
 - Is accountable to perform regular access reviews, and revoke access as appropriate.
- Central IT does the following
 - Enables external sharing by granting the requested role upon training completion.
 - Assigns Azure AD P2 license to the Microsoft 365 group owner to enable access reviews.
 - Creates a Microsoft 365 group access review.
 - Confirms that access reviews are occurring.
 - Removes users directly added to the underlying SharePoint.

Set **Enable Email One-time Passcodes for guests (Preview)** and **Enable up guest self-service sign via user flows** to yes. This setting takes advantage of the integration with Azure AD External collaboration settings.

Collaboration restrictions

There are three choices under collaboration restrictions. Your business requirements dictate which you will choose.

- **Allow invitations to be sent to any domain** means any user can be invited to collaborate.
- **Deny invitations to the specified domains** means any user outside of those can be invited to collaborate.
- **Allow invitations only to the specified domains** means that any user outside of those specified domains cannot be invited.

Govern access in Teams

Teams differentiates between external users (anyone outside your organization) and guest users (those with guest accounts). You manage collaboration setting in the [Teams Admin portal](#) under Org-wide settings.

NOTE

External identities collaboration settings in Azure Active Directory control the effective permissions. You can increase restrictions in Teams, but not decrease them from what is set in Azure AD.

- **External Access settings.** By default, Teams allows external access, which means that organization can communicate with all external domains. If you want to restrict or allow specific domains just for Teams, you can do so here.
- **Guest Access.** Guest access controls what guest users can do in teams.

To learn more about managing external access in Teams, see the following resources.

- [Manage external access in Microsoft Teams](#)
- [Microsoft 365 identity models and Azure Active Directory](#)
- [Identity models and authentication for Microsoft Teams](#)

- Sensitivity labels for Microsoft Teams

Govern access in SharePoint and OneDrive

SharePoint administrators have many settings available for collaboration. Organization-wide settings are managed from the SharePoint admin center. Settings can be adjusted for each SharePoint site. We recommend that your organization-wide settings be at your minimum necessary security levels, and that you increase security on specific sites as needed. For example, for a high-risk project, you may want to restrict users to certain domains, and disable the ability of members to invite guests.

Integrating SharePoint and One-drive with Azure AD B2B

As a part of your overall strategy for governing external collaboration, we recommend that you [enable the Preview of SharePoint and OneDrive integration with Azure AD B2B](#).

Azure AD B2B provides authentication and management of guest users. With SharePoint and OneDrive integration, [Azure AD B2B one-time passcodes](#) are used for external sharing of files, folders, list items, document libraries, and sites. This feature provides an upgraded experience from the existing [secure external sharing recipient experience](#).

NOTE

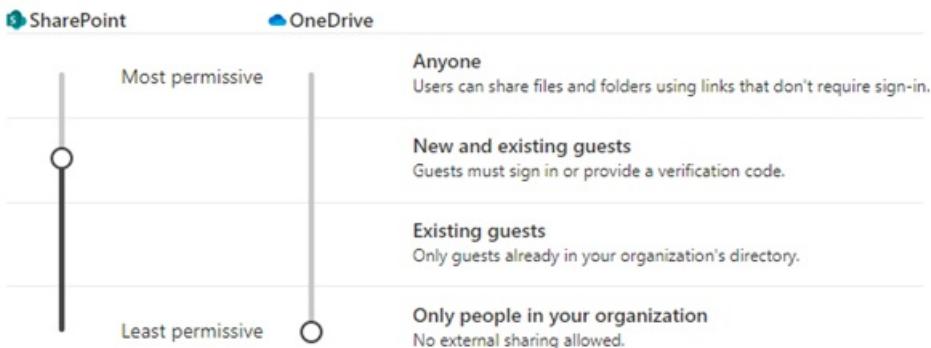
If you enable the preview for Azure AD B2B integration, then SharePoint and OneDrive sharing is subject to the Azure AD organizational relationships settings, such as **Members can invite** and **Guests can invite**.

Sharing policies

External Sharing can be set for both SharePoint and OneDrive. OneDrive restrictions can't be more permissive than the SharePoint settings.

External sharing

Content can be shared with:



You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings ▾

- Limit external sharing by domain
- Allow only users in specific security groups to share externally

[Manage security groups](#)

- Guests must sign in using the same account to which sharing invitations are sent
- Allow guests to share items they don't own
- People who use a verification code must reauthenticate after this many days

SharePoint integration with Azure AD B2B changes how controls interact with accounts.

- **Anyone.** Not recommended
 - Regardless of integration status, enabling Anyone links means no Azure policies will be applied when this type of link is used.
 - In a scenario of governed collaboration, don't enable this functionality.
- NOTE**

You may find a scenario where you need to enable this setting for a specific site, in which case you would enable it here, and set the greater restriction on individual sites.
- **New and existing guests.** Recommended if you have integration enabled.
 - **With Azure AD B2B integration** enabled, new and existing guests will have an Azure AD B2B guest account that can be managed with Azure AD policies.
 - **Without Azure AD B2B integration** enabled, new guests will not have an Azure AD B2B account created, and they cannot be managed from Azure AD. Whether existing guests have an Azure AD B2B account depends on how the guest was created.
- **Existing guests.** Recommended if you do not have integration enabled.
 - With this enabled, users can only share with other users already in your directory.
- **Only people in your organization.** Not recommended when you need to collaborate with external users.
 - Regardless of integration status, users will only be able to share with users in your organization.
- **Limit external sharing by domain.** By default SharePoint allows external access, which means that sharing is allowed with all external domains. If you want to restrict or allow specific domains just for SharePoint, you can do so here.
- **Allow only users in specific security groups to share externally.** This setting restricts who can share content in SharePoint and OneDrive, while the setting in Azure AD applies to all applications. Restricting who can share can be useful if you want to require your users to take a training about sharing securely, then at completion add them to an approved sharing security group. If this setting is selected, and users do not have a way to gain access to being an "approved sharer," they may instead find unapproved ways to share.
- **Allow guests to share items they don't own.** We recommend leaving this disabled.
- **People who use a verification code must reauthenticate after this many days (default is 30).** We recommend enabling this setting.

Access controls

Access controls setting will affect all users in your organization. Given that you may not be able to control whether external users have compliant devices, we will not address those controls here.

- **Idle session sign-out.** We recommend that you enable this control, which allows you to warn and sign-out users on unmanaged devices after a period of inactivity. You can configure the period of inactivity and the warning.
- **Network location.** Setting this control means you can allow access only from IP addresses that your organization owns. In external collaboration scenarios, set this only if all of your external partners will access resources only from within your network, or via your VPN.

File and folder links

In the SharePoint admin center, you can also set how file and folder links are shared. You can also configure these setting for each site.

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

Specific people (only the people the user specifies)
 Only people in your organization
 Anyone with the link

Choose the permission that's selected by default for sharing links.

View
 Edit

Choose expiration and permissions options for Anyone links.

These links must expire within this many days

These links can give these permissions:

Files:

Folders:

If you have enabled the integration with Azure AD B2B, sharing of files and folders with those outside of the organization will result in a B2B user being created when files and folder are shared.

We recommend setting the default link type to **Only people in your organization**, and default permissions to **Edit**. Doing so ensures that items are shared thoughtfully. You can then customize this setting for per-site default that meet specific collaboration needs.

Anyone links

We do not recommend enabling anyone links. If you do, we recommend setting an expiration, and consider restricting them to view permissions. If you choose View only permissions for files or folders, users will not be able to change Anyone links to include edit privileges.

To learn more about governing external access to SharePoint see the following:

- [SharePoint external sharing overview](#)
- [SharePoint and OneDrive integration with Azure AD B2B](#)

Next steps

See the following articles on securing external access to resources. We recommend you take the actions in the listed order.

1. [Determine your security posture for external access](#)
2. [Discover your current state](#)
3. [Create a governance plan](#)
4. [Use groups for security](#)
5. [Transition to Azure AD B2B](#)
6. [Secure access with Entitlement Management](#)
7. [Secure access with Conditional Access policies](#)

8. [Secure access with Sensitivity labels](#)
9. [Secure access to Microsoft Teams, OneDrive, and SharePoint](#) (You are here.)

Introduction to securing Azure service accounts

4/10/2022 • 2 minutes to read • [Edit Online](#)

There are three types of service accounts native to Azure Active Directory: Managed identities, service principals, and user-based service accounts. Service accounts are a special type of account that is intended to represent a non-human entity such as an application, API, or other service. These entities operate within the security context provided by the service account.

Types of Azure Active Directory service accounts

For services hosted in Azure, we recommend using a managed identity if possible, and a service principal if not. Managed identities can't be used for services hosted outside of Azure. In that case, we recommend a service principal. If you can use a managed identity or a service principal, do so. We recommend that you not use an Azure Active Directory user account as a service account. See the following table for a summary.

SERVICE HOSTING	MANAGED IDENTITY	SERVICE PRINCIPAL	AZURE USER ACCOUNT
Service is hosted in Azure.	Yes. Recommended if the service supports a Managed Identity.	Yes.	Not recommended.
Service is not hosted in Azure.	No	Yes. Recommended.	Not recommended.
Service is multi-tenant	No	Yes. Recommended.	No.

Managed identities

Managed identities are secure Azure Active Directory (Azure AD) identities created to provide identities for Azure resources. There are [two types of managed identities](#):

- System-assigned managed identities can be assigned directly to an instance of a service.
- User-assigned managed identities can be created as a standalone resource.

For more information, see [Securing managed identities](#). For general information about managed identities, see [What are managed identities for Azure resources?](#)

Service principals

If you can't use a managed identity to represent your application, use a service principal. Service principals can be used with both single tenant and multi-tenant applications.

A service principal is the local representation of an application object in a single Azure AD tenant. It functions as the identity of the application instance, defines who can access the application, and what resources the application can access. A service principal is created in (local to) each tenant where the application is used and references the globally unique application object. The tenant secures the service principal's sign-in and access to resources.

There are two mechanisms for authentication using service principals—client certificates and client secrets. Certificates are more secure: use client certificates if possible. Unlike client secrets, client certificates cannot

accidentally be embedded in code.

For information on securing service principals, see [Securing service principals](#).

Next steps

For more information on securing Azure service accounts, see:

[Securing managed identities](#)

[Securing service principals](#)

[Governing Azure service accounts](#)

Securing managed identities

4/10/2022 • 4 minutes to read • [Edit Online](#)

Developers are often challenged by the management of secrets and credentials used to secure communication between different services. Managed identities are secure Azure Active Directory (Azure AD) identities created to provide identities for Azure resources.

Benefits of using managed identities for Azure resources

The following are benefits of using managed identities:

- You don't need to manage credentials. With managed identities, credentials are fully managed, rotated, and protected by Azure. Identities are automatically provided and deleted with Azure resources. Managed identities enable Azure resources to communicate with all services that support Azure AD authentication.
- No one (including any Global admin) has access to the credentials, so they cannot be accidentally leaked by, for example, being included in code.

When to use managed identities?

Managed identities are best used for communications among services that support Azure AD authentication.

A source system requests access to a target service. Any Azure resource can be a source system. For example, an Azure VM, Azure Function instance, and Azure App Services instances support managed identities.

How authentication and authorization work

With managed identities the source system can obtain a token from Azure AD without the source owner having to manage credentials. Azure manages the credentials. The token obtained by the source system is presented to the target system for authentication.

The target system needs to authenticate (identify) and authorize the source system before allowing access.

When the target service supports Azure AD-based authentication it accepts an access token issued by Azure AD.

Azure has a control plane and a data plane. In the control plane, you create resources, and in the data plane you access them. For example, you create a Cosmos database in the control plane, but query it in the data plane.

Once the target system accepts the token for authentication, it can support different mechanisms for authorization for its control plane and data plane.

All of Azure's control plane operations are managed by [Azure Resource Manager](#) and use [Azure Role Based Access Control](#). In the data plane, each target system has its own authorization mechanism. Azure Storage supports Azure RBAC on the data plane. For example, applications using Azure App Services can read data from Azure Storage, and applications using Azure Kubernetes Service can read secrets stored in Azure Key Vault.

For more information about control and data planes, see [Control plane and data plane operations - Azure Resource Manager](#).

All Azure services will eventually support managed identities. For more information, see [Services that support managed identities for Azure resources](#).

Types of managed identities

There are two types of managed identities—system-assigned and user-assigned.

System-assigned managed identity has the following properties:

- They have 1:1 relationship with the Azure resource. For example, there's a unique managed identity associated with each VM.
- They are tied to the lifecycle of Azure resources. When the resource is deleted, the managed identity associated with it's automatically deleted, eliminating the risk associated with orphaned accounts.

User-assigned managed identities have the following properties:

- The lifecycle of these identities is independent of an Azure resource, and you must manage the lifecycle. When the Azure resource is deleted, the assigned user-assigned managed identity is not automatically deleted for you.
- A single user-assigned managed identity can be assigned to zero or more Azure resources.
- They can be created ahead of time and then assigned to a resource.

Find managed identity service principals in Azure AD

There are several ways in which you can find managed identities:

- Using the Enterprise Applications page in the Azure portal
- Using Microsoft Graph

Using the Azure portal

1. In Azure Active Directory, select Enterprise applications.
2. Select the filter for "Managed Identities"

The screenshot shows the Azure portal interface for managing enterprise applications. The top navigation bar includes 'Enterprise applications - Microsoft' and a search bar. Below the header, the URL is 'portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllApps/menuld/'. The main content area is titled 'Enterprise applications | All applications' under 'Contoso - Azure Active Directory'. On the left, a sidebar menu lists 'Overview', 'Diagnose and solve problems', 'Manage' (with 'All applications' selected), 'Application proxy', 'User settings', and 'Collections'. The main pane displays application filters: 'Application type' set to 'Managed Identities' (which is highlighted with a red box), 'Applications status' set to 'Any', and 'Application visibility' set to 'Any'. There are 'Apply' and 'Reset' buttons. Below the filters, a table lists applications, with one entry 'cmkdemo' visible.

Using Microsoft Graph

You can get a list of all managed identities in your tenant with the following GET request to Microsoft Graph:

```
https://graph.microsoft.com/v1.0/servicePrincipals?$filter=(servicePrincipalType eq 'ManagedIdentity')
```

You can filter these requests. For more information, see the Graph documentation for [GET servicePrincipal](#).

Assess the security of managed identities

You can assess the security of managed identities in the following ways:

- Examine privileges and ensure that the least privileged model is selected. Use the following PowerShell

cmdlet to get the permissions assigned to your managed identities.

```
Get-AzureADServicePrincipal | % { Get-AzureADServiceAppRoleAssignment -ObjectId $_ }
```

- Ensure the managed identity is not part of any privileged groups, such as an administrators group. You can do this by enumerating the members of your highly privileged groups with PowerShell.

```
Get-AzureADGroupMember -ObjectId <String> [-All <Boolean>] [-Top <Int32>] [<CommonParameters>]
```

- Ensure you know what resources the managed identity is accessing.

Move to managed identities

If you are using a service principal or an Azure AD user account, evaluate if you can instead use a managed identity to eliminate the need to protect, rotate, and manage credentials.

Next steps

For information on creating managed identities, see:

[Create a user assigned managed identity](#).

[Enable a system assigned managed identity during resource creation](#)

[Enable system assigned managed identity on an existing resource](#)

For more information on service accounts see:

[Introduction to Azure Active Directory service accounts](#)

[Securing service principals](#)

[Governing Azure service accounts](#)

[Introduction to on-premises service accounts](#)

Securing service principals

4/10/2022 • 4 minutes to read • [Edit Online](#)

An Azure Active Directory (Azure AD) [service principal](#) is the local representation of an application object in a single tenant or directory. It functions as the identity of the application instance. Service principals define who can access the application, and what resources the application can access. A service principal is created in each tenant where the application is used and references the globally unique application object. The tenant secures the service principal's sign in and access to resources.

Tenant-service principal relationships

A single-tenant application has only one service principal in its home tenant. A multi-tenant web application or API requires a service principal in each tenant. A service principal is created when a user from that tenant has consented to the application's or API's use. This consent creates a one-to-many relationship between the multi-tenant application and its associated service principals.

A multi-tenant application is homed in a single tenant and is designed to have instances in other tenants. Most software-as-a-service (SaaS) applications are designed for multi-tenancy. Use service principals to ensure the right security posture for the application and its users in both single tenant and multi-tenant use cases.

ApplicationID and ObjectID

A given application instance has two distinct properties: the ApplicationID (also known as ClientID) and the ObjectID.

NOTE

You may find that the terms application and service principal are used interchangeably when loosely referring to an application in the context of authentication related tasks. However, they are two different representations of applications in Azure AD.

The ApplicationID represents the global application and is the same for all the application instances across tenants. The ObjectID is a unique value for an application object. As with users, groups, and other resources, the ObjectID helps uniquely identify an application instance in Azure AD.

For more detailed information on this topic, see [Application and service principal relationship](#).

You can also create an application and its service principal object (ObjectID) in a tenant using Azure PowerShell, Azure CLI, Microsoft Graph, the Azure portal, and other tools.

New App

Search (Ctrl+ /) Delete Endpoints Preview features

Overview Quickstart Integration assistant | Preview

Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

Display name : New App Application (client) ID : b444371f-11d4-46e9-8219-02a77910
Directory (tenant) ID : 72f988bf-86f1-46c5-84df-607244a8956b
Object ID : b444371f-11d4-46e9-8219-02a77910

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory. We will longer provide feature updates. Applications will need to be upgraded to the latest version.

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API permissions

Service principal authentication

There are two mechanisms for authentication using service principals—client certificates and client secrets.

New App | Certificates & secrets

Search (Ctrl+ /) Got feedback?

Overview Quickstart Integration assistant | Preview

Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value
No client secrets have been created for this application.		

Certificates are more secure: use client certificates if possible. Unlike client secrets, client certificates cannot accidentally be embedded in code. Use Azure Key Vault for certificate and secrets management when possible to

encrypt the following assets by using keys protected by hardware security modules:

- authentication keys
- storage account keys
- data encryption keys
- .pfx files
- passwords

For more information on Azure Key Vault and how to use it for certificate and secret management, see [About Azure Key Vault](#) and [Assign a Key Vault access policy using the Azure portal](#).

Challenges and mitigations

The following table presents mitigations to challenges you may encounter when using service principals.

CHALLENGES	MITIGATIONS
Access reviews for service principals assigned to privileged roles.	This functionality is in preview, and not yet widely available.
Reviews service principals' access	Manual check of resource's access control list using the Azure portal.
Over permissioned service principals	When you create automation service accounts or service principals, provide only the permissions that are required for the task. Evaluate existing service principals to see if you can reduce privileges.
Identify modifications to service principals' credentials or authentication methods	Use the Sensitive Operations Report workbook, which can help mitigate this issue. See the explanation in this blog post .

Find accounts using service principals

Run the following commands to find accounts using service principals.

Using Azure CLI

```
az ad sp list
```

Using PowerShell

```
Get-AzureADServicePrincipal -All:$true
```

For more information see [Get-AzureADServicePrincipal](#)

Assess service principal security

To assess the security of your service principals, ensure you evaluate privileges and credential storage.

Mitigate potential challenges using the following information.

CHALLENGES	MITIGATIONS

CHALLENGES	MITIGATIONS
Detect the user that consented to a multi-tenant app, and detect illicit consent grants to a multi-tenant app	<p>Run the following PowerShell to find multi-tenant apps.</p> <pre>Get-AzureADServicePrincipal -All:\$true ? {\$_.Tags -eq "WindowsAzureActiveDirectoryIntegratedApp"}</pre> <p>Disable user consent. Allow user consent from verified publishers, for selected permissions (recommended) Configure them under the user context, and their tokens should be used to trigger the service principal.</p>
Use of a hard-coded shared secret in a script using a service principal.	Use a certificate or Azure Key Vault.
Tracking who is using the certificate or the secret	Monitor the service principal's sign-ins using the Azure AD sign-in logs.
Can't manage service principals' sign-in with Conditional Access.	Monitor the sign-ins using the Azure AD sign-in logs
The default Azure RBAC role is Contributor.	Evaluate the needs and apply the role with the least possible permissions to meet that need.

Move from a user account to a service principal

If you are using an Azure user account as a service principal, evaluate if you can move to a [Managed Identity](#) or a service principal. If you cannot use a managed identity, provision a service principal that has just enough permissions and scope to run the required tasks. You can create a service principal by [registering an application](#), or with [PowerShell](#).

When using Microsoft Graph, check the documentation of the specific API, [like in this example](#), and make sure the permission type for application is showing as supported.

Next steps

To learn more about service principals:

[Create a service principal](#)

[Monitor service principal sign-ins](#)

To learn more about securing service accounts:

[Introduction to Azure service accounts](#)

[Securing managed identities](#)

[Governing Azure service accounts](#)

[Introduction to on-premises service accounts](#)

Governing Azure AD service accounts

4/10/2022 • 7 minutes to read • [Edit Online](#)

There are three types of service accounts in Azure Active Directory (Azure AD): [managed identities, service principals](#), and user accounts employed as service accounts. As you create these service accounts for automated use, they're granted permissions to access resources in Azure and Azure AD. Resources can include Microsoft 365 services, software as a service (SaaS) applications, custom applications, databases, HR systems, and so on. Governing Azure AD service accounts means that you manage their creation, permissions, and lifecycle to ensure security and continuity.

IMPORTANT

We do not recommend using user accounts as service accounts as they are inherently less secure. This includes on-premises service accounts that are synced to Azure AD, as they are not converted to service principals. Instead, we recommend the use of managed identities or service principals. Note that at this time the use of conditional access policies with service principals is called Conditional Access for workload identities and it's in public preview.

Plan your service account

Before creating a service account, or registering an application, document the service account's key information. Having information documented makes it easier to effectively monitor and govern the account. We recommend collecting the following data and tracking it in your centralized Configuration Management Database (CMDB).

DATA	DESCRIPTION	DETAILS
Owner	User or group that is accountable for managing and monitoring the service account.	Provision the owner with necessary permissions to monitor the account and implement a way to mitigate issues. Issue mitigation may be done by the owner, or via a request to IT.
Purpose	How the account will be used.	Map the service account to a specific service, application, or script. Avoid creating multi-use service accounts.
Permissions (Scopes)	Anticipated set of permissions.	Document the resources it will access and the permissions to those resources.
CMDB Link	Link to the resources to be accessed, and scripts in which the service account is used.	Ensure you document the resource and script owners so that you can communicate any necessary upstream and downstream effects of changes.
Risk assessment	Risk and business impact if the account were to be compromised.	Use this information to narrow the scope of permissions and determine who should have access to the account information.

DATA	DESCRIPTION	DETAILS
Period for review	The schedule on which the service account is to be reviewed by the owner.	Use this to schedule review communications and reviews. Document what should happen if a review is not performed by a specific time after the scheduled review period.
Lifetime	Anticipated maximum lifetime of account.	Use this to schedule communications to the owner, and to ultimately disable then delete the accounts. Where possible, set an expiration date for credentials, where credentials cannot be rolled over automatically.
Name	Standardized name of account	Create a naming schema for all service accounts so that you can easily search, sort, and filter on service accounts.

Use the principle of least privileges

Grant the service account only the permissions necessary to perform its tasks, and no more. If a service account needs high-level permissions, for example a global administrator level of privilege, evaluate why and try to reduce the necessary permissions.

We recommend the following practices for service account privileges.

Permissions

- Do not assign built-in roles to service accounts. Instead, use the [OAuth2 permission grant model for Microsoft Graph](#),
- If the service principal must be assigned a privileged role, consider assigning a [custom role](#) with specific, required privileged, in a time-bound fashion.
- Do not include service accounts as members of any groups with elevated permissions.
- [Use PowerShell to enumerate members of privileged roles](#), such as
`Get-AzureADDirectoryRoleMember`, and filter for objectType "Service Principal".

or use

```
Get-AzureADServicePrincipal | % { Get-AzureADServiceAppRoleAssignment -ObjectId $_ }
```

- [Use OAuth 2.0 scopes](#) to limit the functionality a service account can access on a resource.
- Service principals and managed identities can use OAuth 2.0 scopes in either a delegated context that is impersonating a signed-on user, or as service account in the application context. In the application context no one is signed-on.
- Check the scopes service accounts request for resources to ensure they're appropriate. For example, if an account is requesting Files.ReadWrite.All, evaluate if it actually needs only File.Read.All. For more information on permissions, see to [Microsoft Graph permission reference](#).
- Ensure you trust the developer of the application or API with the access requested to your resources.

Duration

- Limit service account credentials (client secret, certificate) to an anticipated usage period.
- Schedule periodic reviews the use and purpose of service accounts. Ensure reviews are conducted prior

to expiration of the account.

Once you have a clear understanding of the purpose, scope, and necessary permissions, create your service account.

Create and use managed identities

Create and use service principals

Use a managed identity when possible. If you cannot use a managed identity, use a service principal. If you cannot use a service principal, then and only then use an Azure AD user account.

Build a lifecycle process

Managing the lifecycle of a service account starts with planning and ends with its permanent deletion.

This article has previously covered the planning and creation portion. You must also monitor, review permissions, determine an account's continued usage, and ultimately deprovision the account.

Monitor service accounts

Proactively monitor your service accounts to ensure the service account's usage patterns reflects the intended patterns and that the service account is still actively used.

Collect and monitor service account sign-ins using one of the following methods:

- Using the Azure AD Sign-In Logs in the Azure AD Portal.
- Exporting the Azure AD Sign-In Logs to [Azure Storage](#), [Azure Event Hubs](#), or [Azure Monitor](#).

The screenshot shows the Azure AD Sign-In Logs interface. At the top, there are navigation links: Download, Export Data Settings, Troubleshoot, Refresh, Columns, and Got feedback? Below these are filter options: Date (Last 24 hours), Show data as (Local), Time aggregate (1 day), and Add filters. There are four tabs at the top of the main table: User sign-ins (interactive), User sign-ins (non-interactive), Service principal sign-ins (underlined), and Managed identity sign-ins. A note below the tabs says: "Sign-ins in the table below are grouped by application. Click on a row to see all the sign-ins for an application on that date and time." The table has columns: Date, Request ID, Service principal..., Status, IP address, Resource, Resource ID, and # sign ins. Two rows of data are shown:

Date	Request ID	Service principal...	Status	IP address	Resource	Resource ID	# sign ins
> 11.11.2020, 01:00:00	b8018773-b177-42ef...	c8e2afc0-7e18-4b6b-9	Azure AD Domain Se...	52.146.153.190	Microsoft Graph	00000003-0000-000...	17
> 10.11.2020, 01:00:00	8f2548c6-7c3e-4e09...	c8e2afc0-7e18-4b6b-9	Azure AD Domain Se...	52.146.153.190	Microsoft Graph	00000003-0000-000...	9

Intelligence that you should look for in the Sign-In logs includes:

- Are there service accounts that no longer sign in to the tenant?
- Are sign-in patterns of service accounts changing?

We recommend you export Azure AD sign-In logs and import them into your existing Security Information and Event Management (SIEM) tools such as Microsoft Sentinel. Use your SIEM to build alerting and dashboards.

Review service account permissions

Regularly review the permissions granted and scopes accessed by service accounts to see if they can be reduced or eliminated.

- Use [PowerShell](#) to [build automation for checking and documenting](#) scopes to which consent is granted to a service account.
- Use PowerShell to [review existing service principals' credentials](#) and check their validity.
- Do not set service principal's credentials to "Never expire".
- Use certificates or credentials stored in Azure KeyVault where possible.

Microsoft's free PowerShell sample collects service principal's OAuth2 grants and credential information, records them in a comma-separated values file (CSV), and a Power BI sample dashboard to interpret and use the data. for more information, see [AzureAD/AzureADAssessment: Tooling for assessing an Azure AD tenant state and configuration \(github.com\)](#)

Recertify service account use

Establish a review process to ensure that service accounts are regularly reviewed by their owners and the security or IT team at regular intervals.

The process should include:

- How to determine each service accounts' review cycle (should be documented in your CMDB).
- The communications to owner and security or IT teams before reviews start.
- The timing and content of warning communications if the review is missed.
- Instructions on what to do if the owners fail to review or respond. For example, you may want to disable (but not delete) the account until the review is complete.
- Instructions on determining upstream and downstream dependencies and notifying other resource owners of any effects.

The review should include the owner and their IT partner certifying that:

- The account is still necessary.
- The permissions granted to the account are adequate and necessary, or a change is requested.
- The access to the account and its credentials is controlled.
- The credentials the account uses are appropriate, in respect to the risk the account was assessed with (both credential type and credential lifetime)
- The account's risk scoring hasn't changed since the last recertification
- An update on the expected lifetime of the account, and the next recertification date.

Deprovision service accounts

Deprovision service accounts under the following circumstances:**

- The script or application the service account was created for is retired.
- The function within the script or application the service account is used for (for example, access to a specific resource) is retired.
- The service account is replaced with a different service account.
- The credentials expired, or the account is otherwise non-functional, and there aren't any complaints.

The processes for deprovisioning should include the following tasks.

1. Once the associated application or script is deprovisioned, [monitor sign-ins](#) and resource access by the service account.
 - If the account still is active, determine how it's being used before taking subsequent steps.
2. If this is a managed service identity, then disable the service account from signing in, but don't remove it from the directory.
3. Revoke role assignments and OAuth2 consent grants for the service account.
4. After a defined period, and ample warning to owners, delete the service account from the directory.

Next steps

For more information on securing Azure service accounts, see:

[Introduction to Azure service accounts](#)

[Securing managed identities](#)

[Securing service principles](#)

Introduction to Active Directory service accounts

4/10/2022 • 5 minutes to read • [Edit Online](#)

A service has a primary security identity that determines the access rights for local and network resources. The security context for a Microsoft Win32 service is determined by the service account that's used to start the service. You use a service account to:

- Identify and authenticate a service.
- Successfully start a service.
- Access or execute code or an application.
- Start a process.

Types of on-premises service accounts

Depending on your use case, you can use a managed service account (MSA), a computer account, or a user account to run a service. You must first test a service to confirm that it can use a managed service account. If the service can use an MSA, you should use one.

Group managed service accounts

For services that run in your on-premises environment, use [group managed service accounts \(gMSAs\)](#) whenever possible. gMSAs provide a single identity solution for services that run on a server farm or behind a network load balancer. gMSAs can also be used for services that run on a single server. For information about the requirements for gMSAs, see [Get started with group managed service accounts](#).

Standalone managed service accounts

If you can't use a gMSA, use a [standalone managed service account \(sMSA\)](#). sMSAs require at least Windows Server 2008 R2. Unlike gMSAs, sMSAs run on only one server. They can be used for multiple services on that server.

Computer accounts

If you can't use an MSA, consider using a [computer account](#). The LocalSystem account is a predefined local account that has extensive permissions on the local computer and acts as the computer identity on the network.

Services that run as a LocalSystem account access network resources by using the credentials of the computer account in the format <domain_name>\<computer_name>. Its predefined name is NT AUTHORITY\SYSTEM. You can use it to start a service and provide a security context for that service.

NOTE

When you use a computer account, you can't determine which service on the computer is using that account. Consequently, you can't audit which service is making changes.

User accounts

If you can't use an MSA, consider using a [user account](#). A user account can be a *domain* user account or a *local* user account.

A domain user account enables the service to take full advantage of the service security features of Windows and Microsoft Active Directory Domain Services. The service will have local and network permissions granted to the account. It will also have the permissions of any groups of which the account is a member. Domain service accounts support Kerberos mutual authentication.

A local user account (name format: `.\UserName`) exists only in the Security Account Manager database of the host computer. It doesn't have a user object in Active Directory Domain Services. A local account can't be authenticated by the domain. So, a service that runs in the security context of a local user account doesn't have access to network resources (except as an anonymous user). Services that run in the local user context can't support Kerberos mutual authentication in which the service is authenticated by its clients. For these reasons, local user accounts are ordinarily inappropriate for directory-enabled services.

IMPORTANT

Service accounts shouldn't be members of any privileged groups, because privileged group membership confers permissions that might be a security risk. Each service should have its own service account for auditing and security purposes.

Choose the right type of service account

CRITERION	GMSA	sMSA	COMPUTER ACCOUNT	USER ACCOUNT
App runs on a single server	Yes	Yes. Use a gMSA if possible.	Yes. Use an MSA if possible.	Yes. Use an MSA if possible.
App runs on multiple servers	Yes	No	No. Account is tied to the server.	Yes. Use an MSA if possible.
App runs behind a load balancer	Yes	No	No	Yes. Use only if you can't use a gMSA.
App runs on Windows Server 2008 R2	No	Yes	Yes. Use an MSA if possible.	Yes. Use an MSA if possible.
App runs on Windows Server 2012	Yes	Yes. Use a gMSA if possible.	Yes. Use an MSA if possible.	Yes. Use an MSA if possible.
Requirement to restrict service account to single server	No	Yes	Yes. Use an sMSA if possible.	No

Use server logs and PowerShell to investigate

You can use server logs to determine which servers, and how many servers, an application is running on.

To get a listing of the Windows Server version for all servers on your network, you can run the following PowerShell command:

```
Get-ADComputer -Filter 'operatingsystem -like "*server*" -and enabled -eq "true"' `  
-Properties Name,Operatingsystem,OperatingSystemVersion,IPv4Address |  
sort-Object -Property Operatingsystem |  
Select-Object -Property Name,Operatingsystem,OperatingSystemVersion,IPv4Address |  
Out-GridView
```

Find on-premises service accounts

We recommend that you add a prefix such as "svc-" to all accounts that you use as service accounts. This naming convention will make the accounts easier to find and manage. Also consider using a description attribute for the service account and the owner of the service account. The description can be a team alias or security team owner.

Finding on-premises service accounts is key to ensuring their security. Doing so can be difficult for non-MSA accounts. We recommend that you review all the accounts that have access to your important on-premises resources, and that you determine which computer or user accounts might be acting as service accounts.

To learn how to find a service account, see the article about that account type in the ["Next steps" section](#).

Document service accounts

After you've found the service accounts in your on-premises environment, document the following information:

- **Owner:** The person accountable for maintaining the account.
- **Purpose:** The application the account represents, or other purpose.
- **Permission scopes:** The permissions it has or should have, and any groups it's a member of.
- **Risk profile:** The risk to your business if this account is compromised. If the risk is high, use an MSA.
- **Anticipated lifetime and periodic attestation:** How long you anticipate that this account will be live, and how often the owner should review and attest to its ongoing need.
- **Password security:** For user and local computer accounts, where the password is stored. Ensure that passwords are kept secure, and document who has access. Consider using [Privileged Identity Management](#) to secure stored passwords.

Next steps

To learn more about securing service accounts, see the following articles:

- [Secure group managed service accounts](#)
- [Secure standalone managed service accounts](#)
- [Secure computer accounts](#)
- [Secure user accounts](#)
- [Govern on-premises service accounts](#)

Secure group managed service accounts

4/10/2022 • 4 minutes to read • [Edit Online](#)

Group managed service accounts (gMSAs) are managed domain accounts that you use to help secure services. gMSAs can run on a single server or on a server farm, such as systems behind a network load balancing or Internet Information Services (IIS) server. After you configure your services to use a gMSA principal, password management for that account is handled by the Windows operating system.

Benefits of using gMSAs

gMSAs offer a single identity solution with greater security. At the same time, to help reduce administrative overhead, they:

- **Set strong passwords:** gMSAs use 240-byte, randomly generated complex passwords. The complexity and length of gMSA passwords minimizes the likelihood of a service getting compromised by brute force or dictionary attacks.
- **Cycle passwords regularly:** gMSAs shift password management to the Windows operating system, which changes the password every 30 days. Service and domain administrators no longer need to schedule password changes or manage service outages to help keep service accounts secure.
- **Support deployment to server farms:** The ability to deploy gMSAs to multiple servers allows for the support of load balanced solutions where multiple hosts run the same service.
- **Support simplified service principal name (SPN) management:** You can set up an SPN by using PowerShell when you create an account. In addition, services that support automatic SPN registrations might do so against the gMSA, provided that the gMSA permissions are correctly set.

When to use gMSAs

Use gMSAs as the preferred account type for on-premises services unless a service, such as Failover Clustering, doesn't support it.

IMPORTANT

You must test your service with gMSAs before you deploy it into production. To do so, set up a test environment to ensure that the application can use the gMSA, and then access the resources it needs to access. For more information, see [Support for group managed service accounts](#).

If a service doesn't support the use of gMSAs, your next best option is to use a standalone managed service account (sMSA). An sMSA provides the same functionality as a gMSA, but it's intended for deployment on a single server only.

If you can't use a gMSA or sMSA that's supported by your service, you must configure the service to run as a standard user account. Service and domain administrators are required to observe strong password management processes to help keep the account secure.

Assess the security posture of gMSAs

gMSA accounts are inherently more secure than standard user accounts, which require ongoing password management. However, it's important to consider a gMSA's scope of access as you look at its overall security

posture.

Potential security issues and mitigations for using gMSAs are shown in the following table:

SECURITY ISSUE	MITIGATION
gMSA is a member of privileged groups.	<ul style="list-style-type: none">Review your group memberships. To do so, you create a PowerShell script to enumerate all group memberships. You can then filter a resultant CSV file by the names of your gMSA files.Remove the gMSA from privileged groups.Grant the gMSA only the rights and permissions it requires to run its service (consult with your service vendor).
gMSA has read/write access to sensitive resources.	<ul style="list-style-type: none">Audit access to sensitive resources.Archive audit logs to a SIEM, such as Azure Log Analytics or Microsoft Sentinel, for analysis.Remove unnecessary resource permissions if you detect an undesirable level of access.

Find gMSAs

Your organization might already have created gMSAs. To retrieve these accounts, run the following PowerShell cmdlets:

```
Get-ADServiceAccount  
Install-ADServiceAccount  
New-ADServiceAccount  
Remove-ADServiceAccount  
Set-ADServiceAccount  
Test-ADServiceAccount  
Uninstall-ADServiceAccount
```

To work effectively, gMSAs must be in the Managed Service Accounts AD container.

The screenshot shows the Active Directory Users and Computers (ADUC) interface. The left pane displays a tree view of the directory structure under 'Active Directory Users and Computers [NV-DC01.nathalalvelgi.com]'. The 'Managed Service Accounts' folder is highlighted. The right pane shows a table with one entry:

Name	Type	Description
gmsa_sso	msDS-GroupManagedServiceAccount	

To find service MSAs that might not be in the list, run the following commands:

```
Get-ADServiceAccount -Filter *

# This PowerShell cmdlet will return all managed service accounts (both gMSAs and sMSAs). An administrator can differentiate between the two by examining the ObjectClass attribute on returned accounts.

# For gMSA accounts, ObjectClass = msDS-GroupManagedServiceAccount

# For sMSA accounts, ObjectClass = msDS-ManagedServiceAccount

# To filter results to only gMSAs:

Get-ADServiceAccount -Filter * | where-object {$_._ObjectClass -eq "msDS-GroupManagedServiceAccount"}
```

Manage gMSAs

To manage gMSA accounts, you can use the following Active Directory PowerShell cmdlets:

Get-ADServiceAccount

Install-ADServiceAccount

New-ADServiceAccount

Remove-ADServiceAccount

Set-ADServiceAccount

Test-ADServiceAccount

Uninstall-ADServiceAccount

NOTE

Beginning with Windows Server 2012, the *-ADServiceAccount cmdlets work with gMSAs by default. For more information about using the preceding cmdlets, see [Get started with group managed service accounts](#).

Move to a gMSA

gMSA accounts are the most secure type of service account for on-premises needs. If you can move to one, you should. Additionally, consider moving your services to Azure and your service accounts to Azure Active Directory. To move to a gMSA account, do the following:

1. Ensure that the [Key Distribution Service \(KDS\) root key](#) is deployed in the forest. This is a one-time operation.
2. [Create a new gMSA](#).
3. Install the new gMSA on each host that runs the service.

NOTE

For more information about creating and installing a gMSA on a host, prior to configuring your service to use the gMSA, see [Get started with group managed service accounts](#).

4. Change your service identity to gMSA, and specify a blank password.
5. Validate that your service is working under the new gMSA identity.

6. Delete the old service account identity.

Next steps

To learn more about securing service accounts, see the following articles:

- [Introduction to on-premises service accounts](#)
- [Secure standalone managed service accounts](#)
- [Secure computer accounts](#)
- [Secure user accounts](#)
- [Govern on-premises service accounts](#)

Secure standalone managed service accounts

4/10/2022 • 3 minutes to read • [Edit Online](#)

Standalone managed service accounts (sMSAs) are managed domain accounts that you use to help secure one or more services that run on a server. They can't be reused across multiple servers. sMSAs provide automatic password management, simplified service principal name (SPN) management, and the ability to delegate management to other administrators.

In Active Directory, sMSAs are tied to a specific server that runs a service. You can find these accounts listed in the Active Directory Users and Computers snap-in of the Microsoft Management Console.

The screenshot shows the Microsoft Management Console (MMC) window for Active Directory Users and Computers. The left pane displays the navigation tree under 'Active Directory Users and Computers' for the 'contoso.com' domain, including 'Saved Queries', 'Builtin', 'Computers', 'CORP' (which is expanded to show 'Computers', 'Groups', 'ServiceAccount', and 'Users'), 'DisabledOU', 'Domain Controllers', 'Dont sync', 'ForeignSecurityPrincipals', 'Keys', 'LostAndFound', 'Managed Service Account' (which is selected and highlighted in grey), 'Program Data', 'System', 'Users', 'NTDS Quotas', and 'TPM Devices'. The right pane lists 'Managed Service Account' objects with the following details:

Name	Type	Description
adfssvc	msDS-GroupManagedServiceAccount	
MSA-App1	msDS-GroupManagedServiceAccount	
Service01	msDS-ManagedServiceAccount	

The row for 'Service01' is highlighted with a red rectangle.

Managed service accounts were introduced with Windows Server 2008 R2 Active Directory Schema, and they require at least Windows Server 2008 R2.

Benefits of using sMSAs

sMSAs offer greater security than user accounts that are used as service accounts. At the same time, to help reduce administrative overhead, they:

- **Set strong passwords:** sMSAs use 240-byte, randomly generated complex passwords. The complexity and length of sMSA passwords minimizes the likelihood of a service getting compromised by brute force or dictionary attacks.
- **Cycle passwords regularly:** Windows automatically changes the sMSA password every 30 days.

Service and domain administrators don't need to schedule password changes or manage the associated downtime.

- **Simplify SPN management:** Service principal names are automatically updated if the domain functional level is Windows Server 2008 R2. For instance, the service principal name is automatically updated when you:

- Rename the host computer account.
- Change the domain name server (DNS) name of the host computer.
- Add or remove other sam-accountname or dns-hostname parameters by using [PowerShell](#).

When to use sMSAs

sMSAs can simplify management and security tasks. Use sMSAs when you have one or more services deployed to a single server and you can't use a group managed service account (gMSA).

NOTE

Although you can use sMSAs for more than one service, we recommend that each service have its own identity for auditing purposes.

If the creator of the software can't tell you whether it can use an MSA, you must test your application. To do so, create a test environment and ensure that it can access all required resources. For more information, see [Create and install an sMSA](#).

Assess the security posture of sMSAs

sMSAs are inherently more secure than standard user accounts, which require ongoing password management. However, it's important to consider sMSAs' scope of access as part of their overall security posture.

To see how to mitigate potential security issues posed by sMSAs, refer to the following table:

SECURITY ISSUE	MITIGATION
sMSA is a member of privileged groups.	<ul style="list-style-type: none">● Remove the sMSA from elevated privileged groups, such as Domain Admins.● Use the <i>least privileged</i> model, and grant the sMSA only the rights and permissions it requires to run its services.● If you're unsure of the required permissions, consult the service creator.
sMSA has read/write access to sensitive resources.	<ul style="list-style-type: none">● Audit access to sensitive resources.● Archive audit logs to a Security Information and Event Management (SIEM) program, such as Azure Log Analytics or Microsoft Sentinel, for analysis.● Remediate resource permissions if an undesirable level of access is detected.
By default, the sMSA password rollover frequency is 30 days.	You can use group policy to tune the duration, depending on enterprise security requirements. To set the password expiration duration, use the following path: <i>Computer Configuration\Policies\Windows Settings\Security Settings\Security Options</i> . For domain member, use Maximum machine account password age .

Challenges with sMSAs

The challenges associated with sMSAs are as follows:

CHALLENGE	MITIGATION
sMSAs can be used on a single server only.	Use a gMSA if you need to use the account across servers.
sMSAs can't be used across domains.	Use a gMSA if you need to use the account across domains.
Not all applications support sMSAs.	Use a gMSA if possible. Otherwise, use a standard user account or a computer account, as recommended by the application creator.

Find sMSAs

On any domain controller, run DSA.msc, and then expand the managed service accounts container to view all sMSAs.

To return all sMSAs and gMSAs in the Active Directory domain, run the following PowerShell command:

```
Get-ADServiceAccount -Filter *
```

To return only sMSAs in the Active Directory domain, run the following command:

```
Get-ADServiceAccount -Filter * | where { $_.objectClass -eq "msDS-ManagedServiceAccount" }
```

Manage sMSAs

To manage your sMSAs, you can use the following Active Directory PowerShell cmdlets:

```
Get-ADServiceAccount Install-ADServiceAccount New-ADServiceAccount Remove-ADServiceAccount  
Set-ADServiceAccount Test-ADServiceAccount Uninstall-ADServiceAccount
```

Move to sMSAs

If an application service supports sMSAs but not gMSAs, and you're currently using a user account or computer account for the security context, [Create and install an sMSA](#) on the server.

Ideally, you would move resources to Azure and use Azure Managed Identities or service principals.

Next steps

To learn more about securing service accounts, see the following articles:

- [Introduction to on-premises service accounts](#)
- [Secure group managed service accounts](#)
- [Secure computer accounts](#)
- [Secure user accounts](#)
- [Govern on-premises service accounts](#)

Secure on-premises computer accounts

4/10/2022 • 2 minutes to read • [Edit Online](#)

A computer account, or LocalSystem account, is a built-in, highly privileged account with access to virtually all resources on the local computer. The account is not associated with any signed-on user account. Services run as LocalSystem access network resources by presenting the computer's credentials to remote servers in the format <domain_name>\<computer_name>\$. The computer account's predefined name is NT AUTHORITY\SYSTEM. You can use it to start a service and provide security context for that service.

Services (Local)					
Select an item to view its description.	Name	Description	Status	Startup Type	Log On As
	ActiveX Installer (AxInstSV)	Provides User Account Control validation f...	Manual	Local System	
	Agent Activation Runtime_1c32ede	Runtime for activating conversational agen...	Running	Manual	Local System
	AllJoyn Router Service	Routes AllJoyn messages for the local Alljo...	Manual (Trigg...	Local Service	
	App Readiness	Gets apps ready for use the first time a use...	Manual	Local System	
	Application Guard Container Service	Microsoft Defender Application Guard Con...	Running	Automatic (Tri...	Local System
	Application Identity	Determines and verifies the identity of an a...	Manual (Trigg...	Local Service	

Benefits of using a computer account

A computer account provides the following benefits:

- Unrestricted local access:** The computer account provides complete access to the machine's local resources.
- Automatic password management:** Removes the need for you to manually change passwords. The account is a member of Active Directory, and the account password is changed automatically. Using a computer account eliminates the need to register the service principal name for the service.
- Limited access rights off-machine:** The default access-control list in Active Directory Domain Services (AD DS) permits minimal access to computer accounts. In the event of access by an unauthorized user, the service would have only limited access to resources on your network.

Assess the security posture of computer accounts

Some potential challenges and associated mitigations when you use a computer account are listed in the following table:

ISSUE	MITIGATION
Computer accounts are subject to deletion and re-creation when the computer leaves and rejoins the domain.	Validate the need to add a computer to an Active Directory group, and verify which computer account has been added to a group by using the example scripts in the next section of this article.
If you add a computer account to a group, all services that run as LocalSystem on that computer are given the access rights of the group.	Be selective about the group memberships of your computer account. Avoid making a computer account a member of any domain administrator groups, because the associated service has complete access to AD DS.
Improper network defaults for LocalSystem.	Do not assume that the computer account has the default limited access to network resources. Instead, check group memberships for the account carefully.

ISSUE	MITIGATION
Unknown services that run as LocalSystem.	Ensure that all services that run under the LocalSystem account are Microsoft services or trusted services from third parties.

Find services that run under the computer account

To find services that run under the LocalSystem context, use the following PowerShell cmdlet:

```
Get-WmiObject win32_service | select Name, StartName | Where-Object {($_.StartName -eq "LocalSystem")}
```

To find computer accounts that are members of a specific group, run the following PowerShell cmdlet:

```
Get-ADComputer -Filter {Name -Like "*"} -Properties MemberOf | Where-Object {[STRING]$_.MemberOf -like "Your_Group_Name_here*"} | Select Name, MemberOf
```

To find computer accounts that are members of identity administrators groups (domain administrators, enterprise administrators, and administrators), run the following PowerShell cmdlet:

```
Get-ADGroupMember -Identity Administrators -Recursive | Where objectClass -eq "computer"
```

Move from computer accounts

IMPORTANT

Computer accounts are highly privileged accounts and should be used only when your service needs unrestricted access to local resources on the machine and you can't use a managed service account (MSA).

- Check with your service owner to see whether their service can be run by using an MSA, and use a group managed service account (gMSA) or a standalone managed service account (sMSA) if your service supports it.
- Use a domain user account with only the permissions that you need to run your service.

Next steps

To learn more about securing service accounts, see the following articles:

- [Introduction to on-premises service accounts](#)
- [Secure group managed service accounts](#)
- [Secure standalone managed service accounts](#)
- [Secure user accounts](#)
- [Govern on-premises service accounts](#)

Secure user-based service accounts in Active Directory

4/10/2022 • 4 minutes to read • [Edit Online](#)

Using on-premises user accounts is the traditional approach to helping secure services that run on Windows. Use these accounts as a last resort when group managed service accounts (gMSAs) and standalone managed service accounts (sMSAs) aren't supported by your service. For information about selecting the best type of account to use, see [Introduction to on-premises service accounts](#).

You might also want to investigate whether you can move your service to use an Azure service account such as a managed identity or a service principal.

You can create on-premises user accounts to provide a security context for the services and permissions that the accounts require to access local and network resources. On-premises user accounts require manual password management, much like any other Active Directory user account. Service and domain administrators are required to observe strong password management processes to help keep these accounts secure.

When you create a user account as a service account, use it for a single service only. Name it in a way that makes it clear that it's a service account and which service it's for.

Benefits and challenges

On-premises user accounts can provide significant benefits. They're the most versatile account type for use with services. User accounts used as service accounts can be controlled by all the policies that govern normal user accounts. But you should use them only if you can't use an MSA. Also evaluate whether a computer account is a better option.

The challenges associated with the use of on-premises user accounts are summarized in the following table:

CHALLENGE	MITIGATION
Password management is a manual process that can lead to weaker security and service downtime.	<ul style="list-style-type: none">Make sure that password complexity and password changes are governed by a robust process that ensures regular updates with strong passwords.Coordinate password changes with a password update on the service, which will help reduce service downtime.
Identifying on-premises user accounts that are acting as service accounts can be difficult.	<ul style="list-style-type: none">Document and maintain records of service accounts that are deployed in your environment.Track the account name and the resources to which they're assigned access.Consider adding a prefix of "svc-" to all user accounts that are used as service accounts.

Find on-premises user accounts used as service accounts

On-premises user accounts are just like any other Active Directory user account. It can be difficult to find such accounts, because no single attribute of a user account identifies it as a service account.

We recommend that you create an easily identifiable naming convention for any user account that you use as a service account. For example, you might add "svc-" as a prefix and name the service "svc-HRDataConnector".

You can use some of the following criteria to find these service accounts. However, this approach might not find all accounts, such as:

- Accounts that are trusted for delegation.
- Accounts with service principal names.
- Accounts with passwords that are set to never expire.

To find the on-premises user accounts you've created for services, you can run the following PowerShell commands.

To find accounts that are trusted for delegation:

```
Get-ADObject -Filter {((msDS-AllowedToDelegateTo -like '*') -or (UserAccountControl -band 0x0080000) -or (UserAccountControl -band 0x1000000)) -prop samAccountName,msDS-AllowedToDelegateTo,servicePrincipalName,userAccountControl | select DistinguishedName, ObjectClass, samAccountName, servicePrincipalName, @{name='DelegationStatus';expression={if($_.UserAccountControl -band 0x80000){'AllServices'}else{'SpecificServices'}}}, @{name='AllowedProtocols';expression={if($_.UserAccountControl -band 0x1000000){'Any'}else{'Kerberos'}}}, @{name='DestinationServices';expression={$_.msDS-AllowedToDelegateTo'}}
```

To find accounts that have service principal names:

```
Get-ADUser -Filter * -Properties servicePrincipalName | where {$_.servicePrincipalName -ne $null}
```

To find accounts with passwords that are set to never expire:

```
Get-ADUser -Filter * -Properties PasswordNeverExpires | where {$_.PasswordNeverExpires -eq $true}
```

You can also audit access to sensitive resources, and archive audit logs to a security information and event management (SIEM) system. By using systems such as Azure Log Analytics or Microsoft Sentinel, you can search for and analyze and service accounts.

Assess the security of on-premises user accounts

You can assess the security of on-premises user accounts that are being used as service accounts by using the following criteria:

- What is the password management policy?
- Is the account a member of any privileged groups?
- Does the account have read/write permissions to important resources?

Mitigate potential security issues

Potential security issues and their mitigations for on-premises user accounts are summarized in the following table:

SECURITY ISSUE	MITIGATION
----------------	------------

SECURITY ISSUE	MITIGATION
Password management.	<ul style="list-style-type: none"> • Ensure that password complexity and password change are governed by a robust process that includes regular updates and strong password requirements. • Coordinate password changes with a password update to minimize service downtime.
The account is a member of privileged groups.	<ul style="list-style-type: none"> • Review group memberships. • Remove the account from privileged groups. • Grant the account only the rights and permissions it requires to run its service (consult with service vendor). For example, you might be able to deny sign-in locally or deny interactive sign-in.
The account has read/write permissions to sensitive resources.	<ul style="list-style-type: none"> • Audit access to sensitive resources. • Archive audit logs to a SIEM (Azure Log Analytics or Microsoft Sentinel) for analysis. • Remediate resource permissions if an undesirable level of access is detected.

Move to more secure account types

Microsoft doesn't recommend that you use on-premises user accounts as service accounts. For any service that uses this type of account, assess whether it can instead be configured to use a gMSA or an sMSA.

Additionally, evaluate whether the service itself could be moved to Azure so that more secure service account types can be used.

Next steps

To learn more about securing service accounts, see the following articles:

- [Introduction to on-premises service accounts](#)
- [Secure group managed service accounts](#)
- [Secure standalone managed service accounts](#)
- [Secure computer accounts](#)
- [Govern on-premises service accounts](#)

Govern on-premises service accounts

4/10/2022 • 6 minutes to read • [Edit Online](#)

Active Directory offers four types of on-premises service accounts:

- [Group managed service accounts \(gMSAs\)](#)
- [Standalone managed service accounts \(sMSAs\)](#)
- [Computer accounts](#)
- [User accounts that function as service accounts](#)

It is critical to govern service accounts closely so that you can:

- Protect them based on their use-case requirements and purpose.
- Manage the lifecycle of the accounts and their credentials.
- Assess them based on the risk they'll be exposed to and the permissions they carry.
- Ensure that Active Directory and Azure Active Directory have no stale service accounts with potentially far-reaching permissions.

Principles for creating a new service account

When you create a service account, understand the considerations listed in the following table:

PRINCIPLE	CONSIDERATION
Service account mapping	Tie the service account to a single service, application, or script.
Ownership	Ensure that there's an owner who requests and assumes responsibility for the account.
Scope	Define the scope clearly, and anticipate usage duration for the service account.
Purpose	Create service accounts for a single, specific purpose.
Permissions	Apply the principle of <i>least permission</i> . To do so: <ul style="list-style-type: none">• Never assign permissions to built-in groups, such as administrators.• Remove local machine permissions, where appropriate.• Tailor access, and use Active Directory delegation for directory access.• Use granular access permissions.• Set account expirations and location-based restrictions on user-based service accounts.
Monitor and audit use	Monitor sign-in data, and ensure that it matches the intended usage. Set alerts for anomalous usage.

Set restrictions for user accounts

For user accounts that are used as service accounts, apply the following settings:

- **Account expiration:** Set the service account to automatically expire at a set time after its review period, unless you've determined that the account should continue.
- **LogonWorkstations:** Restrict permissions where the service account can sign in. If it runs locally on a machine and accesses only resources on that machine, restrict it from signing in anywhere else.
- **Cannot change password:** Prevent the service account from changing its own password by setting the parameter to true.

Build a lifecycle management process

To help maintain the security of your service accounts, you must manage them from the time you identify the need until they're decommissioned.

For lifecycle management of service accounts, use the following process:

1. Collect usage information for the account.
2. Move the service account and app to the configuration management database (CMDB).
3. Perform risk assessment or a formal review.
4. Create the service account and apply restrictions.
5. Schedule and perform recurring reviews. Adjust permissions and scopes as necessary.
6. Deprovision the account when appropriate.

Collect usage information for the service account

Collect relevant business information for each service account. The following table lists the minimum amount of information to collect, but you should collect everything that's necessary to make the business case for each account's existence.

DATA	DESCRIPTION
Owner	The user or group that's accountable for the service account
Purpose	The purpose of the service account
Permissions (scopes)	The expected set of permissions
CMDB links	The cross-link service account with the target script or application and owners
Risk	The risk and business impact scoring, based on the security risk assessment
Lifetime	The anticipated maximum lifetime for enabling the scheduling of account expiration or recertification

Ideally, you want to make the request for an account self-service, and require the relevant information. The owner can be an application or business owner, an IT member, or an infrastructure owner. By using a tool such as Microsoft Forms for this request and associated information, you'll make it easier to port it to your CMDB inventory tool if the account is approved.

Onboard service account to CMDB

Store the collected information in a CMDB-type application. In addition to the business information, include all dependencies on other infrastructure, apps, and processes. This central repository makes it easier to:

- Assess risk.
- Configure the service account with the required restrictions.
- Understand any relevant functional and security dependencies.
- Conduct regular reviews for security and continued need.
- Contact the owners for reviewing, retiring, and changing the service account.

Consider a service account that's used to run a website and has permissions to connect to one or more Human Resources (HR) SQL databases. The information stored in your CMDB for the service account, including example descriptions, is listed in the following table:

DATA	EXAMPLE DESCRIPTION
Owner, Deputy	John Bloom, Anna Mayers
Purpose	Run the HR webpage and connect to HR databases. Can impersonate end users when accessing databases.
Permissions, scopes	HR-WEBServer: sign in locally; run web page HR-SQL1: sign in locally; read permissions on all HR databases HR-SQL2: sign in locally; read permissions on Salary database only
Cost Center	883944
Risk Assessed	Medium; Business Impact: Medium; private information; Medium
Account Restrictions	Log on to: only aforementioned servers; Cannot change password; MBI-Password Policy;
Lifetime	Unrestricted
Review Cycle	Biannually (by owner, by security team, by privacy)

Perform a risk assessment or formal review of service account usage

Suppose your account is compromised by an unauthorized source. Assess the risks the account might pose to its associated application or service and to your infrastructure. Consider both direct and indirect risks.

- What would an unauthorized user gain direct access to?
- What other information or systems can the service account access?
- Can the account be used to grant additional permissions?
- How will you know when the permissions change?

After you've conducted and documented the risk assessment, you might find that the risks have an impact on:

- Account restrictions.
- Account lifetime.
- Account review requirements (cadence and reviewers).

Create a service account and apply account restrictions

Create a service account only after you've completed the risk assessment and documented the relevant information in your CMDB. Align the account restrictions with the risk assessment. Consider the following

restrictions when they're relevant to your assessment:

- For all user accounts that you use as service accounts, define a realistic, definite end date. Set the date by using the **Account Expires** flag. For more information, see [Set-ADAccountExpiration](#).
- Login to the [LogonWorkstation](#).
- [Password Policy](#) requirements.
- Account creation in an [organizational unit location](#) that ensures management only for allowed users.
- Setting up and collecting auditing [that detects changes](#) to the service account, and [service account use](#).

When you're ready to put the service account into production, grant access to it more securely.

Schedule regular reviews of service accounts

Set up regular reviews of service accounts that are classified as medium and high risk. Reviews should include:

- Owner attestation to the continued need for the account, and a justification of permissions and scopes.
- Review by privacy and security teams, including an evaluation of upstream and downstream connections.
- Data from audits, ensuring that it's being used only for its intended purposes.

Deprovision service accounts

In your deprovisioning process, first remove permissions and monitoring, and then remove the account, if appropriate.

You deprovision service accounts when:

- The script or application that the service account was created for is retired.
- The function within the script or application, which the service account is used for (for example, access to a specific resource), is retired.
- The service account has been replaced with a different service account.

After you've removed all permissions, remove the account by doing the following:

1. When the associated application or script is deprovisioned, monitor the sign-ins and resource access for the associated service accounts to be sure that they're not being used in another process. If you're sure it's no longer needed, go to next step.
2. Disable the service account to prevent sign-in, and ensure that it's no longer needed. Create a business policy for the time during which accounts should remain disabled.
3. After the remain-disabled policy is fulfilled, delete the service account.
 - **For MSAs:** [Uninstall the account](#) by using PowerShell, or delete it manually from the managed service account container.
 - **For computer or user accounts:** Manually delete the account from within Active Directory.

Next steps

To learn more about securing service accounts, see the following articles:

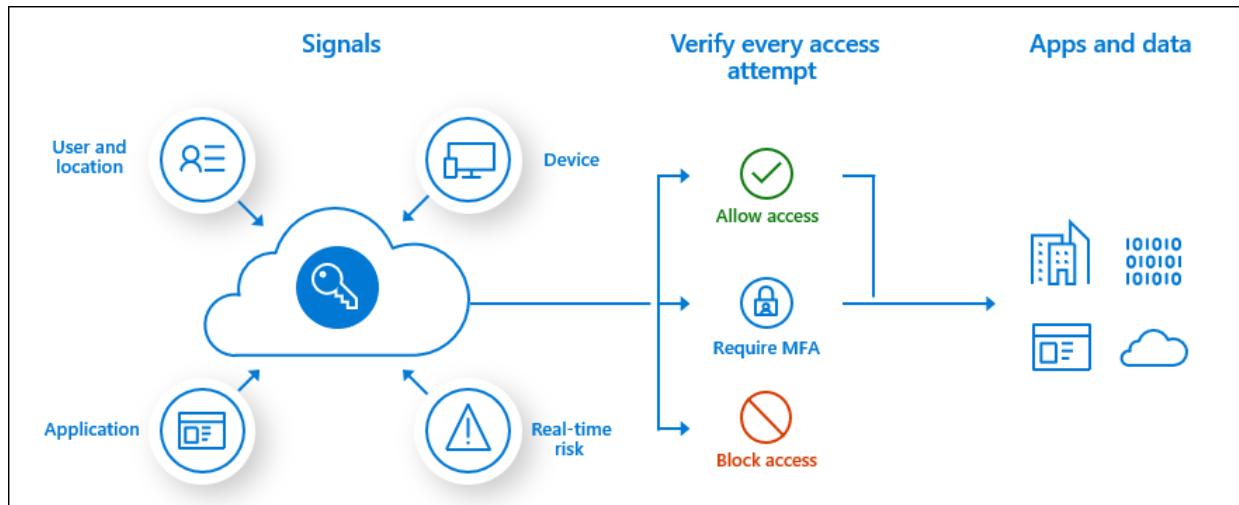
- [Introduction to on-premises service accounts](#)
- [Secure group managed service accounts](#)
- [Secure standalone managed service accounts](#)
- [Secure computer accounts](#)

- Secure user accounts

Overview of Azure AD Multi-Factor Authentication for your organization

4/10/2022 • 2 minutes to read • [Edit Online](#)

There are multiple ways to enable Azure AD Multi-Factor Authentication for your Azure Active Directory (AD) users based on the licenses that your organization owns.



Based on our studies, your account is more than 99.9% less likely to be compromised if you use multi-factor authentication (MFA).

So how does your organization turn on MFA even for free, before becoming a statistic?

Free option

Customers who are utilizing the free benefits of Azure AD can use [security defaults](#) to enable multi-factor authentication in their environment.

Microsoft 365 Business, E3, or E5

For customers with Microsoft 365, there are two options:

- Azure AD Multi-Factor Authentication is either enabled or disabled for all users, for all sign-in events. There is no ability to only enable multi-factor authentication for a subset of users, or only under certain scenarios. Management is through the Office 365 portal.
- For an improved user experience, upgrade to Azure AD Premium P1 or P2 and use Conditional Access. For more information, see [secure Microsoft 365 resources with multi-factor authentication](#).

Azure AD Premium P1

For customers with Azure AD Premium P1 or similar licenses that include this functionality such as Enterprise Mobility + Security E3, Microsoft 365 F1, or Microsoft 365 E3:

Use [Azure AD Conditional Access](#) to prompt users for multi-factor authentication during certain scenarios or events to fit your business requirements.

Azure AD Premium P2

For customers with Azure AD Premium P2 or similar licenses that include this functionality such as Enterprise Mobility + Security E5 or Microsoft 365 E5:

Provides the strongest security position and improved user experience. Adds [risk-based Conditional Access](#) to the Azure AD Premium P1 features that adapts to user's patterns and minimizes multi-factor authentication prompts.

Authentication methods

METHOD	SECURITY DEFAULTS	ALL OTHER METHODS
Notification through mobile app	X	X
Verification code from mobile app or hardware token		X
Text message to phone		X
Call to phone		X

Next steps

To get started, see the tutorial to [secure user sign-in events with Azure AD Multi-Factor Authentication](#).

For more information on licensing, see [Features and licenses for Azure AD Multi-Factor Authentication](#).

Security defaults in Azure AD

4/10/2022 • 8 minutes to read • [Edit Online](#)

Managing security can be difficult with common identity-related attacks like password spray, replay, and phishing becoming more popular. Security defaults make it easier to help protect your organization from these attacks with preconfigured security settings:

- Requiring all users to register for Azure AD Multi-Factor Authentication.
- Requiring administrators to do multi-factor authentication.
- Blocking legacy authentication protocols.
- Requiring users to do multi-factor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.

Why security defaults?

Quoting Alex Weinert, Director of Identity Security at Microsoft:

...our telemetry tells us that more than 99.9% of organization account compromise could be stopped by simply using MFA, and that disabling legacy authentication correlates to a 67% reduction in compromise risk (and completely stops password spray attacks, 100% of which come in via legacy authentication)...

More details on why security defaults are being made available can be found in Alex Weinert's blog post, [Introducing security defaults](#).

Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You turn on security defaults in the Azure portal. If your tenant was created on or after October 22, 2019, security defaults may be enabled in your tenant. To protect all of our users, security defaults are being rolled out to new tenants at creation.

Who's it for?

- Organizations who want to increase their security posture, but don't know how or where to start.
- Organizations using the free tier of Azure Active Directory licensing.

Who should use Conditional Access?

- If you're an organization currently using Conditional Access policies, security defaults are probably not right for you.
- If you're an organization with Azure Active Directory Premium licenses, security defaults are probably not right for you.
- If your organization has complex security requirements, you should consider Conditional Access.

Policies enforced

Unified Multi-Factor Authentication registration

All users in your tenant must register for multi-factor authentication (MFA) in the form of the Azure AD Multi-Factor Authentication. Users have 14 days to register for Azure AD Multi-Factor Authentication by using the Microsoft Authenticator app. After the 14 days have passed, the user can't sign in until registration is completed. A user's 14-day period begins after their first successful interactive sign-in after enabling security defaults.

Protecting administrators

Users with privileged access have increased access to your environment. Because of the power these accounts have, you should treat them with special care. One common method to improve the protection of privileged accounts is to require a stronger form of account verification for sign-in. In Azure AD, you can get a stronger account verification by requiring multi-factor authentication. We recommend having separate accounts for administration and standard productivity tasks to significantly reduce the number of times your admins are prompted for MFA.

After registration with Azure AD Multi-Factor Authentication is finished, the following Azure AD administrator roles will be required to do extra authentication every time they sign in:

- Global administrator
- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Security administrator
- SharePoint administrator
- User administrator

Protecting all users

We tend to think that administrator accounts are the only accounts that need extra layers of authentication. Administrators have broad access to sensitive information and can make changes to subscription-wide settings. But attackers frequently target end users.

After these attackers gain access, they can request access to privileged information for the original account holder. They can even download the entire directory to do a phishing attack on your whole organization.

One common method to improve protection for all users is to require a stronger form of account verification, such as Multi-Factor Authentication, for everyone. After users complete Multi-Factor Authentication registration, they'll be prompted for another authentication whenever necessary. Azure AD decides when a user will be prompted for Multi-Factor Authentication, based on factors such as location, device, role and task. This functionality protects all applications registered with Azure AD including SaaS applications.

Blocking legacy authentication

To give your users easy access to your cloud apps, Azure AD supports various authentication protocols, including legacy authentication. *Legacy authentication* is a term that refers to an authentication request made by:

- Clients that don't use modern authentication (for example, an Office 2010 client).
- Any client that uses older mail protocols such as IMAP, SMTP, or POP3.

Today, most compromising sign-in attempts come from legacy authentication. Legacy authentication doesn't support Multi-Factor Authentication. Even if you have a Multi-Factor Authentication policy enabled on your directory, an attacker can authenticate by using an older protocol and bypass Multi-Factor Authentication.

After security defaults are enabled in your tenant, all authentication requests made by an older protocol will be blocked. Security defaults blocks Exchange Active Sync basic authentication.

WARNING

Before you enable security defaults, make sure your administrators aren't using older authentication protocols. For more information, see [How to move away from legacy authentication](#).

- [How to set up a multifunction device or application to send email using Microsoft 365](#)

Protecting privileged actions

Organizations use various Azure services managed through the Azure Resource Manager API, including:

- Azure portal
- Azure PowerShell
- Azure CLI

Using Azure Resource Manager to manage your services is a highly privileged action. Azure Resource Manager can alter tenant-wide configurations, such as service settings and subscription billing. Single-factor authentication is vulnerable to various attacks like phishing and password spray.

It's important to verify the identity of users who want to access Azure Resource Manager and update configurations. You verify their identity by requiring more authentication before you allow access.

After you enable security defaults in your tenant, any user accessing the following services must complete multi-factor authentication:

- Azure portal
- Azure PowerShell
- Azure CLI

This policy applies to all users who are accessing Azure Resource Manager services, whether they're an administrator or a user.

NOTE

Pre-2017 Exchange Online tenants have modern authentication disabled by default. In order to avoid the possibility of a login loop while authenticating through these tenants, you must [enable modern authentication](#).

NOTE

The Azure AD Connect synchronization account is excluded from security defaults and will not be prompted to register for or perform multi-factor authentication. Organizations should not be using this account for other purposes.

Deployment considerations

The following extra considerations are related to deployment of security defaults.

Emergency access accounts

Every organization should have at least two emergency access account configured.

These accounts may be used in scenarios where your normal administrator accounts can't be used. For example: The person with the most recent Global Administrator access has left the organization. Azure AD prevents the last Global Administrator account from being deleted, but it doesn't prevent the account from being deleted or disabled on-premises. Either situation might make the organization unable to recover the account.

Emergency access accounts are:

- Assigned Global Administrator rights in Azure AD
- Aren't used on a daily basis
- Are protected with a long complex password

The credentials for these emergency access accounts should be stored offline in a secure location such as a fireproof safe. Only authorized individuals should have access to these credentials.

To create an emergency access account:

1. Sign in to the **Azure portal** as an existing Global Administrator.
2. Browse to **Azure Active Directory > Users**.
3. Select **New user**.
4. Select **Create user**.
5. Give the account a **User name**.
6. Give the account a **Name**.
7. Create a long and complex password for the account.
8. Under **Roles**, assign the **Global Administrator** role.
9. Under **Usage location**, select the appropriate location.
10. Select **Create**.

You may choose [disable password expiration](#) to for these accounts using Azure AD PowerShell.

For more detailed information about emergency access accounts, see the article [Manage emergency access accounts in Azure AD](#).

Authentication methods

These free security defaults allow registration and use of Azure AD Multi-Factor Authentication **using only the Microsoft Authenticator app using notifications**. Conditional Access allows the use of any authentication method the administrator chooses to enable.

METHOD	SECURITY DEFAULTS	CONDITIONAL ACCESS
Notification through mobile app	X	X
Verification code from mobile app or hardware token	X**	X
Text message to phone		X
Call to phone		X
App passwords		X***

- ** Users may use verification codes from the Microsoft Authenticator app but can only register using the notification option.
- *** App passwords are only available in per-user MFA with legacy authentication scenarios only if enabled by administrators.

WARNING

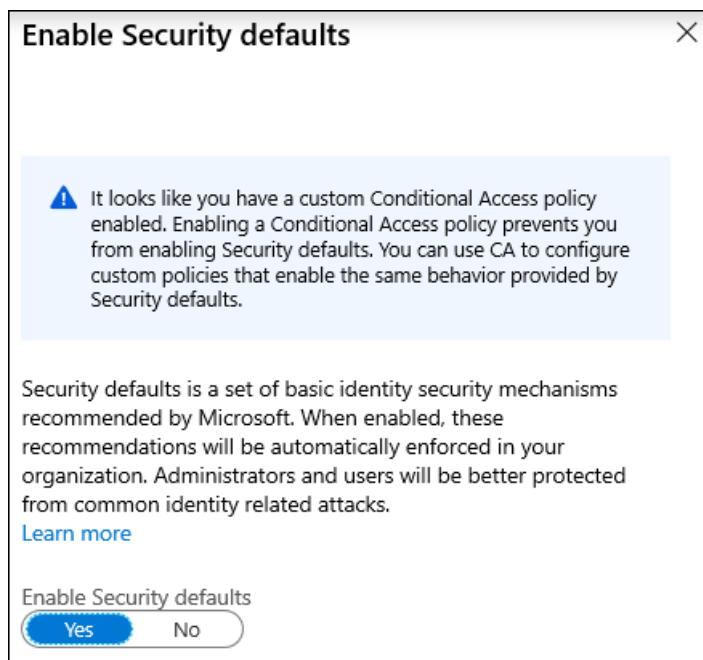
Do not disable methods for your organization if you are using Security Defaults. Disabling methods may lead to locking yourself out of your tenant. Leave all **Methods available to users** enabled in the [MFA service settings portal](#).

Disabled MFA status

If your organization is a previous user of per-user based Azure AD Multi-Factor Authentication, don't be alarmed to not see users in an **Enabled** or **Enforced** status if you look at the Multi-Factor Auth status page. **Disabled** is the appropriate status for users who are using security defaults or Conditional Access based Azure AD Multi-Factor Authentication.

Conditional Access

You can use Conditional Access to configure policies similar to security defaults, but with more granularity including user exclusions, which aren't available in security defaults. If you're using Conditional Access and have Conditional Access policies enabled in your environment, security defaults won't be available to you. More information about Azure AD licensing can be found on the [Azure AD pricing page](#).



Here are step-by-step guides for Conditional Access to configure a set of policies, which form a good starting point for protecting your identities:

- [Require MFA for administrators](#)
- [Require MFA for Azure management](#)
- [Block legacy authentication](#)
- [Require MFA for all users](#)

Enabling security defaults

To enable security defaults in your directory:

1. Sign in to the [Azure portal](#) as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to [Azure Active Directory > Properties](#).
3. Select **Manage security defaults**.
4. Set the **Enable security defaults** toggle to **Yes**.
5. Select **Save**.

Microsoft Azure

Home > Contoso - Properties

Contoso - Properties

Azure Active Directory

Search (Ctrl+)

Save Discard

Directory properties

Name *****
Contoso

Country or region
United States

Location
United States datacenters

Notification language
English

Directory ID
69997834-fa40-45da-bad8-382c3bdc66c3

Technical contact
technical@contoso.com

Global privacy contact
privacy@contoso.com

Privacy statement URL
|

Access management for Azure resources

balas@contoso.com Bala Sandhu (balas@contoso.com) can manage access to management groups in this directory [Learn more](#)

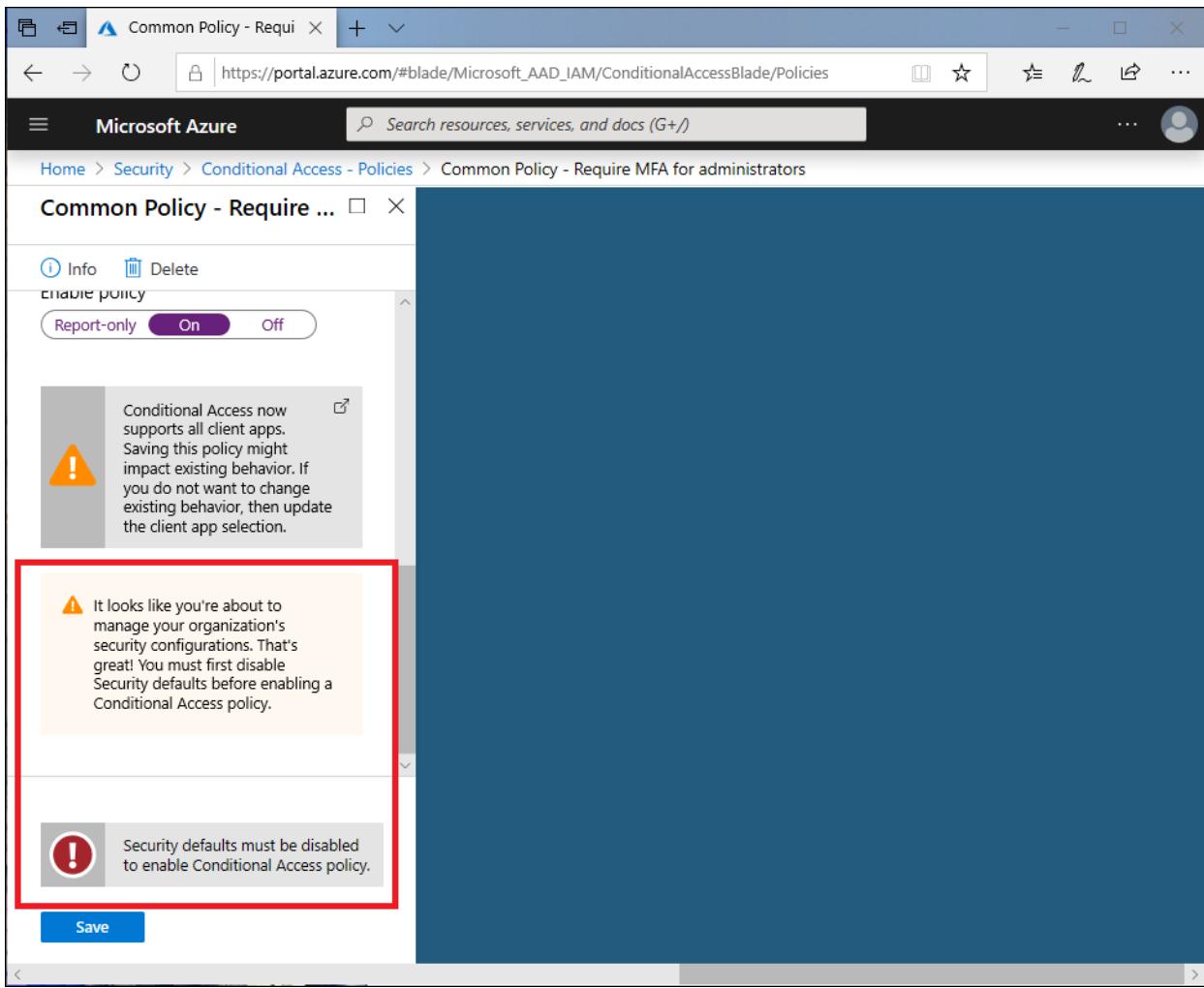
Yes No

Manage Security defaults

Save

Disabling security defaults

Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults.



To disable security defaults in your directory:

1. Sign in to the [Azure portal](#) as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to **Azure Active Directory > Properties**.
3. Select **Manage security defaults**.
4. Set the **Enable security defaults** toggle to **No**.
5. Select **Save**.

Next steps

[Common Conditional Access policies](#)

Blocking legacy authentication

4/10/2022 • 6 minutes to read • [Edit Online](#)

To give your users easy access to your cloud apps, Azure Active Directory (Azure AD) supports a broad variety of authentication protocols including legacy authentication. Legacy authentication is a term that refers to an authentication request made by:

- Older Office clients that do not use modern authentication (for example, Office 2010 client)
- Any client that uses legacy mail protocols such as IMAP/SMTP/POP3

Today, the majority of all compromising sign-in attempts come from legacy authentication. Legacy authentication does not support multi-factor authentication (MFA). Even if you have an MFA policy enabled on your directory, a bad actor can authenticate using a legacy protocol and bypass MFA. The best way to protect your account from malicious authentication requests made by legacy protocols is to block these attempts altogether.

Identify legacy authentication use

Before you can block legacy authentication in your directory, you need to first understand if your users have apps that use legacy authentication and how it affects your overall directory. Azure AD sign-in logs can be used to understand if you're using legacy authentication.

1. Navigate to the [Azure portal](#) > [Azure Active Directory](#) > [Sign-ins](#).
2. Add the **Client App** column if it is not shown by clicking on [Columns](#) > [Client App](#).
3. Filter by **Client App** > check all the **Legacy Authentication Clients** options presented.
4. Filter by **Status** > **Success**.
5. Expand your date range if necessary using the **Date** filter.
6. If you have activated the [new sign-in activity reports preview](#), repeat the above steps also on the **User sign-ins (non-interactive)** tab.

Filtering will only show you successful sign-in attempts that were made by the selected legacy authentication protocols. Clicking on each individual sign-in attempt will show you additional details. The Client App column or the Client App field under the Basic Info tab after selecting an individual row of data will indicate which legacy authentication protocol was used. These logs will indicate which users are still depending on legacy authentication and which applications are using legacy protocols to make authentication requests. For users that do not appear in these logs and are confirmed to not be using legacy authentication, implement a Conditional Access policy or enable the Baseline policy: block legacy authentication for these users only.

Moving away from legacy authentication

Once you have a better idea of who is using legacy authentication in your directory and which applications depend on it, the next step is upgrading your users to use modern authentication. Modern authentication is a method of identity management that offers more secure user authentication and authorization. If you have an MFA policy in place on your directory, modern authentication ensures that the user is prompted for MFA when required. It is the more secure alternative to legacy authentication protocols.

This section gives a step-by-step overview on how to update your environment to modern authentication. Read through the steps below before enabling a legacy authentication blocking policy in your organization.

Step 1: Enable modern authentication in your directory

The first step in enabling modern authentication is making sure your directory supports modern authentication. Modern authentication is enabled by default for directories created on or after August 1, 2017. If your directory was created prior to this date, you'll need to manually enable modern authentication for your directory using the following steps:

1. Check to see if your directory already supports modern authentication by running `Get-CsOAuthConfiguration` from the [Skype for Business Online PowerShell module](#).
2. If your command returns an empty `OAuthServers` property, then Modern Authentication is disabled. Update the setting to enable modern authentication using `Set-CsOAuthConfiguration`. If your `OAuthServers` property contains an entry, you're good to go.

Be sure to complete this step before moving forward. It's critical that your directory configurations are changed first because they dictate which protocol will be used by all Office clients. Even if you're using Office clients that support modern authentication, they will default to using legacy protocols if modern authentication is disabled on your directory.

Step 2: Office applications

Once you have enabled modern authentication in your directory, you can start updating applications by enabling modern authentication for Office clients. Office 2016 or later clients support modern authentication by default. No extra steps are required.

If you are using Office 2013 Windows clients or older, we recommend upgrading to Office 2016 or later. Even after completing the prior step of enabling modern authentication in your directory, the older Office applications will continue to use legacy authentication protocols. If you are using Office 2013 clients and are unable to immediately upgrade to Office 2016 or later, follow the steps in the following article to [Enable Modern Authentication for Office 2013 on Windows devices](#). To help protect your account while you're using legacy authentication, we recommend using strong passwords across your directory. Check out [Azure AD password protection](#) to ban weak passwords across your directory.

Office 2010 does not support modern authentication. You will need to upgrade any users with Office 2010 to a more recent version of Office. We recommend upgrading to Office 2016 or later, as it blocks legacy authentication by default.

If you are using macOS, we recommend upgrading to Office for Mac 2016 or later. If you are using the native mail client, you will need to have macOS version 10.14 or later on all devices.

Step 3: Exchange and SharePoint

For Windows-based Outlook clients to use modern authentication, Exchange Online must be modern authentication enabled as well. If modern authentication is disabled for Exchange Online, Windows-based Outlook clients that support modern authentication (Outlook 2013 or later) will use basic authentication to connect to Exchange Online mailboxes.

SharePoint Online is enabled for modern authentication default. For directories created after August 1, 2017, modern authentication is enabled by default in Exchange Online. However, if you had previously disabled modern authentication or are you using a directory created prior to this date, follow the steps in the following article to [Enable modern authentication in Exchange Online](#).

Step 4: Skype for Business

To prevent legacy authentication requests made by Skype for Business, it is necessary to enable modern authentication for Skype for Business Online. For directories created after August 1, 2017, modern authentication for Skype for Business is enabled by default.

We suggest you transition to Microsoft Teams, which supports modern authentication by default. However, if you are unable to migrate at this time, you will need to enable modern authentication for Skype for Business Online so that Skype for Business clients start using modern authentication. Follow the steps in this article [Skype](#)

for Business topologies supported with [Modern Authentication](#), to enable Modern Authentication for Skype for Business.

In addition to enabling modern authentication for Skype for Business Online, we recommend enabling modern authentication for Exchange Online when enabling modern authentication for Skype for Business. This process will help synchronize the state of modern authentication in Exchange Online and Skype for Business online and will prevent multiple sign-in prompts for Skype for Business clients.

Step 5: Using mobile devices

Applications on your mobile device need to block legacy authentication as well. We recommend using Outlook for Mobile. Outlook for Mobile supports modern authentication by default and will satisfy other MFA baseline protection policies.

In order to use the native iOS mail client, you will need to be running iOS version 11.0 or later to ensure the mail client has been updated to block legacy authentication.

Step 6: On-premises clients

If you are a hybrid customer using Exchange Server on-premises and Skype for Business on-premises, both services will need to be updated to enable modern authentication. When using modern authentication in a hybrid environment, you're still authenticating users on-premises. The story of authorizing their access to resources (files or emails) changes.

Before you can begin enabling modern authentication on-premises, please be sure that you have met the prerequisites. You're now ready to enable modern authentication on-premises.

Steps for enabling modern authentication can be found in the following articles:

- [How to configure Exchange Server on-premises to use Hybrid Modern Authentication](#)
- [How to use Modern Authentication \(ADAL\) with Skype for Business](#)

Next steps

- [How to configure Exchange Server on-premises to use Hybrid Modern Authentication](#)
- [How to use Modern Authentication \(ADAL\) with Skype for Business](#)
- [Block legacy authentication](#)

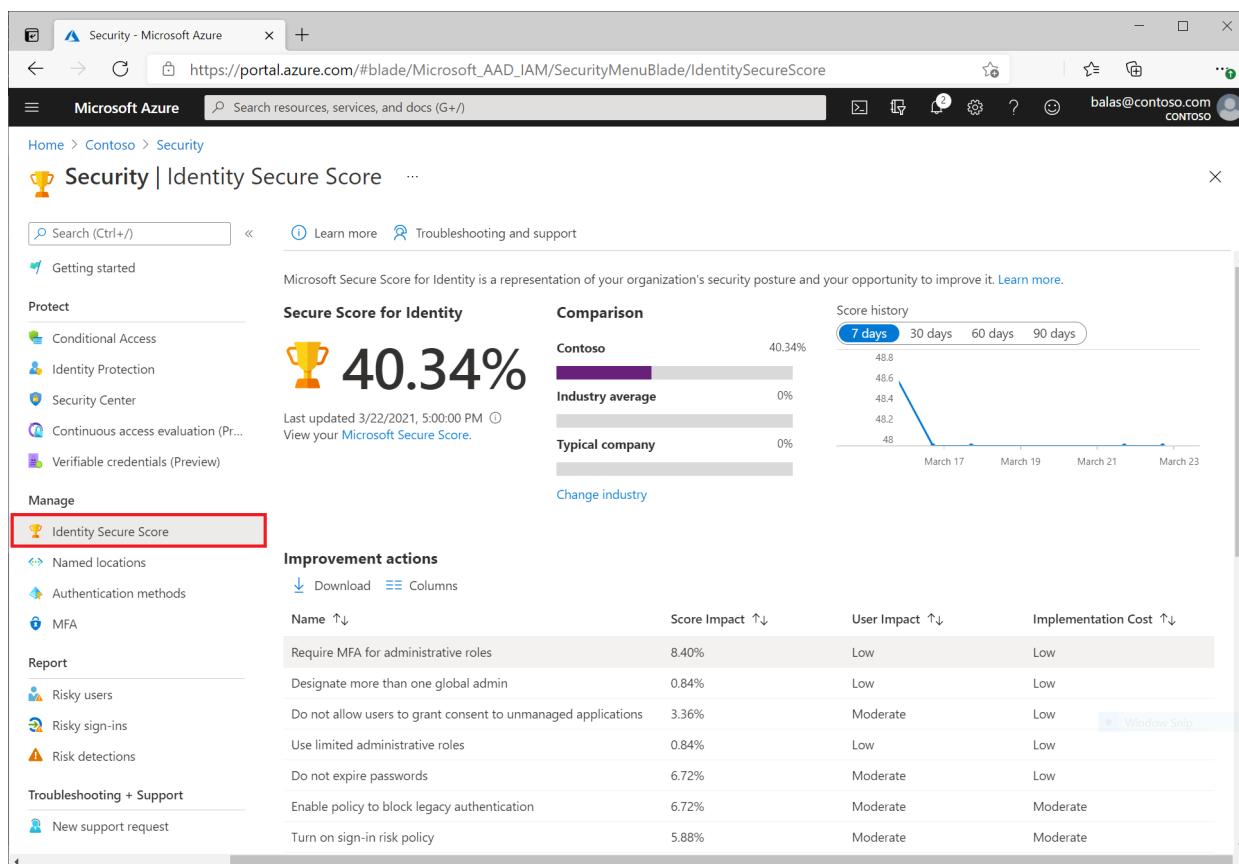
What is the identity secure score in Azure Active Directory?

4/10/2022 • 5 minutes to read • [Edit Online](#)

How secure is your Azure AD tenant? If you don't know how to answer this question, this article explains how the identity secure score helps you to monitor and improve your identity security posture.

What is an identity secure score?

The identity secure score is percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security. Each improvement action in identity secure score is tailored to your specific configuration.



The score helps you to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

You can access the score and related information on the identity secure score dashboard. On this dashboard, you find:

- Your identity secure score
- A comparison graph showing how your Identity secure score compares to other tenants in the same industry and similar size
- A trend graph showing how your Identity secure score has changed over time
- A list of possible improvements

By following the improvement actions, you can:

- Improve your security posture and your score
- Take advantage the features available to your organization as part of your identity investments

How do I get my secure score?

The identity secure score is available in all editions of Azure AD. Organizations can access their identity secure score from the [Azure portal > Azure Active Directory > Security > Identity Secure Score](#).

How does it work?

Every 48 hours, Azure looks at your security configuration and compares your settings with the recommended best practices. Based on the outcome of this evaluation, a new score is calculated for your directory. It's possible that your security configuration isn't fully aligned with the best practice guidance and the improvement actions are only partially met. In these scenarios, you will only be awarded a portion of the max score available for the control.

Each recommendation is measured based on your Azure AD configuration. If you are using third-party products to enable a best practice recommendation, you can indicate this configuration in the settings of an improvement action. You also have the option to set recommendations to be ignored if they don't apply to your environment. An ignored recommendation does not contribute to the calculation of your score.

The screenshot shows a card titled 'Improvement action' for the recommendation 'Use limited administrative roles'. The card includes the following details:

- SCORE IMPACT**: +1.79%
- CURRENT SCORE**: 1
- MAX SCORE**: 1
- STATUS**: A dropdown menu with the following options:
 - To address (selected)
 - To address
 - Risk accepted
 - Planned
 - Resolved through third party
 - Resolved through alternate mitigation
- USER IMPACT**: Low
- IMPLEMENTATION COST**: Low
- WHAT AM I ABOUT TO CHANGE?**: Reduce the number of persistent global administrator roles
- A note: "Secure score updates can take up to 48 hours."
- Save** button at the bottom

- **To address** - You recognize that the improvement action is necessary and plan to address it at some point in the future. This state also applies to actions that are detected as partially, but not fully completed.
- **Planned** - There are concrete plans in place to complete the improvement action.
- **Risk accepted** - Security should always be balanced with usability, and not every recommendation will work for your environment. When that is the case, you can choose to accept the risk, or the remaining risk, and not enact the improvement action. You won't be given any points, but the action will no longer be visible in the list of improvement actions. You can view this action in history or undo it at any time.

- **Resolved through third party** and **Resolved through alternate mitigation** - The improvement action has already been addressed by a third-party application or software, or an internal tool. You'll gain the points that the action is worth, so your score better reflects your overall security posture. If a third party or internal tool no longer covers the control, you can choose another status. Keep in mind, Microsoft will have no visibility into the completeness of implementation if the improvement action is marked as either of these statuses.

How does it help me?

The secure score helps you to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

What you should know

Who can use the identity secure score?

The identity secure score can be used by the following roles:

- Global admin
- Security admin
- Security readers

How are controls scored?

Controls can be scored in two ways. Some are scored in a binary fashion - you get 100% of the score if you have the feature or setting configured based on our recommendation. Other scores are calculated as a percentage of the total configuration. For example, if the improvement recommendation states you'll get a maximum of 10.71% if you protect all your users with MFA and you only have 5 of 100 total users protected, you would be given a partial score around 0.53% ($5 \text{ protected} / 100 \text{ total} * 10.71\% \text{ maximum} = 0.53\% \text{ partial score}$).

What does [Not Scored] mean?

Actions labeled as [Not Scored] are ones you can perform in your organization but won't be scored because they aren't hooked up in the tool (yet!). So, you can still improve your security, but you won't get credit for those actions right now.

How often is my score updated?

The score is calculated once per day (around 1:00 AM PST). If you make a change to a measured action, the score will automatically update the next day. It takes up to 48 hours for a change to be reflected in your score.

My score changed. How do I figure out why?

Head over to the [Microsoft 365 Defender portal](#), where you'll find your complete Microsoft secure score. You can easily see all the changes to your secure score by reviewing the in-depth changes on the history tab.

Does the secure score measure my risk of getting breached?

In short, no. The secure score does not express an absolute measure of how likely you are to get breached. It expresses the extent to which you have adopted features that can offset the risk of being breached. No service can guarantee that you will not be breached, and the secure score should not be interpreted as a guarantee in any way.

How should I interpret my score?

Your score improves for configuring recommended security features or performing security-related tasks (like reading reports). Some actions are scored for partial completion, like enabling multi-factor authentication (MFA) for your users. Your secure score is directly representative of the Microsoft security services you use. Remember

that security must be balanced with usability. All security controls have a user impact component. Controls with low user impact should have little to no effect on your users' day-to-day operations.

To see your score history, head over to the [Microsoft 365 Defender portal](#) and review your overall Microsoft secure score. You can review changes to your overall secure score by clicking on View History. Choose a specific date to see which controls were enabled for that day and what points you earned for each one.

How does the identity secure score relate to the Microsoft 365 secure score?

The [Microsoft secure score](#) contains five distinct control and score categories:

- Identity
- Data
- Devices
- Infrastructure
- Apps

The identity secure score represents the identity part of the Microsoft secure score. This overlap means that your recommendations for the identity secure score and the identity score in Microsoft are the same.

Next steps

[Find out more about Microsoft secure score](#)

Rapidly respond to secure identities with Azure AD

4/10/2022 • 11 minutes to read • [Edit Online](#)

It can seem daunting trying to secure your workers in today's world, especially when you have to respond rapidly and provide access to many services quickly. This article is meant to provide a concise list of all the actions to take, helping you identify and prioritize which order to deploy the Azure AD features based on the license type you own. Azure AD offers many features and provides many layers of security for your Identities, navigating which feature is relevant can sometimes be overwhelming. Many organizations are already in the cloud or moving quickly to the cloud, this document is intended to allow you to deploy services quickly, with securing your identities as the primary consideration.

Each table provides a consistent security recommendation, protecting both Administrator and User identities from the main security attacks (breach replay, phishing, and password spray) while minimizing the user impact and improving the user experience.

The guidance will also allow administrators to configure access to SaaS and on-premises applications in a secure and protected manner and is applicable to either cloud or hybrid (synced) identities and applies to users working remotely or in the office.

This checklist will help you quickly deploy critical recommended actions to protect your organization immediately by explaining how to:

- Strengthen your credentials.
- Reduce your attack surface area.
- Automate threat response.
- Utilize cloud intelligence.
- Enable end-user self-service.

Prerequisites

This guide assumes that your cloud only or hybrid identities have been established in Azure AD already. For help with choosing your identity type see the article, [Choose the right authentication method for your Azure Active Directory hybrid identity solution](#)

Summary

There are many aspects to a secure identity infrastructure, but this checklist focuses on a safe and secure identity infrastructure enabling users to work remotely. Securing your identity is just part of your security story, protecting data, applications, and devices should also be considered.

Guidance for Azure AD Free, Office 365, or Microsoft 365 customers.

There are a number of recommendations that Azure AD Free, Office 365, or Microsoft 365 app customers should take to protect their user identities, the following table is intended to highlight the key actions for the following license subscriptions:

- Office 365 (Office 365 E1, E3, E5, F1, A1, A3, A5)
- Microsoft 365 (Business Basic, Apps for Business, Business Standard, Business Premium, A1)
- Azure AD Free (included with Azure, Dynamics 365, Intune, and Power Platform)

RECOMMENDED ACTION	DETAIL
Enable Security Defaults	Protect all user identities and applications by enabling MFA and blocking legacy authentication
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials.)
Enable ADFS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Azure Active Directory smart lockout (if using managed identities)	Smart lockout assists in locking out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Disable end-user consent to applications	The admin consent workflow gives admins a secure way to grant access to applications that require admin approval so end users do not expose corporate data. Microsoft recommends disabling future user consent operations to help reduce your surface area and mitigate this risk.
Integrate supported SaaS applications from the gallery to Azure AD and enable Single sign on	Azure AD has a gallery that contains thousands of pre-integrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS applications remotely and securely with improved user experience (SSO)
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable)	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Azure AD with your existing application delivery controller or network.
Enable self-service password reset (applicable to cloud only accounts)	This ability reduces help desk calls and loss of productivity when a user cannot sign into their device or an application.
Use non-global administrative roles where possible	Give your administrators only the access they need to only the areas they need access to. Not all administrators need to be global administrators.
Enable Microsoft's password guidance	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.

Guidance for Azure AD Premium Plan 1 customers.

The following table is intended to highlight the key actions for the following license subscriptions:

- Azure Active Directory Premium P1 (Azure AD P1)
- Enterprise Mobility + Security (EMS E3)
- Microsoft 365 (M365 E3, A3, F1, F3)

Recommended Action	Detail
Enable combined registration experience for Azure AD MFA and SSPR to simplify user registration experience	Allow your users to register from one common experience for both Azure AD Multi-Factor Authentication and self-service password reset.
Configure MFA settings for your organization	Ensure accounts are protected from being compromised with multi-factor authentication
Enable self-service password reset	This ability reduces help desk calls and loss of productivity when a user cannot sign into their device or an application
Implement Password Writeback (if using hybrid identities)	Allow password changes in the cloud to be written back to an on-premises Windows Server Active Directory environment.
Create and enable Conditional Access policies	<p>MFA for admins to protect accounts that are assigned administrative rights.</p> <p>Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols.</p> <p>MFA for all users and applications to create a balanced MFA policy for your environment, securing your users and applications.</p> <p>Require MFA for Azure Management to protect your privileged resources by requiring multi-factor authentication for any user accessing Azure resources.</p>
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials.)
Enable ADFS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Azure Active Directory smart lockout (if using managed identities)	Smart lockout assists in locking out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Disable end-user consent to applications	The admin consent workflow gives admins a secure way to grant access to applications that require admin approval so end users do not expose corporate data. Microsoft recommends disabling future user consent operations to help reduce your surface area and mitigate this risk.
Enable remote access to on-premises legacy applications with Application Proxy	Enable Azure AD Application Proxy and integrate with legacy apps for users to securely access on-premises applications by signing in with their Azure AD account.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable).	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Azure AD with your existing application delivery controller or network.

RECOMMENDED ACTION	DETAIL
Integrate supported SaaS applications from the gallery to Azure AD and enable Single sign on	Azure AD has a gallery that contains thousands of pre-integrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS applications remotely and securely with improved user experience (SSO).
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Conditional Access – Device based	Improve security and user experiences with device-based Conditional Access. This step ensures users can only access from devices that meet your standards for security and compliance. These devices are also known as managed devices. Managed devices can be Intune compliant or Hybrid Azure AD joined devices.
Enable Password Protection	Protect users from using weak and easy to guess passwords.
Designate more than one global administrator	Assign at least two cloud-only permanent global administrator accounts for use if there is an emergency. These accounts are not be used daily and should have long and complex passwords. Break Glass Accounts ensure you can access the service in an emergency.
Use non-global administrative roles where possible	Give your administrators only the access they need to only the areas they need access to. Not all administrators need to be global administrators.
Enable Microsoft's password guidance	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.
Create a plan for guest user access	Collaborate with guest users by letting them sign into your apps and services with their own work, school, or social identities.

Guidance for Azure AD Premium Plan 2 customers.

The following table is intended to highlight the key actions for the following license subscriptions:

- Azure Active Directory Premium P2 (Azure AD P2)
- Enterprise Mobility + Security (EMS E5)
- Microsoft 365 (M365 E5, A5)

RECOMMENDED ACTION	DETAIL
Enable combined registration experience for Azure AD MFA and SSPR to simplify user registration experience	Allow your users to register from one common experience for both Azure AD Multi-Factor Authentication and self-service password reset.

Recommended Action	Detail
Configure MFA settings for your organization	Ensure accounts are protected from being compromised with multi-factor authentication
Enable self-service password reset	This ability reduces help desk calls and loss of productivity when a user cannot sign into their device or an application
Implement Password Writeback (if using hybrid identities)	Allow password changes in the cloud to be written back to an on-premises Windows Server Active Directory environment.
Enable Identity Protection policies to enforce MFA registration	Manage the roll-out of Azure AD Multi-Factor Authentication (MFA).
Enable Identity Protection user and sign-in risk policies	Enable Identity Protection User and Sign-in policies. The recommended sign-in policy is to target medium risk sign-ins and require MFA. For User policies it should target high risk users requiring the password change action.
<p>Create and enable Conditional Access policies</p> <p>MFA for admins to protect accounts that are assigned administrative rights</p> <p>Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols</p> <p>Require MFA for Azure Management to protect your privileged resources by requiring multi-factor authentication for any user accessing Azure resources</p>	
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials.)
Enable ADFS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Azure Active Directory smart lockout (if using managed identities)	Smart lockout assists in locking out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Disable end-user consent to applications	The admin consent workflow gives admins a secure way to grant access to applications that require admin approval so end users do not expose corporate data. Microsoft recommends disabling future user consent operations to help reduce your surface area and mitigate this risk.
Enable remote access to on-premises legacy applications with Application Proxy	Enable Azure AD Application Proxy and integrate with legacy apps for users to securely access on-premises applications by signing in with their Azure AD account.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable).	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Azure AD with your existing application delivery controller or network.

RECOMMENDED ACTION	DETAIL
Integrate supported SaaS applications from the gallery to Azure AD and enable Single sign on	Azure AD has a gallery that contains thousands of pre-integrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS applications remotely and securely with improved user experience (SSO).
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Conditional Access – Device based	Improve security and user experiences with device-based Conditional Access. This step ensures users can only access from devices that meet your standards for security and compliance. These devices are also known as managed devices. Managed devices can be Intune compliant or Hybrid Azure AD joined devices.
Enable Password Protection	Protect users from using weak and easy to guess passwords.
Designate more than one global administrator	Assign at least two cloud-only permanent global administrator accounts for use if there is an emergency. These accounts are not be used daily and should have long and complex passwords. Break Glass Accounts ensure you can access the service in an emergency.
Use non-global administrative roles where possible	Give your administrators only the access they need to only the areas they need access to. Not all administrators need to be global administrators.
Enable Microsoft's password guidance	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.
Create a plan for guest user access	Collaborate with guest users by letting them sign into your apps and services with their own work, school, or social identities.
Enable Privileged Identity Management	Enables you to manage, control, and monitor access to important resources in your organization, ensuring admins have access only when needed and with approval

Next steps

- For detailed deployment guidance for individual features of Azure AD, review the [Azure AD project deployment plans](#).
- For an end-to-end Azure AD deployment checklist, see the article [Azure Active Directory feature deployment guide](#)

Sign up your organization to use Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Sign up for Azure Active Directory (Azure AD) or a new Microsoft Azure subscription, using either:

- **Microsoft account.** Use your personal Microsoft account to get access to Azure and all consumer-oriented Microsoft products and cloud services, such as Outlook (Hotmail), Messenger, OneDrive, MSN, Xbox LIVE, or Microsoft 365. Signing up for an Outlook.com mailbox automatically creates a Microsoft account. For more information, see [Microsoft account overview](#).
- **Work or school account.** Use your work or school-related account to get access to all the small, medium, and enterprise cloud services from Microsoft, such as Azure, Microsoft Intune, or Microsoft 365. After you sign up for one of these services as an organization, Azure AD automatically provisions a cloud-based directory that represents your organization. For more information, see [Manage your Azure AD directory](#).

NOTE

We recommend that you use your work or school account if you already have access to Azure AD. However, you should use whichever type of account is associated with your Azure subscription.

Next steps

- [How to buy Azure](#)
- [Sign up for Azure Active Directory Premium editions](#)
- [Learn more about Azure AD](#)
- [Use your on-premises identity infrastructure in the cloud](#)
- [Visit the Microsoft Azure blog](#)

Sign up for Azure Active Directory Premium editions

4/10/2022 • 3 minutes to read • [Edit Online](#)

You can purchase and associate Azure Active Directory (Azure AD) Premium editions with your Azure subscription. If you need to create a new Azure subscription, you'll also need to activate your licensing plan and Azure AD service access.

Before you sign up for Active Directory Premium 1 or Premium 2, you must first determine which of your existing subscription or plan to use:

- Through your existing Azure or Microsoft 365 subscription
- Through your Enterprise Mobility + Security licensing plan
- Through a Microsoft Volume Licensing plan

Signing up using your Azure subscription with previously purchased and activated Azure AD licenses, automatically activates the licenses in the same directory. If that's not the case, you must still activate your license plan and your Azure AD access. For more information about activating your license plan, see [Activate your new license plan](#). For more information about activating your Azure AD access, see [Activate your Azure AD access](#).

Sign up using your existing Azure or Microsoft 365 subscription

As an Azure or Microsoft 365 subscriber, you can purchase the Azure Active Directory Premium editions online. For detailed steps, see [How to Purchase Azure Active Directory Premium - New Customers](#).

Sign up using your Enterprise Mobility + Security licensing plan

Enterprise Mobility + Security is a suite, comprised of Azure AD Premium, Azure Information Protection, and Microsoft Intune. If you already have an EMS license, you can get started with Azure AD, using one of these licensing options:

For more information about EMS, see [Enterprise Mobility + Security web site](#).

- Try out EMS with a free [Enterprise Mobility + Security E5 trial subscription](#)
- Purchase [Enterprise Mobility + Security E5 licenses](#)
- Purchase [Enterprise Mobility + Security E3 licenses](#)

Sign up using your Microsoft Volume Licensing plan

Through your Microsoft Volume Licensing plan, you can sign up for Azure AD Premium using one of these two programs, based on the number of licenses you want to get:

- **For 250 or more licenses.** [Microsoft Enterprise Agreement](#)
- **For 5 to 250 licenses.** [Open Volume License](#)

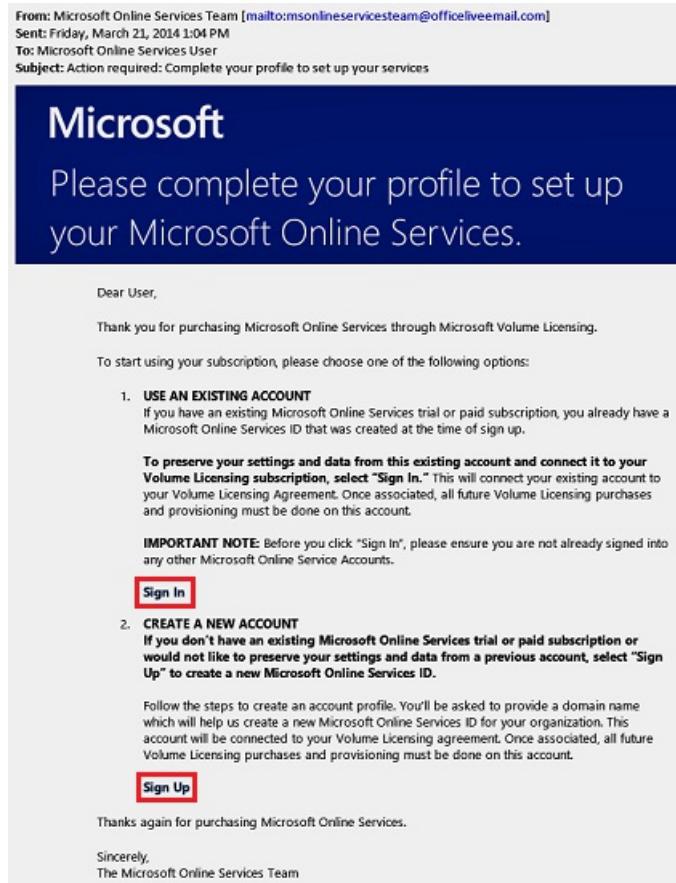
For more information about volume licensing purchase options, see [How to purchase through Volume Licensing](#).

Activate your new license plan

If you signed up using a new Azure AD license plan, you must activate it for your organization, using the confirmation email sent after purchase.

To activate your license plan

- Open the confirmation email you received from Microsoft after you signed up, and then click either **Sign In** or **Sign Up**.



- Sign in.** Choose this link if you have an existing tenant, and then sign in using your existing administrator account. You must be a global administrator on the tenant where the licenses are being activated.
- Sign up.** Choose this link if you want to open the **Create Account Profile** page and create a new Azure AD tenant for your licensing plan.

Create Account Profile

If your company is already using Microsoft Online Services for services such as Microsoft Office 365, we recommend that you use the same user ID to sign up for Windows Intune. Learn more about why it is important to sign up with the same User ID. Sign in

* Required

* Country or region: United States
Can't be changed after signup. Why?

* Organization language: English

* First name: myfirstname

* Last name: mylastname

* Organization name: domoorg4

* Address 1: one microsoft way

Address 2:

* City: redmond

* State: Washington

* ZIP code: 98052

* Phone number: 4252222222

* Email address: amyrotest@live.com

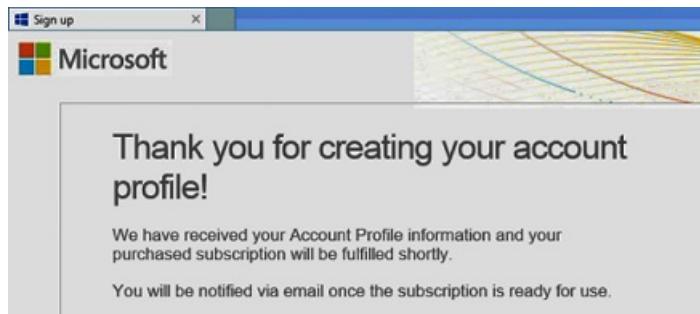
* New domain name: do101010 .ccscstp.net Check availability

Start Using your Online Service Solution!

Get started now by following these simple steps:

- Complete your customer profile
- Select a unique domain name
- Create your new user ID you will use each time to sign-in to the service
- Create a new password
- As an option, you can select among contact options where Microsoft can provide you information and offers
- Upon submission of the form, a confirmation email will be sent to the email address you provided

When you're done, you will see a confirmation box thanking you for activating the license plan for your tenant.



Activate your Azure AD access

If you're adding new Azure AD Premium licenses to an existing subscription, your Azure AD access should already be activated. Otherwise, you need to activate Azure AD access after you receive the **Welcome email**.

After your purchased licenses are provisioned in your directory, you'll receive a **Welcome email**. This email confirms that you can start managing your Azure AD Premium or Enterprise Mobility + Security licenses and features.

TIP

You won't be able to access Azure AD for your new tenant until you activate Azure AD directory access from the welcome email.

To activate your Azure AD access

1. Open the **Welcome email**, and then click **Sign In**.

From: Microsoft Online Services Team [mailto:msonlineserviceteam@officeliveemail.com]
Sent: Tuesday, March 25, 2014 10:07 AM
To: Microsoft Azure Active Directory User
Subject: Get started with your Windows Azure Active Directory Premium!

Microsoft Azure

Welcome to your Azure Active Directory

GET STARTED TODAY

Organization: AAD.Premium

Sign in to get started!

Sign in

<http://go.microsoft.com/fwlink/?LinkId=393623>

User ID ([What is this?](#))

Name: AAD Premium

User ID: admin@aadpremium.csctp.net

Your organization now has access to Windows Azure Active Directory Premium, Microsoft's cloud identity and access management service. Sign in with your User ID and start building directory and access management in the cloud, configure seamless sign-in to cloud resources and enhance application access security.

Thank you for choosing Windows Azure Active Directory Premium through Microsoft Volume Licensing. We look forward to helping your organization get the most value from your subscription.

Sincerely,
The Windows Azure Active Directory Team

- After successfully signing in, you'll go through two-step verification using a mobile device.

The screenshot shows the Microsoft Azure sign-up interface. On the left, there's a blue sidebar with the title "Sign up" and "Access to Azure Active Directory". Below this, there's a "Learn more" button and some decorative white clouds against a blue background. On the right, the main form is titled "Microsoft Azure". It has two sections: "1 About you" and "2 Mobile verification". In section 1, fields for "FIRST NAME" (Lorna), "LAST NAME" (Garner), and "COUNTRY/REGION" (United States) are filled out. In section 2, under "Mobile verification", there are options for "Send text message" (selected) or "Call me", a dropdown for "United States (+1)", a text input for "(425) 555-0100", and a green "Send text message" button. At the bottom of section 2 is a grey "Sign up" button with a circular arrow icon.

The activation process typically takes only a few minutes and then you can use your Azure AD tenant.

Next steps

Now that you have Azure AD Premium, you can [customize your domain](#), add your [corporate branding](#), create a [tenant](#), and [add groups](#) and [users](#).

Add your custom domain name using the Azure Active Directory portal

4/10/2022 • 4 minutes to read • [Edit Online](#)

Every new Azure AD tenant comes with an initial domain name, <domainname>.onmicrosoft.com. You can't change or delete the initial domain name, but you can add your organization's names. Adding custom domain names helps you to create user names that are familiar to your users, such as *alain@contoso.com*.

Before you begin

Before you can add a custom domain name, create your domain name with a domain registrar. For an accredited domain registrar, see [ICANN-Accredited Registrars](#).

Create your directory in Azure AD

After you get your domain name, you can create your first Azure AD directory. Sign in to the Azure portal for your directory, using an account with the **Owner** role for the subscription.

Create your new directory by following the steps in [Create a new tenant for your organization](#).

IMPORTANT

The person who creates the tenant is automatically the Global administrator for that tenant. The Global administrator can add additional administrators to the tenant.

For more information about subscription roles, see [Azure roles](#).

TIP

If you plan to federate your on-premises Windows Server AD with Azure AD, then you need to select **I plan to configure this domain for single sign-on with my local Active Directory** when you run the Azure AD Connect tool to synchronize your directories.

You also need to register the same domain name you select for federating with your on-premises directory in the **Azure AD Domain** step in the wizard. To see what that setup looks like, see [Verify the Azure AD domain selected for federation](#). If you don't have the Azure AD Connect tool, you can [download it here](#).

Add your custom domain name to Azure AD

After you create your directory, you can add your custom domain name.

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Search for and select *Azure Active Directory* from any page. Then select **Custom domain names > Add custom domain**.

The screenshot shows the 'Custom domain names' section of the Azure Active Directory portal. The left sidebar includes links for Overview, Getting started, Manage (Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, Application proxy, Licenses, Azure AD Connect), and Custom domain names. The main area has a search bar, a 'Add custom domain' button (highlighted with a red box), and a troubleshoot link. A tooltip message says: 'Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?'. A table lists the domain 'fabrikam.onmicrosoft.com' with columns for NAME, STATUS (Available), FEDERATED (Yes), and PRIMARY (Yes).

3. In **Custom domain name**, enter your organization's new name, in this example, *contoso.com*. Select **Add domain**.

The screenshot shows the 'Custom domain name' configuration page. It displays the domain 'contoso.com' in the input field, which is highlighted with a purple box. The 'Add Domain' button at the bottom is highlighted with a red box.

IMPORTANT

You must include *.com*, *.net*, or any other top-level extension for this to work properly.

The unverified domain is added. The **contoso.com** page appears showing your DNS information. Save this information. You need it later to create a TXT record to configure DNS.

To use contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE **TXT** **MX**

ALIAS OR HOST NAME @

DESTINATION OR POINTS TO ADDRESS MS=ms64983159

TTL 3600

[Share these settings via email](#)

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

Add your DNS information to the domain registrar

After you add your custom domain name to Azure AD, you must return to your domain registrar and add the Azure AD DNS information from your copied TXT file. Creating this TXT record for your domain verifies ownership of your domain name.

Go back to your domain registrar and create a new TXT record for your domain based on your copied DNS information. Set the time to live (TTL) to 3600 seconds (60 minutes), and then save the record.

IMPORTANT

You can register as many domain names as you want. However, each domain gets its own TXT record from Azure AD. Be careful when you enter the TXT file information at the domain registrar. If you enter the wrong or duplicate information by mistake, you'll have to wait until the TTL times out (60 minutes) before you can try again.

Verify your custom domain name

After you register your custom domain name, make sure it's valid in Azure AD. The propagation from your domain registrar to Azure AD can be instantaneous or it can take a few days, depending on your domain registrar.

To verify your custom domain name, follow these steps:

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Search for and select *Azure Active Directory* from any page, then select **Custom domain names**.
3. In **Custom domain names**, select the custom domain name. In this example, select **contoso.com**.

NAME	STATUS	FEDERATED	PRIMARY
contoso.com	⚠️ Unverified		
fabrikam.onmicrosoft.com	✓ Available		✓

- On the **contoso.com** page, select **Verify** to make sure your custom domain is properly registered and is valid for Azure AD.

contoso.com
Custom domain name

Delete

To use contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE	TXT	MX
ALIAS OR HOST NAME	@	
DESTINATION OR POINTS TO ADDRESS	MS=ms64983159	
TTL	3600	

[Share these settings via email](#)

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

After you've verified your custom domain name, you can delete your verification TXT or MX file.

Common verification issues

If Azure AD can't verify a custom domain name, try the following suggestions:

- Wait at least an hour and try again.** DNS records must propagate before Azure AD can verify the domain. This process can take an hour or more.
- If you are trying to verify a child domain, verify the parent domain first.** Make sure the parent domain is created and verified first before you try to verify child domain.
- Make sure the DNS record is correct.** Go back to the domain name registrar site. Make sure the entry is there, and that it matches the DNS entry information provided by Azure AD.

If you can't update the record on the registrar site, share the entry with someone who has permissions to

add the entry and verify it's correct.

- **Make sure the domain name isn't already in use in another directory.** A domain name can only be verified in one directory. If your domain name is currently verified in another directory, it can't also be verified in the new directory. To fix this duplication problem, you must delete the domain name from the old directory. For more information about deleting domain names, see [Manage custom domain names](#).
- **Make sure you don't have any unmanaged Power BI tenants.** If your users have activated Power BI through self-service sign-up and created an unmanaged tenant for your organization, you must take over management as an internal or external admin, using PowerShell. For more information, see [Take over an unmanaged directory as administrator in Azure Active Directory](#).

Next steps

- Add another Global administrator to your directory. For more information, see [How to assign roles and administrators](#).
- Add users to your domain. For more information, see [How to add or delete users](#).
- Manage your domain name information in Azure AD. For more information, see [Managing custom domain names](#).
- If you have on-premises versions of Windows Server that you want to use alongside Azure Active Directory, see [Integrate your on-premises directories with Azure Active Directory](#).

Add branding to your organization's Azure Active Directory sign-in page

4/10/2022 • 7 minutes to read • [Edit Online](#)

Use your organization's logo and custom color schemes to provide a consistent look-and-feel on your Azure Active Directory (Azure AD) sign-in pages. Your sign-in pages appear when users sign in to your organization's web-based apps, such as Microsoft 365, which uses Azure AD as your identity provider.

NOTE

Adding custom branding requires you to have either Azure Active Directory Premium 1, Premium 2, or Office 365 (for Office 365 apps) licenses. For more information about licensing and editions, see [Sign up for Azure AD Premium](#).

Azure AD Premium editions are available for customers in China using the worldwide instance of Azure Active Directory. Azure AD Premium editions aren't currently supported in the Azure service operated by 21Vianet in China. For more information, talk to us using the [Azure Active Directory Forum](#).

Customize your Azure AD sign-in page

You can customize your Azure AD sign-in pages, which appear when users sign in to your organization's tenant-specific apps, such as <https://outlook.com/contoso.com>, or when passing a domain variable, such as

<https://passwordreset.microsoftonline.com/?whr=contoso.com>.

Your custom branding won't immediately appear when your users go to sites such as, www.office.com. Instead, the user has to sign-in before your customized branding appears. After the user has signed in, the branding may take 15 minutes or longer to appear.

NOTE

All branding elements are optional and will remain default when unchanged. For example, if you specify a banner logo with no background image, the sign-in page will show your logo with a default background image from the destination site such as Microsoft 365.

Additionally, sign-in page branding doesn't carry over to personal Microsoft accounts. If your users or business guests sign in using a personal Microsoft account, the sign-in page won't reflect the branding of your organization.

To configure your branding for the first time

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **Configure**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a dark sidebar with various service icons like App Services, Function Apps, SQL databases, Virtual machines, and Azure Active Directory. The 'Azure Active Directory' icon is highlighted. The main content area has a header 'Contoso - Company branding' under 'Azure Active Directory'. Below the header is a search bar and a 'Configure' button, which is highlighted with a red box. A status message 'STATUS: Not configured' is displayed. To the right of the status is a descriptive text: 'Configure the text and graphics your users see when they sign in to Azure Active Directory.' A vertical sidebar on the left lists management options: Overview, Getting started, Manage (with sub-options: Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset), and Company branding.

3. On the **Configure company branding** page, provide any or all of the following information.

IMPORTANT

All the custom images you add on this page have image size (pixels), and potentially file size (KB), restrictions. Because of these restrictions, you'll most-likely need to use a photo editor to create the right-sized images.

- General settings

Configure company branding

Contoso



Save

Discard

Delete

Language

Default



Sign-in page background image

Image size: 1920x1080px

File size: <300KB

File type: PNG or JPG

Remove

 Select a file**Microsoft**

Remove

 Select a file

Banner logo

Image size: 280x60px

File size: 10KB

File type: Transparent PNG or JPG

Username hint

 Forgot your username?

Sign-in page text

 If you need help, contact the Help Desk online at www.contoso.com/helpdesk.

- **Language.** The language is automatically set as your default and can't be changed.
- **Sign-in page background image.** Select a .png or .jpg image file to appear as the background for your sign-in pages. The image will be anchored to the center of the browser, and will scale to the size of the viewable space. You can't select an image larger than 1920x1080 pixels in size or that has a file size more than 300,000 bytes.
It's recommended to use images without a strong subject focus, e.g., an opaque white box appears in the center of the screen, and could cover any part of the image depending on the dimensions of the viewable space.
- **Banner logo.** Select a .png or .jpg version of your logo to appear on the sign-in page after the user enters a username and on the **My Apps** portal page.
The image can't be taller than 60 pixels or wider than 280 pixels, and the file shouldn't be larger than 10KB. We recommend using a transparent image since the background might not match your logo background. We also recommend not adding padding around the image or it might make your logo look small.
- **Username hint.** Type the hint text that appears to users if they forget their username. This text must be Unicode, without links or code, and can't exceed 64 characters. If guests sign in to your app, we suggest not adding this hint.
- **Sign-in page text and formatting.** Type the text that appears on the bottom of the sign-in page. You can use this text to communicate additional information, such as the phone number to your help desk or a legal statement. This text must be Unicode and not exceed 1024 characters.

You can customize the sign-in page text you entered. To begin a new paragraph, use the enter key twice. You can also change text formatting to include bold, italics, an underline or clickable link. Use the following syntax to add formatting to text:

Hyperlink: [text](link)

Bold: **text** or __text__

Italics: *text* or _text_

Underline: ++text++

IMPORTANT

Hyperlinks that are added with sign-in page text render as text in native environments, like in desktop and mobile applications.

• Advanced settings

Advanced settings

Sign-in page background color ⓘ #FFFFFF ✓

Square logo image
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG ⓘ

Select a file Remove

Square logo image, dark theme
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG ⓘ

Select a file Remove

Show option to remain signed in ⓘ Yes No

- **Sign-in page background color.** Specify the hexadecimal color (for example, white is #FFFFFF) that will appear in place of your background image in low-bandwidth connection situations. We recommend using the primary color of your banner logo or your organization color.
- **Square logo image.** Select a .png (preferred) or .jpg image of your organization's logo to appear to users during the setup process for new Windows 10 Enterprise devices. This image is only used for Windows authentication and appears only on tenants that are using [Windows Autopilot](#) for deployment or for password entry pages in other Windows 10 experiences. In some cases it may also appear in the consent dialog.

The image can't be larger than 240x240 pixels in size and must have a file size of less than 10 KB. We recommend using a transparent image since the background might not match your logo background. We also recommend not adding padding around the image or it might make your logo look small.

- **Square logo image, dark theme.** Same as the square logo image above. This logo image takes the place of the square logo image when used with a dark background, such as with Windows 10 Azure AD joined screens during the out-of-box experience (OOBE). If your logo looks good on white, dark blue, and black backgrounds, you don't need to add this image.

IMPORTANT

Transparent logos are supported with the square logo image. However, the color palette used in the transparent logo could conflict with backgrounds (such as, white, light grey, dark grey, and black backgrounds) used within Microsoft 365 apps and services that consume the square logo image. Solid color backgrounds may need to be used to ensure the square image logo is rendered correctly in all situations.

- **Show option to remain signed in.** You can choose to let your users remain signed in to Azure AD until explicitly signing out. If you choose **No**, this option is hidden, and users must sign in each time the browser is closed and reopened.

This capability is only available on the default branding object and not on any language-specific object. To learn more about configuring and troubleshooting the option to remain signed in, see [Configure the 'Stay signed in?' prompt for Azure AD accounts](#)

NOTE

Some features of SharePoint Online and Office 2010 depend on users being able to choose to remain signed in. If you set this option to **No**, your users may see additional and unexpected prompts to sign-in.

4. After you've finished adding your branding, select **Save**.

This process creates your first custom branding configuration, and it becomes the default for your tenant. The default custom branding configuration serves as a fallback option for all language-specific branding configurations. The configuration can't be removed after you create it.

IMPORTANT

To add more corporate branding configurations to your tenant, you must choose **New language** on the **Contoso - Company branding** page. This opens the **Configure company branding** page, where you can follow the same steps as above.

Update your custom branding

After you've created your custom branding, you can go back and change anything you want.

To edit your custom branding

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **Configure**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like App Services, Function Apps, SQL databases, and Virtual machines. The main area is titled 'Contoso - Company branding' under 'Configure company branding'. At the top, there's a search bar and some navigation icons. Below the title, there's a table with columns: LOCALE, BACKGROUND IMAGE, BANNER LOGO, USERNAME HINT, and SIGN-IN PAGE TEXT. A single row is shown for 'Default', with green checkmarks in the first three columns. The 'SIGN-IN PAGE TEXT' column contains the text 'Forgot your username? If you need help, contact the Help Desk online at www.contoso.com/helpdesk.' A red box highlights the '+ New language' button in the top right of the main content area.

3. On the **Configure company branding** page, add, remove, or change any of the information, based on the descriptions in the [Customize your Azure AD sign-in page](#) section of this article.

4. Select **Save**.

It can take up to an hour for any changes you made to the sign-in page branding to appear.

Add language-specific company branding to your directory

You can't change your original configuration's language from your default language. However, if you need a configuration in a different language, you can create a new configuration.

To add a language-specific branding configuration

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **New language**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like App Services, Function Apps, SQL databases, and Virtual machines. The main area is titled 'Contoso - Company branding' under 'Configure company branding'. At the top, there's a search bar and some navigation icons. Below the title, there's a table with columns: LOCALE, BACKGROUND IMAGE, BANNER LOGO, USERNAME HINT, and SIGN-IN PAGE TEXT. A single row is shown for 'Default', with green checkmarks in the first three columns. The 'SIGN-IN PAGE TEXT' column contains the text 'Forgot your username? If you need help, contact the Help Desk online at www.contoso.com/helpdesk.' A red box highlights the '+ New language' button in the top right of the main content area.

3. On the **Configure company branding** page, select your language (for example, French) and then add your translated information, based on the descriptions in the [Customize your Azure AD sign-in page](#) section of this article.

4. Select **Save**.

The Contoso – Company branding page updates to show your new French configuration.

The screenshot shows the Microsoft Azure portal's 'Company branding' configuration page. On the left, there's a sidebar with various service icons like App Services, SQL databases, and Virtual machines. The main area has a header 'Contoso - Company branding' and a sub-header 'Configure company branding'. Below this is a table with columns: LOCALE, BACKGROUND IMAGE, BANNER LOGO, USERNAME HINT, and SIGN-IN PAGE TEXT. There are two rows: 'Default' and 'français (France)'. The 'français (France)' row is highlighted with a red box. The 'BACKGROUND IMAGE' and 'BANNER LOGO' columns for this row show green checkmarks. The 'USERNAME HINT' column contains the text 'Forgot your username? If you need help, contact the Help Desk online at www.contoso.com/helpdesk.' The 'SIGN-IN PAGE TEXT' column contains the text 'Vous avez oublié votre nom ... Si vous avez besoin d'aide, contactez le service d'assistance en ligne à l'adr...'. At the top right of the main area, there are icons for search, refresh, and columns.

Add your custom branding to pages

Add your custom branding to pages by modifying the end of the URL with the text, `?whr=yourdomainname`. This specific modification works on different types of pages, including the Multi-Factor Authentication (MFA) setup page, the Self-service Password Reset (SSPR) setup page, and the sign in page.

Whether an application supports customized URLs for branding or not depends on the specific application, and should be checked before attempting to add a custom branding to a page.

Examples:

Original URL: <https://aka.ms/MFASetup>

Custom URL: <https://account.activedirectory.windowsazure.com/proofup.aspx?whr=contoso.com>

Original URL: <https://aka.ms/SSPR>

Custom URL: <https://passwordreset.microsoftonline.com/?whr=contoso.com>

Add your organization's privacy info using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

This article explains how a tenant admin can add privacy-related info to an organization's Azure Active Directory (Azure AD) tenant, through the Azure portal.

We strongly recommend you add both your global privacy contact and your organization's privacy statement, so your internal employees and external guests can review your policies. Because privacy statements are uniquely created and tailored for each business, we strongly recommend you contact a lawyer for assistance.

NOTE

For information about viewing or deleting personal data, see [Azure Data Subject Requests for the GDPR](#). For more information about GDPR, see the [GDPR section of the Microsoft Trust Center](#) and the [GDPR section of the Service Trust portal](#).

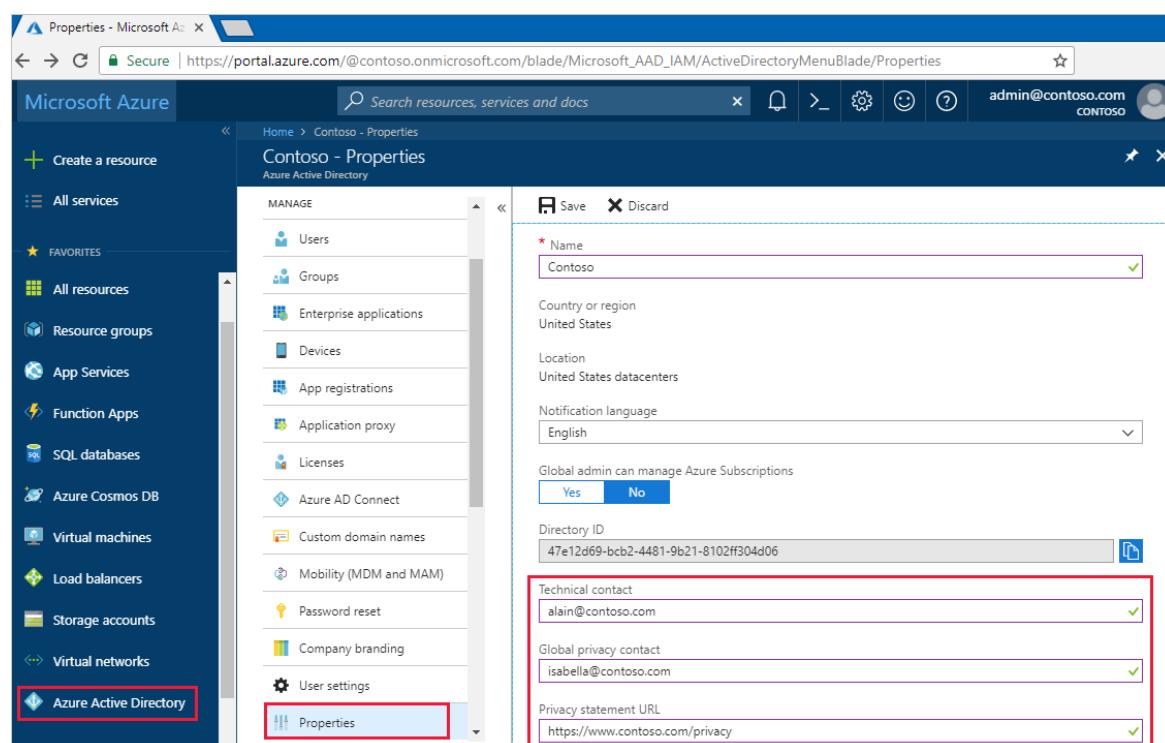
Add your privacy info on Azure AD

You add your organization's privacy information in the **Properties** area of Azure AD.

To access the Properties area and add your privacy information

1. Sign in to the Azure portal as a tenant administrator.
2. On the left navbar, select **Azure Active Directory**, and then select **Properties**.

The **Properties** area appears.



The screenshot shows the Azure portal interface with the URL https://portal.azure.com/@contoso.onmicrosoft.com/blade/Microsoft_AAD_JAM/ActiveDirectoryMenuBlade/Properties. The left sidebar has 'Azure Active Directory' selected. The main area is titled 'Contoso - Properties' under 'Azure Active Directory'. The 'Properties' tab is selected in the ribbon. The 'MANAGE' section on the left includes links for Users, Groups, Enterprise applications, Devices, App registrations, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, and User settings. The right pane shows fields for Name (Contoso), Country or region (United States), Location (United States datacenters), Notification language (English), Global admin can manage Azure Subscriptions (Yes), Directory ID (47e12d69-bcb2-4481-9b21-8102ff304d06), Technical contact (alain@contoso.com), Global privacy contact (isabella@contoso.com), and Privacy statement URL (<https://www.contoso.com/privacy>). A red box highlights the 'Technical contact' input field.

3. Add your privacy info for your employees:

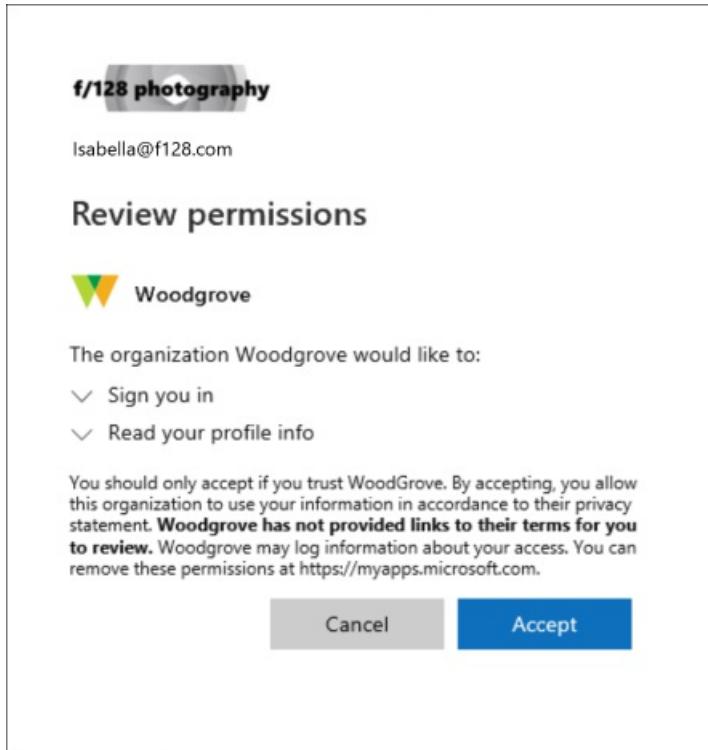
- **Technical contact.** Type the email address for the person to contact for technical support within

your organization.

- **Global privacy contact.** Type the email address for the person to contact for inquiries about personal data privacy. This person is also who Microsoft contacts if there's a data breach related to Azure Active Directory services . If there's no person listed here, Microsoft contacts your global administrators. For Microsoft 365 related privacy incident notifications please see [Microsoft 365 Message center FAQs](#)
- **Privacy statement URL.** Type the link to your organization's document that describes how your organization handles both internal and external guest's data privacy.

IMPORTANT

If you don't include either your own privacy statement or your privacy contact, your external guests will see text in the **Review Permissions** box that says, **<your org name> has not provided links to their terms for you to review**. For example, a guest user will see this message when they receive an invitation to access an organization through B2B collaboration.



4. Select **Save**.

Next steps

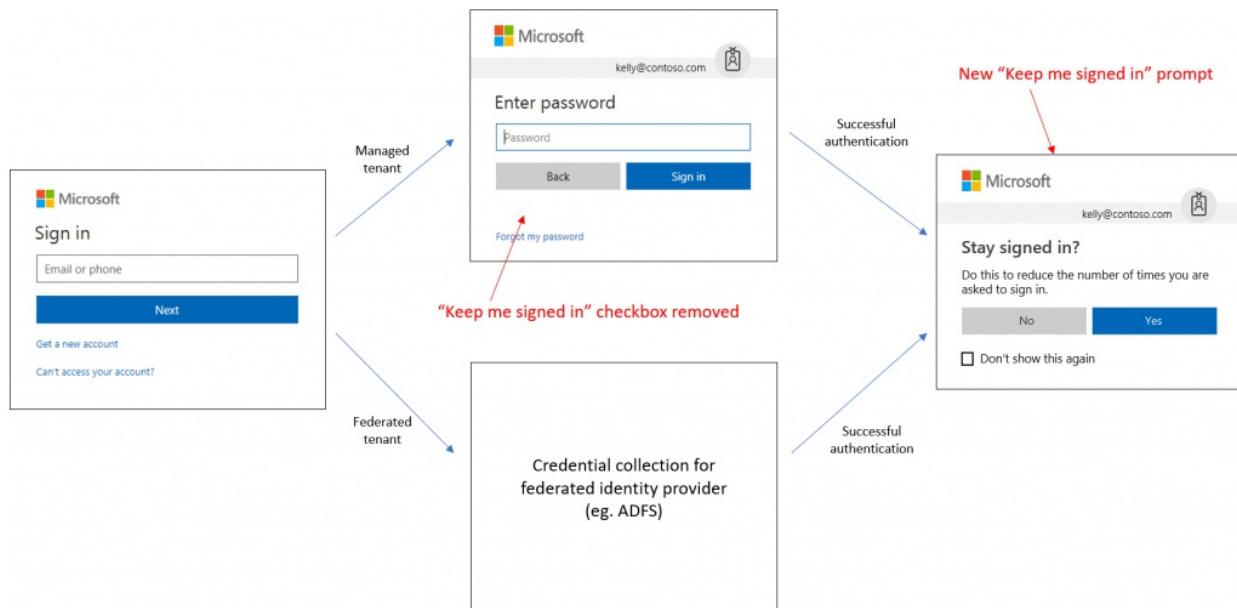
- [Azure Active Directory B2B collaboration invitation redemption](#)
- [Add or change profile information for a user in Azure Active Directory](#)

Configure the 'Stay signed in?' prompt for Azure AD accounts

4/10/2022 • 2 minutes to read • [Edit Online](#)

Keep me signed in (KMSI) displays a **Stay signed in?** prompt after a user successfully signs in. If a user answers **Yes** to this prompt, the keep me signed in service gives them a persistent [refresh token](#). For federated tenants, the prompt will show after the user successfully authenticates with the federated identity service.

The following diagram shows the user sign-in flow for a managed tenant and federated tenant and the new keep me signed in prompt. This flow contains smart logic so that the **Stay signed in?** option won't be displayed if the machine learning system detects a high-risk sign-in or a sign-in from a shared device.



NOTE

Configuring the keep me signed in option requires you to use Azure Active Directory (Azure AD) Premium 1, Premium 2, or Basic editions, or to have a Microsoft 365 license. For more information about licensing and editions, see [Sign up for Azure AD Premium](#).

Azure AD Premium and Basic editions are available for customers in China using the worldwide instance of Azure AD. Azure AD Premium and Basic editions aren't currently supported in the Azure service operated by 21Vianet in China. For more information, talk to us using the [Azure AD Forum](#).

Configure KMSI

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, select **Company branding**, and then select **Configure**.
3. In the **Advanced settings** section, find the **Show option to remain signed in** setting.

This setting lets you choose whether your users remain signed in to Azure AD until they explicitly sign out.

- If you choose **No**, the **Stay signed in?** option is hidden after the user successfully signs in and the

user must sign in each time the browser is closed and reopened.

- If you choose Yes, the Stay signed in? option is shown to the user.

Advanced settings

The screenshot shows the 'Advanced settings' section of the Azure Active Directory 'Sign-in' page. It includes fields for 'Sign-in page background color' set to #FFFFFF, 'Square logo image' (two versions: light and dark theme), and 'Show option to remain signed in' (Yes selected). Buttons for 'Select a file' and 'Remove' are also visible.

Troubleshoot sign-in issues

If a user doesn't act on the Stay signed in? prompt, as shown in the following diagram, but abandons the sign-in attempt, you'll see a sign-in log entry that indicates the interrupt.

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

Don't show this again

No

Yes

Details about the sign-in error are as follows and highlighted in the example.

- **Sign in error code:** 50140
- **Failure reason:** This error occurred due to "Keep me signed in" interrupt when the user was signing in.

The screenshot shows the 'Sign-ins' blade in the Azure Active Directory portal. A log entry is selected, showing details like date, request ID, user, application, status, IP address, location, and conditional access. The 'Status' field is highlighted as 'Interrupted'. The 'Failure reason' field contains the message: 'This error occurred due to 'Keep me signed in' interrupt when the user was signing in.' Other log entries show 'Success' status.

You can stop users from seeing the interrupt by setting the **Show option to remain signed in** setting to No in the advanced branding settings. This disables the KMSI prompt for all users in your Azure AD directory.

You also can use the persistent browser session controls in conditional access to prevent users from seen the KMSI prompt. This option allows you to disable the KMSI prompt for a select group of users (such as the global administrators) without affecting sign-in behavior for the remaining users in the directory. For more information, see [User sign-in frequency](#).

To ensure that the KMSI prompt is shown only when it can benefit the user, the KMSI prompt is intentionally not shown in the following scenarios:

- User is signed in via seamless SSO and integrated Windows authentication (IWA)
- User is signed in via Active Directory Federation Services and IWA
- User is a guest in the tenant
- User's risk score is high
- Sign-in occurs during user or admin consent flow
- Persistent browser session control is configured in a conditional access policy

Next steps

Learn about other settings that affect sign-in session timeout:

- Microsoft 365 – [Idle session timeout](#)
- Azure AD Conditional Access - [User sign-in frequency](#)
- Azure portal – [Directory-level inactivity timeout](#)

Associate or add an Azure subscription to your Azure Active Directory tenant

4/10/2022 • 4 minutes to read • [Edit Online](#)

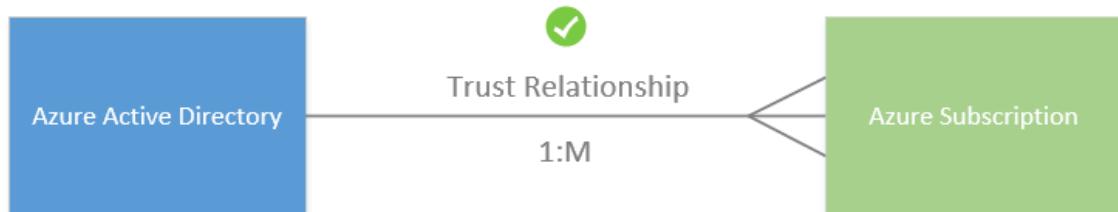
An Azure subscription has a trust relationship with Azure Active Directory (Azure AD). A subscription trusts Azure AD to authenticate users, services, and devices.

Multiple subscriptions can trust the same Azure AD directory. Each subscription can only trust a single directory.

One or more Azure subscriptions can establish a trust relationship with an instance of Azure Active Directory (Azure AD) in order to authenticate and authorize security principals and devices against Azure services. When a subscription expires, the trusted instance of the Azure AD service remains, but the security principals lose access to Azure resources.

When a user signs up for a Microsoft cloud service, a new Azure AD tenant is created and the user is made a member of the Global Administrator role. However, when an owner of a subscription joins their subscription to an existing tenant, the owner isn't assigned to the Global Administrator role.

All of your users have a single *home* directory for authentication. Your users can also be guests in other directories. You can see both the home and guest directories for each user in Azure AD.



IMPORTANT

When you associate a subscription with a different directory, users that have roles assigned using [Azure role-based access control](#) lose their access. Classic subscription administrators, including Service Administrator and Co-Administrators, also lose access.

Moving your Azure Kubernetes Service (AKS) cluster to a different subscription, or moving the cluster-owning subscription to a new tenant, causes the cluster to lose functionality due to lost role assignments and service principal's rights. For more information about AKS, see [Azure Kubernetes Service \(AKS\)](#).

Before you begin

Before you can associate or add your subscription, do the following tasks:

- Review the following list of changes that will occur after you associate or add your subscription, and how you might be affected:
 - Users that have been assigned roles using Azure RBAC will lose their access.
 - Service Administrator and Co-Administrators will lose access.
 - If you have any key vaults, they'll be inaccessible and you'll have to fix them after association.
 - If you have any managed identities for resources such as Virtual Machines or Logic Apps, you must re-enable or recreate them after the association.
 - If you have a registered Azure Stack, you'll have to re-register it after association.
 - For more information, see [Transfer an Azure subscription to a different Azure AD directory](#).
- Sign in using an account that:
 - Has an **Owner** role assignment for the subscription. For information about how to assign the Owner role, see [Assign Azure roles using the Azure portal](#).
 - Exists in both the current directory and in the new directory. The current directory is associated with the subscription. You'll associate the new directory with the subscription. For more information about getting access to another directory, see [Add Azure Active Directory B2B collaboration users in the Azure portal](#).
- Make sure that you're not using an Azure Cloud Service Providers (CSP) subscription (MS-AZR-0145P, MS-AZR-0146P, MS-AZR-159P), a Microsoft Internal subscription (MS-AZR-0015P), or a Microsoft Azure for Students Starter subscription (MS-AZR-0144P).

Associate a subscription to a directory

To associate an existing subscription to your Azure AD directory, follow these steps:

1. Sign in and select the subscription you want to use from the [Subscriptions page in Azure portal](#).
2. Select **Change directory**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and a user profile for 'admin@contoso.onmicrosoft.com'. Below the header, the title 'Contoso Enterprise Subscription' is displayed, followed by a 'Subscription' link. A left sidebar contains links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events, Cost Management, Cost analysis, Budgets, and Advisor recommendations. The main content area shows subscription details: Subscription ID (czzad00c-ef00-0000-00df-0a0zz00da000), Directory (Default Directory (contoso.onmicrosoft.com)), My role (Account admin), Offer (MSDN), Offer ID (MS-AZR-0063P), Subscription name (Contoso Enterprise Subscription), Current billing period (6/2/2020-7/1/2020), Currency (USD), and Status (Active). There's also a 'See more' link and a 'Costs' section. At the top right of the main content area, there are buttons for Manage, Cancel subscription, Rename, Change directory (which is highlighted with a red box), and Transfer billing ownership.

3. Review any warnings that appear, and then select **Change**.

The screenshot shows a modal dialog titled 'Change the directory'. It contains two informational sections: one with a warning icon about removing access for Role-Based Access Control users and another with an info icon about billing ownership. Below these are 'From' and 'To' fields. The 'From' field shows 'Default Directory (contoso.onmicrosoft.com)'. The 'To' field has a dropdown menu with 'Contoso East Coast (000fb00a-0000-00fe-a00f-0d0ae0bcd0...)' selected. At the bottom are 'Change' and 'Cancel' buttons, with 'Change' being highlighted with a red box.

After the directory is changed for the subscription, you will get a success message.

4. Select **Switch directories** on the subscription page to go to your new directory.

The screenshot shows the Azure portal interface. On the left, the 'Subscriptions' page is displayed with a list of subscriptions. A red box highlights the 'Switch directories' link in the top right corner of the main content area. On the right, the 'Directory + subscription' sidebar is open, showing the current directory as 'ajaneaburnley@gmail.onmicrosoft.com'. It also includes links to learn about directories and subscriptions, and a 'Switch directory' section with a dropdown menu set to 'Sign in to your last visited directory'.

It can take several hours for everything to show up properly. If it seems to be taking too long, check the **Global subscription filter**. Make sure the moved subscription isn't hidden. You may need to sign out of the Azure portal and sign back in to see the new directory.

Changing the subscription directory is a service-level operation, so it doesn't affect subscription billing ownership. To delete the original directory, you must transfer the subscription billing ownership to a new Account Admin. To learn more about transferring billing ownership, see [Transfer ownership of an Azure subscription to another account](#).

Post-association steps

After you associate a subscription to a different directory, you might need to do the following tasks to resume operations:

- If you have any key vaults, you must change the key vault tenant ID. For more information, see [Change a key vault tenant ID after a subscription move](#).
- If you used system-assigned Managed Identities for resources, you must re-enable these identities. If you used user-assigned Managed Identities, you must re-create these identities. After re-enabling or recreating the Managed Identities, you must re-establish the permissions assigned to those identities. For more information, see [What are managed identities for Azure resources?](#).
- If you've registered an Azure Stack using this subscription, you must re-register. For more information, see [Register Azure Stack Hub with Azure](#).
- For more information, see [Transfer an Azure subscription to a different Azure AD directory](#).

Next steps

- To create a new Azure AD tenant, see [Quickstart: Create a new tenant in Azure Active Directory](#).
- To learn more about how Microsoft Azure controls resource access, see [Classic subscription administrator roles, Azure roles, and Azure AD administrator roles](#).
- To learn more about how to assign roles in Azure AD, see [Assign administrator and non-administrator roles to users with Azure Active Directory](#).

Add or delete users using Azure Active Directory

4/10/2022 • 4 minutes to read • [Edit Online](#)

Add new users or delete existing users from your Azure Active Directory (Azure AD) organization. To add or delete users you must be a User administrator or Global administrator.

NOTE

For information about viewing or deleting personal data, please review Microsoft's guidance on the [Windows data subject requests for the GDPR site](#). For general information about GDPR, see the [GDPR section of the Microsoft Trust Center](#) and the [GDPR section of the Service Trust portal](#).

Add a new user

You can create a new user using the Azure Active Directory portal.

NOTE

The user name and email address properties can't contain accent characters.

To add a new user, follow these steps:

1. Sign in to the [Azure portal](#) in the User Administrator role for the organization.
2. Search for and select *Azure Active Directory* from any page.
3. Select **Users**, and then select **New user**.

Name	User name	User type	Source
Alain Charon	alain@contoso.com	Member	Azure Active Directory
Charles Anhalt	charlesan@contoso.com	Member	Azure Active Directory
Danielle McKay	danielle@contoso.com	Member	Azure Active Directory
Eggert Schafer	eggert@contoso.com	Member	Azure Active Directory

4. On the **User** page, enter information for this user:

- **Name**. Required. The first and last name of the new user. For example, *Mary Parker*.
- **User name**. Required. The user name of the new user. For example, `mary@contoso.com`.

The domain part of the user name must use either the initial default domain name, `<yourdomainname>.onmicrosoft.com`, or a custom domain name, such as `contoso.com`. For more information about how to create a custom domain name, see [Add your custom domain name using the Azure Active Directory portal](#).

- **Groups.** Optionally, you can add the user to one or more existing groups. You can also add the user to groups at a later time. For more information about adding users to groups, see [Create a basic group and add members using Azure Active Directory](#).
- **Directory role:** If you require Azure AD administrative permissions for the user, you can add them to an Azure AD role. You can assign the user to be a Global administrator or one or more of the limited administrator roles in Azure AD. For more information about assigning roles, see [How to assign roles to users](#).
- **Job info:** You can add more information about the user here, or do it later. For more information about adding user info, see [How to add or change user profile information](#).

5. Copy the autogenerated password provided in the **Password** box. You'll need to give this password to the user to sign in for the first time.

6. Select **Create**.

The user is created and added to your Azure AD organization.

Add a new guest user

You can also invite new guest user to collaborate with your organization by selecting **Invite user** from the **New user** page. If your organization's external collaboration settings are configured such that you're allowed to invite guests, the user will be emailed an invitation they must accept in order to begin collaborating. For more information about inviting B2B collaboration users, see [Invite B2B users to Azure Active Directory](#)

Add a consumer user

There might be scenarios in which you want to manually create consumer accounts in your Azure Active Directory B2C (Azure AD B2C) directory. For more information about creating consumer accounts, see [Create and delete consumer users in Azure AD B2C](#).

Add a new user within a hybrid environment

If you have an environment with both Azure Active Directory (cloud) and Windows Server Active Directory (on-premises), you can add new users by syncing the existing user account data. For more information about hybrid environments and users, see [Integrate your on-premises directories with Azure Active Directory](#).

Delete a user

You can delete an existing user using Azure Active Directory portal.

NOTE

You must have a Global administrator or User administrator role assignment to delete users in your organization. Global admins can delete any users including other admins. User administrators can delete any non-admin users, Helpdesk administrators and other User administrators. For more information, see [Administrator role permissions in Azure AD](#).

To delete a user, follow these steps:

1. Sign in to the [Azure portal](#) using a User administrator account for the organization.
2. Search for and select *Azure Active Directory* from any page.
3. Search for and select the user you want to delete from your Azure AD tenant. For example, *Mary Parker*.
4. Select **Delete user**.

The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. On the left, there's a navigation sidebar with links like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Activity', 'Sign-ins', 'Audit logs', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area has a header with buttons for 'New user', 'New guest user', 'Reset password', 'Delete user' (which is highlighted with a red box), 'Multi-Factor Authentication', and 'More'. Below the header, there's a search bar for 'Name' with 'Mary' typed in and a 'Show' dropdown set to 'All users'. A table lists a single user: 'Mary Parker' (represented by a blue profile icon with 'MP'), 'mary@contoso.com', 'Member', and 'Azure Active Directory' as the source. The 'NAME' column has a checked checkbox.

The user is deleted and no longer appears on the **Users - All users** page. The user can be seen on the **Deleted users** page for the next 30 days and can be restored during that time. For more information about restoring a user, see [Restore or remove a recently deleted user using Azure Active Directory](#).

When a user is deleted, any licenses consumed by the user are made available for other users.

NOTE

To update the identity, contact information, or job information for users whose source of authority is Windows Server Active Directory, you must use Windows Server Active Directory. After you complete the update, you must wait for the next synchronization cycle to complete before you'll see the changes.

Next steps

After you've added your users, you can do the following basic processes:

- [Add or change profile information](#)
- [Assign roles to users](#)
- [Create a basic group and add members](#)
- [Work with dynamic groups and users](#)

Or you can do other user management tasks, such as [adding guest users from another directory](#) or [restoring a deleted user](#). For more information about other available actions, see [Azure Active Directory user management documentation](#).

Add or update a user's profile information using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Add user profile information, including a profile picture, job-specific information, and some settings using Azure Active Directory (Azure AD). For more information about adding new users, see [How to add or delete users in Azure Active Directory](#).

Add or change profile information

As you'll see, there's more information available in a user's profile than what you're able to add during the user's creation. All this additional information is optional and can be added as needed by your organization.

To add or change profile information

NOTE

The user name and email address properties can't contain accent characters.

1. Sign in to the [Azure portal](#) in the User Administrator role for the organization.
2. Select **Azure Active Directory**, select **Users**, and then select a user. For example, *Alain Charon*.

The **Alain Charon - Profile** page appears.

The screenshot shows the Azure Active Directory User Profile page for 'Alain Charon'. The top navigation bar includes 'Microsoft Azure', a search bar, and links for 'Home', 'Identity IT Pro', 'Users', and 'Alain Charon'. The main content area displays the user's profile information: 'Alain Charon' and 'alain@identityitpro.com'. A large circular profile picture placeholder is shown with the letters 'AC'. Below the profile picture, there are sections for 'User Sign-ins' (with a note that only global administrators, security administrators, security readers, and report readers can view sign-ins) and 'Group memberships' (showing 2 groups). On the left, a sidebar lists 'Manage' options: 'Profile' (selected), 'Assigned roles', 'Administrative units', 'Groups', 'Applications', 'Licenses', 'Devices', 'Azure role assignments', and 'Authentication methods'. At the bottom, there are sections for 'Identity' (Name, First name, Last name) and 'Last sign-in date' (8/12/2019, 10:15:39 AM).

3. Select **Edit** to optionally add or update the information included in each of the editable sections.
 - **Profile picture.** Select a thumbnail image for the user's account. This picture appears in Azure Active Directory and on the user's personal pages, such as the [myapps.microsoft.com](#) page.
 - **Identity.** Add or update an additional identity value for the user, such as a married last name. You can set this name independently from the values of First name and Last name. For example, you could use it to include initials, a company name, or to change the sequence of names shown. In another example, for two users whose names are 'Chris Green' you could use the Identity string to set their names to 'Chris B. Green' 'Chris R. Green (Contoso)'.
 - **Job info.** Add any job-related information, such as the user's job title, department, or manager.

- **Settings.** Decide whether the user can sign in to Azure Active Directory tenant. You can also specify the user's global location.
- **Contact info.** Add any relevant contact information for the user, except for some user's phone or mobile contact info (only a global administrator can update for users in administrator roles).
- **Authentication contact info.** Verify this information to make sure there's an active phone number and email address for the user. This information is used by Azure Active Directory to make sure the user is really the user during sign-in. Authentication contact info can be updated only by a global administrator.

4. Select Save.

All your changes are saved for the user.

NOTE

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory. After you complete your update, you must wait for the next synchronization cycle to complete before you'll see the changes.

Next steps

After you've updated your users' profiles, you can perform the following basic processes:

- [Add or delete users](#)
- [Assign roles to users](#)
- [Create a basic group and add members](#)

Or you can perform other user management tasks, such as assigning delegates, using policies, and sharing user accounts. For more information about other available actions, see [Azure Active Directory user management documentation](#).

Reset a user's password using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

As an administrator, you can reset a user's password if the password is forgotten, if the user gets locked out of a device, or if the user never received a password.

NOTE

Unless your Azure AD tenant is the home directory for a user, you won't be able to reset their password. This means that if your user is signing in to your organization using an account from another organization, a Microsoft account, or a Google account, you won't be able to reset their password.

If your user has a source of authority as Windows Server Active Directory, you'll only be able to reset the password if you've turned on password writeback.

If your user has a source of authority as External Azure AD, you won't be able to reset the password. Only the user, or an administrator in External Azure AD, can reset the password.

NOTE

If you're not an administrator and are instead looking for instructions about how to reset your own work or school password, see [Reset your work or school password](#).

To reset a password

1. Sign in to the [Azure portal](#) as a user administrator, or password administrator. For more information about the available roles, see [Azure AD built-in roles](#)
2. Select **Azure Active Directory**, select **Users**, search for and select the user that needs the reset, and then select **Reset Password**.

The **Alain Charon - Profile** page appears with the **Reset password** option.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, All services, Dashboard, etc. The main area shows a user profile for 'Alain Charon - Profile'. At the top right of the profile card, there are three buttons: 'Edit', 'Reset password' (which is highlighted with a red box), and 'Delete'. Below the buttons is a circular profile picture with 'AC' initials. To the right of the picture is a chart titled 'User Sign-ins' showing two spikes in September. Below the chart is a section titled 'Identity' with fields for Name (Alain Charon), User name (alain@flo.pro), Object ID (xxxxxx-xxxx-xxxx-xxxx), First name (...), Last name (...), User type (Member), Source (Azure Active Directory), and a 'Edit' link. At the bottom of the profile card is a section titled 'Job info' with fields for Job title, Department, and Manager.

3. In the Reset password page, select **Reset password**.

NOTE

When using Azure Active Directory, a temporary password is auto-generated for the user. When using Active Directory on-premises, you create the password for the user.

4. Copy the password and give it to the user. The user will be required to change the password during the next sign-in process.

NOTE

The temporary password never expires. The next time the user signs in, the password will still work, regardless how much time has passed since the temporary password was generated.

IMPORTANT

If an administrator is unable to reset the user's password, and in the Application Event Logs on the Azure AD Connect server the following error code hr=80231367 is seen, review the user's attributes in Active Directory. If the attribute **AdminCount** is set to 1, this will prevent an administrator from resetting the user's password. The attribute **AdminCount** must be set to 0, in order for an administrators to reset the user's password.

Next steps

After you've reset your user's password, you can perform the following basic processes:

- [Add or delete users](#)
- [Assign roles to users](#)
- [Add or change profile information](#)
- [Create a basic group and add members](#)

Or you can perform more complex user scenarios, such as assigning delegates, using policies, and sharing user accounts. For more information about other available actions, see [Azure Active Directory user management documentation](#).

Assign administrator and non-administrator roles to users with Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

In Azure Active Directory (Azure AD), if one of your users needs permission to manage Azure AD resources, you must assign them to a role that provides the permissions they need. For info on which roles manage Azure resources and which roles manage Azure AD resources, see [Classic subscription administrator roles](#), [Azure roles](#), and [Azure AD roles](#).

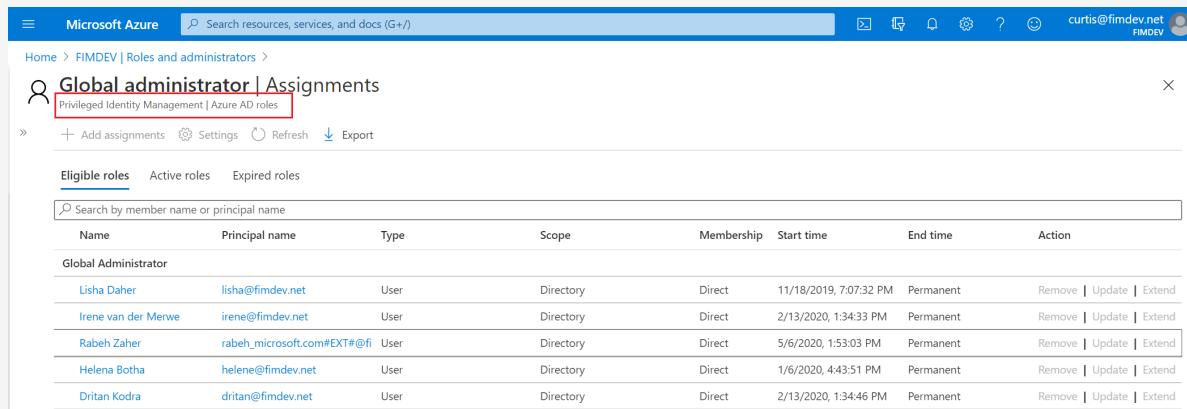
For more information about the available Azure AD roles, see [Assigning administrator roles in Azure Active Directory](#). To add users, see [Add new users to Azure Active Directory](#).

Assign roles

A common way to assign Azure AD roles to a user is on the **Assigned roles** page for a user. You can also configure the user eligibility to be elevated just-in-time into a role using Privileged Identity Management (PIM). For more information about how to use PIM, see [Privileged Identity Management](#).

NOTE

If you have an Azure AD Premium P2 license plan and already use PIM, all role management tasks are performed in the [Privileged Identity Management experience](#). This feature is currently limited to assigning only one role at a time. You can't currently select multiple roles and assign them to a user all at once.



The screenshot shows the 'Global administrator | Assignments' page in the Azure portal. The page title is 'Global administrator | Assignments'. Below it, there's a sub-header 'Privileged Identity Management | Azure AD roles'. The main area has tabs for 'Eligible roles', 'Active roles', and 'Expired roles', with 'Eligible roles' being the active tab. A search bar 'Search by member name or principal name' is present. A table lists five users assigned to the 'Global Administrator' role:

Name	Principal name	Type	Scope	Membership	Start time	End time	Action
Lisha Daher	lisha@fimdev.net	User	Directory	Direct	11/18/2019, 7:07:32 PM	Permanent	Remove Update Extend
Irene van der Merwe	irene@fimdev.net	User	Directory	Direct	2/13/2020, 1:34:33 PM	Permanent	Remove Update Extend
Rabeh Zaher	rabeh_microsoft.com#EXT#@fimdev.net	User	Directory	Direct	5/6/2020, 1:53:03 PM	Permanent	Remove Update Extend
Helene Botha	helene@fimdev.net	User	Directory	Direct	1/6/2020, 4:43:51 PM	Permanent	Remove Update Extend
Dritan Kodra	dritan@fimdev.net	User	Directory	Direct	2/13/2020, 1:34:46 PM	Permanent	Remove Update Extend

Assign a role to a user

1. Go to the [Azure portal](#) and sign in using a Global administrator account for the directory.
2. Search for and select **Azure Active Directory**.

Azure Active Directory

Services All 41 results

- Azure Active Directory**
- Activity log
- Azure Cosmos DB
- Azure Database for MySQL servers
- Azure Arc
- Azure Databricks
- Azure DevOps
- Azure Lighthouse
- Azure Migrate
- Azure Sentinel

Resources

No results were found.

Resource Groups

No results were found.

Documentation All 1000+ results

[What is Azure Active Directory? - Azure Active Directory ...](#)

[Azure Active Directory documentation | Microsoft Docs](#)

3. Select **Users**.

4. Search for and select the user getting the role assignment. For example, *Alain Charon*.

Users - All users

Name	User name	User type	Source
admin1	admin1@firstupconsultants.com	Member	External Azure Active Directory
Alain Charon	alain@firstupconsultants.com	Member	Azure Active Directory
Isabella Simonsen	isabella@firstupconsultants.com	Member	Azure Active Directory

5. On the **Alain Charon - Profile** page, select **Assigned roles**.

The **Alain Charon - Administrative roles** page appears.

6. Select **Add assignments**, select the role to assign to Alain (for example, *Application administrator*), and then choose **Select**.

The Application administrator role is assigned to Alain Charon and it appears on the **Alain Charon - Administrative roles** page.

The Application administrator role is assigned to Alain Charon and it appears on the **Alain Charon - Administrative roles** page.

Remove a role assignment

If you need to remove the role assignment from a user, you can also do that from the **Alain Charon - Administrative roles** page.

To remove a role assignment from a user

1. Select **Azure Active Directory**, select **Users**, and then search for and select the user getting the role assignment removed. For example, *Alain Charon*.
2. Select **Assigned roles**, select **Application administrator**, and then select **Remove assignment**.

The Application administrator role is removed from Alain Charon and it no longer appears on the **Alain Charon - Administrative roles** page.

The Application administrator role is removed from Alain Charon and it no longer appears on the **Alain Charon - Administrative roles** page.

Next steps

- [Add or delete users](#)
- [Add or change profile information](#)
- [Add guest users from another directory](#)

Other user management tasks you can check out are available in [Azure Active Directory user management documentation](#).

Assign or remove licenses in the Azure Active Directory portal

4/10/2022 • 4 minutes to read • [Edit Online](#)

Many Azure Active Directory (Azure AD) services require you to license each of your users or groups (and associated members) for that service. Only users with active licenses will be able to access and use the licensed Azure AD services for which that's true. Licenses are applied per tenant and do not transfer to other tenants.

Available license plans

There are several license plans available for the Azure AD service, including:

- Azure AD Free
- Azure AD Premium P1
- Azure AD Premium P2

For specific information about each license plan and the associated licensing details, see [What license do I need?](#). To sign up for Azure AD premium license plans see [here](#).

Not all Microsoft services are available in all locations. Before a license can be assigned to a group, you must specify the **Usage location** for all members. You can set this value in the **Azure Active Directory > Users > Profile > Settings** area in Azure AD. Any user whose usage location is not specified inherits the location of the Azure AD organization.

View license plans and plan details

You can view your available service plans, including the individual licenses, check pending expiration dates, and view the number of available assignments.

To find your service plan and plan details

1. Sign in to the [Azure portal](#) using a License administrator account in your Azure AD organization.
2. Select **Azure Active Directory**, and then select **Licenses**.
3. Select **All products** to view the All Products page and to see the **Total**, **Assigned**, **Available**, and **Expiring soon** numbers for your license plans.

Name	Total	Assigned	Available	Expiring soon
Microsoft Power Automate Free	10000	1	9999	0

NOTE

The numbers are defined as:

- Total: Total number of licenses purchased
- Assigned: Number of licenses assigned to users
- Available: Number of licenses available for assignment including expiring soon
- Expiring soon: Number of licenses expiring soon

4. Select a plan name to see its licensed users and groups.

Assign licenses to users or groups

Make sure that anyone needing to use a licensed Azure AD service has the appropriate license. You can add the licensing rights to users or to an entire group.

To assign a license to a user

1. On the **Products** page, select the name of the license plan you want to assign to the user.
2. After you select the license plan, select **Assign**.

The screenshot shows the 'Licenses | All products' page in the Azure portal. The 'Microsoft Power Automate Free' plan is selected in the list, indicated by a red box around the checkbox and the plan name. The page includes navigation links like 'Home > Fourth Coffee > Licenses', a search bar, and tabs for 'Overview', 'Diagnose and solve problems', 'Manage', 'Licensed features', 'All products', and 'Self-service sign up products'. Below the list, there are columns for 'Name', 'Total', 'Assigned', 'Available', and 'Expiring soon'.

3. On the **Assign** page, select **Users and groups**, and then search for and select the user you're assigning the license.

The screenshot shows the 'Assign license' page. It displays a list of users under the heading 'Users'. One user, 'Alan J. Bigham' (aj@fourthcoffee.club), is highlighted with a red box and labeled 'Selected'. Below this, there's a 'Selected items' section with a 'Remove' button. At the bottom of the page, there are 'Assign' and 'Select' buttons, with the 'Select' button also highlighted with a red box.

4. Select **Assignment options**, make sure you have the appropriate license options turned on, and then select **OK**.

Assign license

Fourth Coffee

The screenshot shows the 'Assign license' page. At the top, there's a note: 'Learn how to activate license assignments to groups.' Below it, it says '*Users' and '1 user selected'. A section titled 'Assignment options' is highlighted with a red box. At the bottom, there are two buttons: 'Assign' and 'Ok', with 'Ok' also highlighted with a red box.

The **Assign license** page updates to show that a user is selected and that the assignments are configured.

NOTE

Not all Microsoft services are available in all locations. Before a license can be assigned to a user, you must specify the **Usage location**. You can set this value in the **Azure Active Directory > Users > Profile > Settings** area in Azure AD. Any user whose usage location is not specified inherits the location of the Azure AD organization.

5. Select Assign.

The user is added to the list of licensed users and has access to the included Azure AD services.

NOTE

Licenses can also be assigned directly to a user from the user's **Licenses** page. If a user has a license assigned through a group membership and you want to assign the same license to the user directly, it can be done only from the **Products** page mentioned in step 1 only.

To assign a license to a group

1. On the **Products** page, select the name of the license plan you want to assign to the user.

The screenshot shows the 'Products' page. It lists two license plans: 'Azure Active Directory Premium Plan 1' and 'Azure Active Directory Premium Plan 2'. The 'Azure Active Directory Premium Plan 2' row is highlighted with a blue dashed border. The columns are labeled: NAME, ASSIGNED, AVAILABLE, and EXPIRING SOON.

NAME	ASSIGNED	AVAILABLE	EXPIRING SOON
Azure Active Directory Premium Plan 1	25	100	0
Azure Active Directory Premium Plan 2	300	0	250

2. On the **Azure Active Directory Premium Plan 2** page, select **Assign**.

Licenses | All products

Fourth Coffee - Azure Active Directory

+ Try / Buy + Assign Bills Columns Got feedback?

Overview Diagnose and solve problems Manage Licensed features All products Self-service sign up products

Name	Total	Assigned	Available	Expiring soon
Microsoft Power Automate Free	10000	1	9999	0

3. On the **Assign license** page, select **Users and groups**, and then search for and select the group you're assigning the license.

Home > Licenses > Products > Azure Active

Assign license

This feature is currently in public preview

* Users and groups
1 user selected

Assignment options
Assignment options

Select

mdm

MDM policy - North

MDM policy - South

MDM policy - West

Selected members:

Mary Parker
mary@contoso.com
Remove

MDM policy - West
Remove

Assign Select

4. Select **Assignment options**, make sure you have the appropriate license options turned on, and then select **OK**.

Dashboard > Company Name cDeQx > Licenses - Overview > Products > Microsoft Dynamics

X Assign license

Company Name cDeQx

* Users and groups
1 group selected

Assignment options
Assignment options

Microsoft Dynamics CRM Online

Flow for Dynamics 365

Microsoft Dynamics CRM Online Professional

Microsoft Dynamics Marketing Sales Collaboration – Eligibility criteria apply

Microsoft Social Engagement Professional – Eligibility Criteria apply

PowerApps for Dynamics 365

License options

Off On

Off On

Off On

Off On

Off On

Assign Ok

The **Assign license** page updates to show that a user is selected and that the assignments are configured.

5. Select Assign.

The group is added to the list of licensed groups and all of the members have access to the included Azure AD services.

Remove a license

You can remove a license from a user's Azure AD user page, from the group overview page for a group assignment, or starting from the Azure AD **Licenses** page to see the users and groups for a license.

To remove a license from a user

1. On the **Licensed users** page for the service plan, select the user that should no longer have the license.
For example, *Alain Charon*.

2. Select **Remove license**.

Assignment	User	Email	Status	Entitlements	Inheritance
AG	agilanico	agilar@aad27.cscstp.net	Active	6/6	Inherit
AL	allochroous	allochthon@aad27.cscstp.net	Active	6/6	Direct
AM	almhult	almi@aad27.cscstp.net	Active	6/6	Inherit
AN	alteration	alteration's@aad27.cscstp.net	Active	6/6	Inherit
AM	amidases	amidate@aad27.cscstp.net	Active	6/6	Inherit
AN	anatahan	anatalia@aad27.cscstp.net	Active	6/6	Inherit
AN	ancientgreymon	ancientism@aad27.cscstp.net	Active	6/6	Inherit
AN	andrezinho	andrezj@aad27.cscstp.net	Active	6/6	Inherit
AN	aneurumatic	aneurusmaticmu@aad27.cscstp.net	Active	6/6	Inherit

IMPORTANT

Licenses that a user inherits from a group can't be removed directly. Instead, you have to remove the user from the group from which they're inheriting the license.

To remove a license from a group

1. On the **Licensed groups** page for the license plan, select the group that should no longer have the license.
2. Select **Remove license**.

Name	State	Enabled Services
AN AniGroup	Active	16/17

NOTE

When an on-premises user account synced to Azure AD falls out of scope for the sync or when the sync is removed, the user is soft-deleted in Azure AD. When this occurs, licenses assigned to the user directly or via group-based licensing will be marked as **suspended** rather than **deleted**.

Next steps

After you've assigned your licenses, you can perform the following processes:

- [Identify and resolve license assignment problems](#)
- [Add licensed users to a group for licensing](#)
- [Scenarios, limitations, and known issues using groups to manage licensing in Azure Active Directory](#)
- [Add or change profile information](#)

Restore or remove a recently deleted user using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

After you delete a user, the account remains in a suspended state for 30 days. During that 30-day window, the user account can be restored, along with all its properties. After that 30-day window passes, the permanent deletion process is automatically started.

You can view your restorable users, restore a deleted user, or permanently delete a user using Azure Active Directory (Azure AD) in the Azure portal.

IMPORTANT

Neither you nor Microsoft customer support can restore a permanently deleted user.

Required permissions

You must have one of the following roles to restore and permanently delete users.

- Global administrator
- Partner Tier1 Support
- Partner Tier2 Support
- User administrator

View your restorable users

You can see all the users that were deleted less than 30 days ago. These users can be restored.

To view your restorable users

1. Sign in to the [Azure portal](#) using a Global administrator account for the organization.
2. Select **Azure Active Directory**, select **Users**, and then select **Deleted users**.

Review the list of users that are available to restore.

The screenshot shows the Azure portal interface. On the left, there's a sidebar with 'Create a resource', 'All services', 'Favorites' (which includes 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', and 'Azure Active Directory'), 'Security Center', 'Cost Management + Billing', and 'Help + support'. The 'Azure Active Directory' item is highlighted with a red box. The main content area has a breadcrumb navigation: 'Home > Contoso > Users - Deleted users'. The title is 'Users - Deleted users' under 'Contoso - Azure Active Directory'. Below the title, there are buttons for 'Delete permanently' and 'Restore user', and links for 'Refresh' and 'Columns'. A message box says 'Users are permanently deleted automatically 30 days after they are deleted.' There's a search bar labeled 'Search by name or email'. A table lists two deleted users:

Name	User Name	User Type	Source	Deletion Date	Permanent Deletion Date
Mary Parker	marypa@contoso.com	Member	Azure Active Directory	9/6/2018, 11:21:10 AM	10/6/2018, 11:21:10 AM
Rae Huff	rae@contoso.com	Member	Azure Active Directory	9/6/2018, 11:21:10 AM	10/6/2018, 11:21:10 AM

Restore a recently deleted user

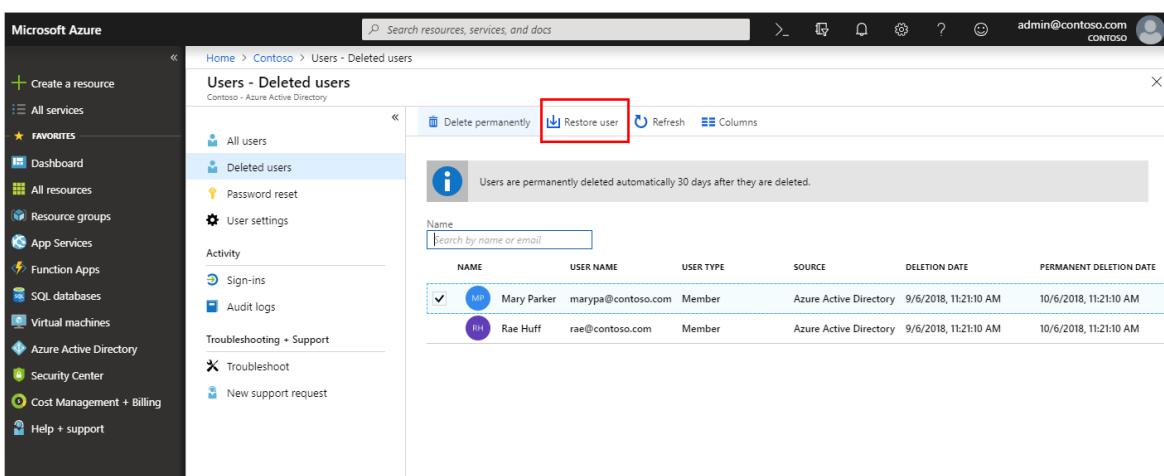
When a user account is deleted from the organization, the account is in a suspended state and all the related organization information is preserved. When you restore a user, this organization information is also restored.

NOTE

Once a user is restored, licenses that were assigned to the user at the time of deletion are also restored even if there are no seats available for those licenses. If you are then consuming more licenses more than you purchased, your organization could be temporarily out of compliance for license usage.

To restore a user

1. On the **Users - Deleted users** page, search for and select one of the available users. For example, *Mary Parker*.
2. Select **Restore user**.



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like App Services, Function Apps, SQL databases, etc. The main area is titled 'Users - Deleted users' under 'Contoso - Azure Active Directory'. It shows a list of deleted users with columns for Name, User Name, User Type, Source, Deletion Date, and Permanent Deletion Date. Two users are listed: 'Mary Parker' and 'Rae Huff'. Below the table, there's a note: 'Users are permanently deleted automatically 30 days after they are deleted.' At the top of the page, there are buttons for 'Delete permanently' and 'Restore user', with 'Restore user' being highlighted by a red box.

Permanently delete a user

You can permanently delete a user from your organization without waiting the 30 days for automatic deletion. A permanently deleted user can't be restored by you, another administrator, nor by Microsoft customer support.

NOTE

If you permanently delete a user by mistake, you'll have to create a new user and manually enter all the previous information. For more information about creating a new user, see [Add or delete users](#).

To permanently delete a user

1. On the **Users - Deleted users** page, search for and select one of the available users. For example, *Rae Huff*.
2. Select **Delete permanently**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons and links like 'Create a resource', 'All services', 'Dashboard', etc. The main area is titled 'Users - Deleted users' under 'Contoso - Azure Active Directory'. At the top right of this area, there are buttons for 'Delete permanently', 'Restore user', 'Refresh', and 'Columns'. Below these buttons, a message states: 'Users are permanently deleted automatically 30 days after they are deleted.' There's a search bar labeled 'Name' with the placeholder 'Search by name or email'. A table below lists a single user: 'Rae Huff' (rae@contoso.com), who is a 'Member' from 'Azure Active Directory'. The table columns are 'NAME', 'USER NAME', 'USER TYPE', 'SOURCE', 'DELETION DATE', and 'PERMANENT DELETION DATE'. The 'DELETION DATE' is 9/6/2018, 11:21:10 AM, and the 'PERMANENT DELETION DATE' is 10/6/2018, 11:21:10 AM.

Next steps

After you've restored or deleted your users, you can:

- [Add or delete users](#)
- [Assign roles to users](#)
- [Add or change profile information](#)
- [Add guest users from another organization](#)

For more information about other available user management tasks, [Azure AD user management documentation](#).

Create a basic group and add members using Azure Active Directory

4/10/2022 • 4 minutes to read • [Edit Online](#)

You can create a basic group using the Azure Active Directory (Azure AD) portal. For the purposes of this article, a basic group is added to a single resource by the resource owner (administrator) and includes specific members (employees) that need to access that resource. For more complex scenarios, including dynamic memberships and rule creation, see the [Azure Active Directory user management documentation](#).

Group and membership types

There are several group and membership types. The following information explains each group and membership type and why they are used, to help you decide which options to use when you create a group.

Group types:

- **Security.** Used to manage member and computer access to shared resources for a group of users. For example, you can create a security group for a specific security policy. By doing it this way, you can give a set of permissions to all the members at once, instead of having to add permissions to each member individually. A security group can have users, devices, groups and service principals as its members and users and service principals as its owners. For more info about managing access to resources, see [Manage access to resources with Azure Active Directory groups](#).
- **Microsoft 365.** Provides collaboration opportunities by giving members access to a shared mailbox, calendar, files, SharePoint site, and more. This option also lets you give people outside of your organization access to the group. A Microsoft 365 group can have only users as its members. Both users and service principals can be owners of a Microsoft 365 group. For more info about Microsoft 365 Groups, see [Learn about Microsoft 365 Groups](#).

Membership types:

- **Assigned.** Lets you add specific users to be members of this group and to have unique permissions. For the purposes of this article, we're using this option.
- **Dynamic user.** Lets you use dynamic membership rules to automatically add and remove members. If a member's attributes change, the system looks at your dynamic group rules for the directory to see if the member meets the rule requirements (is added) or no longer meets the rules requirements (is removed).
- **Dynamic device.** Lets you use dynamic group rules to automatically add and remove devices. If a device's attributes change, the system looks at your dynamic group rules for the directory to see if the device meets the rule requirements (is added) or no longer meets the rules requirements (is removed).

IMPORTANT

You can create a dynamic group for either devices or users, but not for both. You also can't create a device group based on the device owners' attributes. Device membership rules can only reference device attributions. For more info about creating a dynamic group for users and devices, see [Create a dynamic group and check status](#)

Create a basic group and add members

You can create a basic group and add your members at the same time. To create a basic group and add members use the following procedure:

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Search for and select **Azure Active Directory**.
3. On the **Active Directory** page, select **Groups** and then select **New group**.

The screenshot shows the 'Groups | All groups' page in the Azure Active Directory. The top navigation bar includes 'Home > First Up Consultants > Groups | All groups'. Below the navigation is a search bar and filter options. A red box highlights the '+ New group' button. The main area displays a table of existing groups with columns for Name, Object Id, Group Type, Membership Type, Email, and Source. The groups listed are CA, MP (MDM policy), and several other entries.

	Name	Object Id	Group Type	Membership Type	Email	Source
<input type="checkbox"/>	CA	CA-MFA-Azure...	xxxxxx-xxxx-xxxx-xx...	Security	Assigned	Cloud
<input type="checkbox"/>	MP	MDM policy - ...	xxxxxx-xxxx-xxxx-xx...	Security	Assigned	Cloud
<input type="checkbox"/>	MP	MDM policy - ...	xxxxxx-xxxx-xxxx-xx...	Security	Assigned	Cloud
<input type="checkbox"/>	MP	MDM policy - ...	xxxxxx-xxxx-xxxx-xx...	Security	Assigned	Cloud
<input type="checkbox"/>	MP	MDM policy - ...	xxxxxx-xxxx-xxxx-xx...	Security	Assigned	Cloud

4. The **New Group** pane will appear and you must fill out the required information.

The screenshot shows the 'New Group' creation pane. It includes fields for Group type (set to Office 365), Group name (MDM Policy-East), Group email address (MDMPolicy-East@firstupconsultants92157408.onmicrosoft.com), Group description (MDM users on East coast), Membership type (Assigned), Owners (No owners selected), and Members (No members selected). The 'Create' button at the bottom is highlighted with a red box.

5. Select a pre-defined **Group type**. For more information on group types, see [Group and membership types](#).
6. Create and add a **Group name**. Choose a name that you'll remember and that makes sense for the group. A check will be performed to determine if the name is already in use by another group. If the

name is already in use, to avoid duplicate naming, you'll be asked to change the name of your group.

7. Add a **Group email address** for the group, or keep the email address that is filled in automatically.
8. **Group description**. Add an optional description to your group.
9. Select a pre-defined **Membership type (required)**. For more information on membership types, see [Group and membership types](#).
10. Select **Create**. Your group is created and ready for you to add members.
11. Select the **Members** area from the **Group** page, and then begin searching for the members to add to your group from the **Select members** page.

The screenshot shows the 'Add members' dialog box. At the top is a search bar. Below it is a table titled 'Direct members' with columns for 'Name' and 'Type'. Two users are listed: Isabella Simonsen (User) and Isabella Simonsen (User). Below the table is a section titled 'Selected items' containing the same two users, each with a 'Remove' button. At the bottom right is a large blue 'Select' button.

12. When you're done adding members, choose **Select**.

The **Group Overview** page updates to show the number of members who are now added to the group.

The screenshot shows the 'MDM Policy-East' Group Overview page. On the left is a sidebar with links like Overview, Diagnose and solve problems, Properties, Members (which is selected and highlighted in grey), Owners, etc. The main area has a green 'MP' logo and the title 'MDM Policy-East'. It displays the group's description 'MDM users on East coast'. Below this are several input fields: 'Membership type' (Assigned), 'Source' (Cloud), 'Type' (Office), 'Object Id' (empty), 'Creation date' (6/4/2020, 6:35:38 PM), and 'Email' (MDMPolicy-East@firstupconsultants.com). At the bottom, there are sections for 'Direct members' (3 User(s)), 'Group memberships' (0 Group(s)), 'Device(s)' (0 Device(s)), 'Other(s)' (0 Other(s)), and 'Owners' (1 owner).

Turn off group welcome email

When any new Microsoft 365 group is created, whether with dynamic or static membership, a welcome notification is sent to all users who are added to the group. When any attributes of a user or device change, all dynamic group rules in the organization are processed for potential membership changes. Users who are added then also receive the welcome notification. You can turn this behavior off in [Exchange PowerShell](#).

Next steps

- [Manage access to SaaS apps using groups](#)
- [Manage groups using PowerShell commands](#)

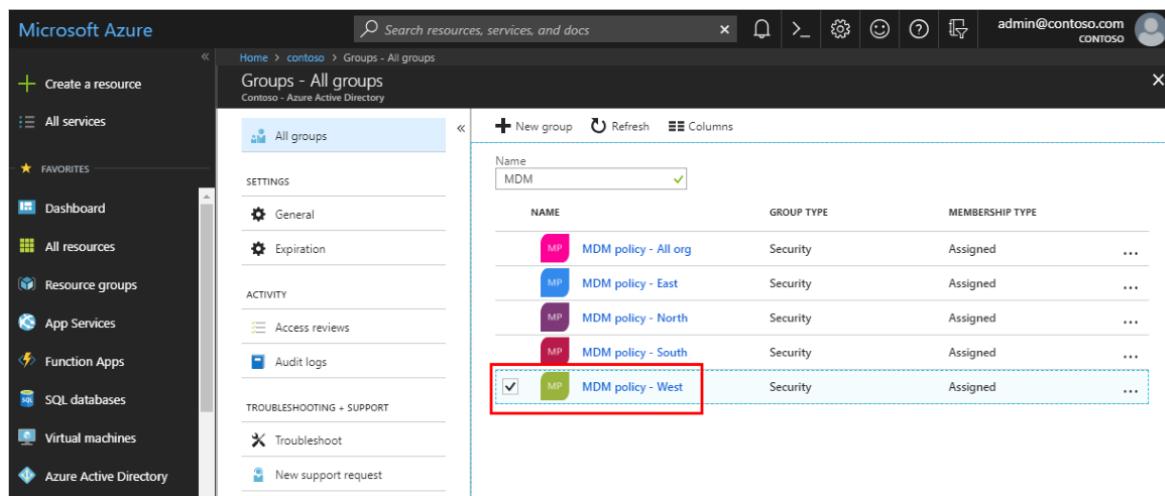
Add or remove group members using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Using Azure Active Directory, you can continue to add and remove group members.

To add group members

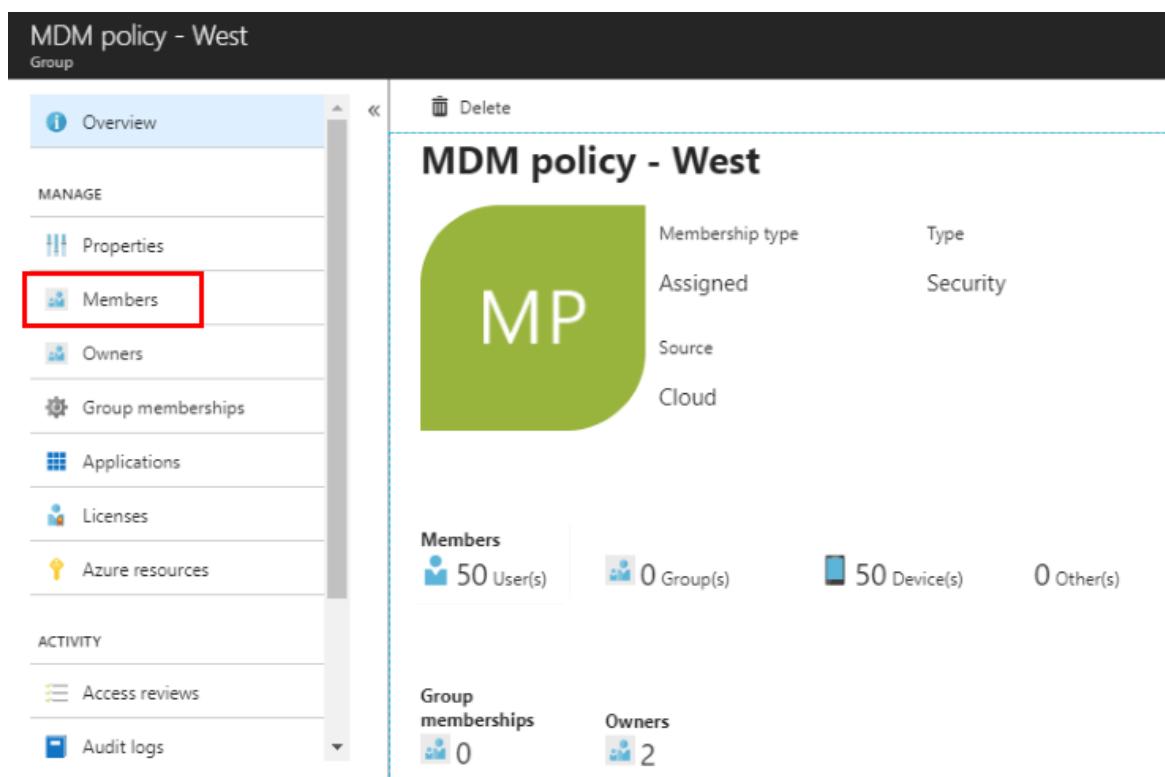
1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.
3. From the **Groups - All groups** page, search for and select the group you want to add the member to. In this case, use our previously created group, **MDM policy - West**.



The screenshot shows the 'Groups - All groups' page in the Microsoft Azure portal. The left sidebar includes 'Create a resource', 'All services', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', and 'Azure Active Directory'. The main area shows a table of groups with columns: NAME, GROUP TYPE, and MEMBERSHIP TYPE. A search bar at the top right says 'Search resources, services, and docs'. The 'Groups - All groups' page has a breadcrumb trail: Home > contoso > Groups - All groups. The 'MDM policy - West' group is highlighted with a red box and a checkmark in the 'Selected' column.

NAME	GROUP TYPE	MEMBERSHIP TYPE
MDM policy - All org	Security	Assigned
MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned
MDM policy - West	Security	Assigned

4. From the **MDM policy - West Overview** page, select **Members** from the **Manage** area.



The screenshot shows the 'MDM policy - West' overview page. The left sidebar under 'MANAGE' has options: Properties, **Members** (which is highlighted with a red box), Owners, Group memberships, Applications, Licenses, and Azure resources. The main area displays the group's details: 'MDM policy - West' with a large green 'MP' logo, membership type (Assigned), source (Cloud), and activity counts (50 User(s), 0 Group(s), 50 Device(s), 0 Other(s)). The 'Members' section is expanded, showing 50 User(s) and 2 Owners.

5. Select **Add members**, and then search and select each of the members you want to add to the group, and then choose **Select**.

You'll get a message that says the members were added successfully.

The screenshot shows the 'Add members' dialog box. At the top, there's a search bar with 'Select member or invite an external user' and a placeholder 'Alain'. Below it, a list shows 'No members have been found'. On the right, under 'Selected members:', there are two entries: Danielle McKay (danielle@contoso.com) and Eggert Schafer (eggert@contoso.com). Each entry has a 'Remove' link. At the bottom of the dialog is a large blue 'Select' button, which is also highlighted with a red box.

6. Refresh the screen to see all of the member names added to the group.

To remove group members

1. From the Groups - All groups page, search for and select the group you want to remove the member from. Again we'll use, **MDM policy - West**.
2. Select **Members** from the Manage area, search for and select the name of the member to remove, and then select **Remove**.

The screenshot shows the 'Alain Charon' group details page. At the top, there's a 'Remove' button, which is highlighted with a red box. Below it, under 'MEMBER', there's a list with 'Alain Charon' (highlighted with a dashed blue border). Further down, under 'GROUP', it shows 'MDM policy - West'. Under 'MEMBERSHIP TYPE', it says 'Assigned'. Under 'MEMBER TYPE', it says 'User'.

Next steps

- [View your groups and members](#)
- [Edit your group settings](#)

- Manage access to resources using groups
- Manage dynamic rules for users in a group
- Associate or add an Azure subscription to Azure Active Directory

Delete a group using Azure Active Directory

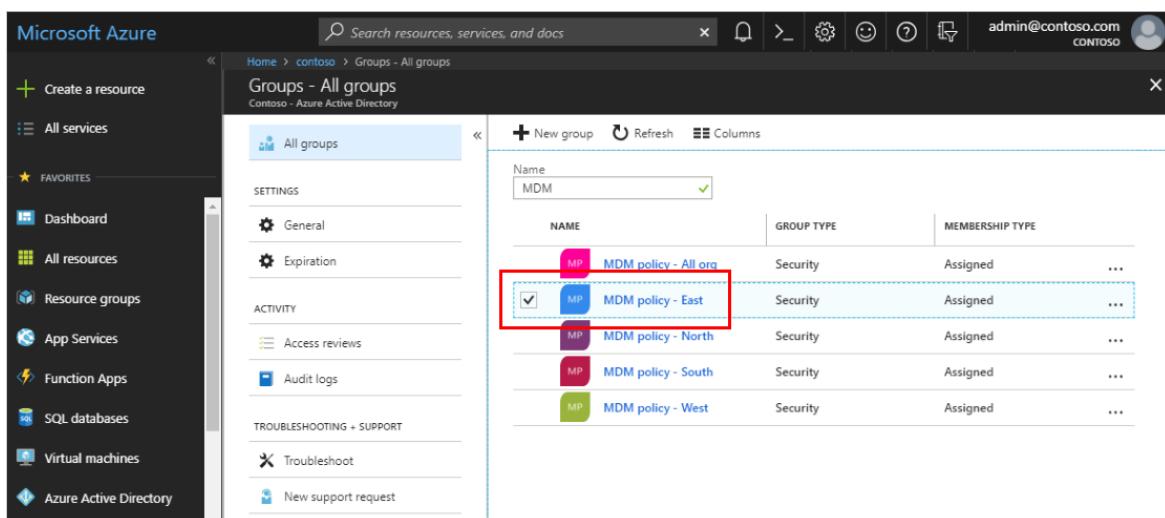
4/10/2022 • 2 minutes to read • [Edit Online](#)

You can delete an Azure Active Directory (Azure AD) group for any number of reasons, but typically it will be because you:

- Incorrectly set the **Group type** to the wrong option.
- Created the wrong or a duplicate group by mistake.
- No longer need the group.

To delete a group

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.
3. From the **Groups - All groups** page, search for and select the group you want to delete. For these steps, we'll use **MDM policy - East**.



The screenshot shows the Azure portal interface. On the left, the navigation menu includes 'Create a resource', 'All services', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', and 'Azure Active Directory'. The 'Azure Active Directory' option is selected. In the center, the 'Groups - All groups' page is displayed under 'Contoso - Azure Active Directory'. The left sidebar shows 'All groups' and 'SETTINGS' (General, Expiration). The main area shows a table with columns: NAME, GROUP TYPE, and MEMBERSHIP TYPE. The table lists five groups: 'MDM policy - All org' (Security, Assigned), 'MDM policy - East' (Security, Assigned, highlighted with a red box and checked), 'MDM policy - North' (Security, Assigned), 'MDM policy - South' (Security, Assigned), and 'MDM policy - West' (Security, Assigned). The 'MDM policy - East' row is also highlighted with a dashed blue border.

NAME	GROUP TYPE	MEMBERSHIP TYPE
MDM policy - All org	Security	Assigned
<input checked="" type="checkbox"/> MDM policy - East	Security	Assigned
MDM policy - North	Security	Assigned
MDM policy - South	Security	Assigned
MDM policy - West	Security	Assigned

4. On the **MDM policy - East Overview** page, and then select **Delete**.

The group is deleted from your Azure Active Directory tenant.

MDM policy - East

Group

Overview

Delete

MDM policy - East

Membership type: Assigned; Type: Security; Source: Cloud

Members: 0 User(s) | 0 Group(s) | 0 Device(s) | 0 Other(s)

Group memberships: 0 | Owners: 0

Next steps

- If you delete a group by mistake, you can create it again. For more information, see [How to create a basic group and add members](#).
- If you delete a Microsoft 365 group by mistake, you might be able to restore it. For more information, see [Restore a deleted Office 365 group](#).

Add or remove a group from another group using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

This article helps you to add and remove a group from another group using Azure Active Directory.

NOTE

If you're trying to delete the parent group, see [How to update or delete a group and its members](#).

Add a group to another group

You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

IMPORTANT

We don't currently support:

- Adding groups to a group synced with on-premises Active Directory.
- Adding Security groups to Microsoft 365 groups.
- Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups.
- Assigning apps to nested groups.
- Applying licenses to nested groups.
- Adding distribution groups in nesting scenarios.
- Adding security groups as members of mail-enabled security groups

To add a group as a member of another group

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.
3. On the **Groups - All groups** page, search for and select the group that's to become a member of another group. For this exercise, we're using the **MDM policy - West** group.

NOTE

You can add your group as a member to only one group at a time. Additionally, the **Select Group** box filters the display based on matching your entry to any part of a user or device name. However, wildcard characters aren't supported.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a 'Groups' menu item highlighted with a red box. The main content area is titled 'Groups - All groups' and shows a list of groups. One group, 'MDM policy - West', is selected and highlighted with a red box.

- On the **MDM policy - West - Group memberships** page, select **Group memberships**, select **Add**, locate the group you want your group to be a member of, and then choose **Select**. For this exercise, we're using the **MDM policy - All org** group.

The **MDM policy - West** group is now a member of the **MDM policy - All org** group, inheriting all the properties and configuration of the **MDM policy - All org** group.

The screenshot shows the 'MDM policy - West - Group memberships' page. The 'Group memberships' menu item is highlighted with a red box. The '+ Add memberships' button is highlighted with a red box. A modal window titled 'Select groups' is open, showing a list of groups. One group, 'MDM policy - All org', is selected and highlighted with a red box. The 'Select' button at the bottom of the modal is also highlighted with a red box.

- Review the **MDM policy - West - Group memberships** page to see the group and member relationship.
- For a more detailed view of the group and member relationship, select the group name (**MDM policy - All org**) and take a look at the **MDM policy - West** page details.

Remove a group from another group

You can remove an existing Security group from another Security group. However, removing the group also removes any inherited attributes and properties for its members.

To remove a member group from another group

- On the **Groups - All groups** page, search for and select the group that's to be removed as a member of another group. For this exercise, we're again using the **MDM policy - West** group.
- On the **MDM policy - West overview** page, select **Group memberships**.

3. Select the **MDM policy - All org** group from the **MDM policy - West - Group memberships** page, and then select **Remove** from the **MDM policy - West** page details.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the breadcrumb path is 'Home > Contoso > Groups - All groups > MDM policy - West - Group memberships'. The main title is 'MDM policy - West - Group memberships'. On the left, a sidebar under 'Manage' has options like 'Properties', 'Members', 'Owners', and 'Group memberships' (which is highlighted with a red box). In the center, there's a table with columns 'Name', 'Object Id', 'Group Type', and 'Membership Type'. One row is visible: 'MDM policy - All o...' (with a blue checkmark icon), 'MP', 'Security', and 'Assigned'. At the top of the table area, there are buttons for 'Add memberships' (with a plus sign) and 'Remove memberships' (with a trash bin icon, also highlighted with a red box). Other buttons include 'Refresh', 'Columns', and 'Got feedback?'. A purple banner at the bottom says 'Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview.' with a right-pointing arrow.

Additional information

These articles provide additional information on Azure Active Directory.

- [View your groups and members](#)
- [Create a basic group and add members](#)
- [Add or remove members from a group](#)
- [Edit your group settings](#)
- [Using a group to manage access to SaaS applications](#)
- [Scenarios, limitations, and known issues using groups to manage licensing in Azure Active Directory](#)

Edit your group information using Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Using Azure Active Directory (Azure AD), you can edit a group's settings, including updating its name, description, or membership type.

To edit your group settings

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.

The **Groups - All groups** page appears, showing all of your active groups.

3. From the **Groups - All groups** page, type as much of the group name as you can into the **Search** box.
For the purposes of this article, we're searching for the **MDM policy - West** group.

The search results appear under the **Search** box, updating as you type more characters.

NAME	GROUP TYPE	MEMBERSHIP TYPE	...
MDM	Security	Assigned	...
MDM policy - All org	Security	Assigned	...
MDM policy - East	Security	Assigned	...
MDM policy - North	Security	Assigned	...
MDM policy - South	Security	Assigned	...
MDM policy - West	Security	Assigned	...

4. Select the group **MDM policy - West**, and then select **Properties** from the **Manage** area.

MDM policy - West

Properties

Membership type: Assigned; Type: Security; Source: Cloud

Members: 50 User(s), 0 Group(s), 50 Device(s), 0 Other(s)

Group memberships: 0; Owners: 2

- Update the General settings information as needed, including:

MDM policy - West - Properties

General settings

- Group name: MDM policy - West
- Group description: MDM users on West coast
- Group type: Security
- Membership type: Assigned
- Object ID: 9f33d478-96e3-4577-894e-02f406e8c804

- Group name.** Edit the existing group name.
- Group description.** Edit the existing group description.
- Group type.** You can't change the type of group after it's been created. To change the **Group type**, you must delete the group and create a new one.
- Membership type.** Change the membership type. For more info about the various available membership types, see [How to: Create a basic group and add members using the Azure Active Directory portal](#).
- Object ID.** You can't change the Object ID, but you can copy it to use in your PowerShell commands for the group. For more info about using PowerShell cmdlets, see [Azure Active Directory cmdlets for configuring group settings](#).

Next steps

These articles provide additional information on Azure Active Directory.

- [View your groups and members](#)
- [Create a basic group and add members](#)
- [How to add or remove members from a group](#)
- [Manage dynamic rules for users in a group](#)
- [Manage memberships of a group](#)
- [Manage access to resources using groups](#)
- [Associate or add an Azure subscription to Azure Active Directory](#)

Add or remove group owners in Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) groups are owned and managed by group owners. Group owners can be users or service principals, and are able to manage the group including membership. Only existing group owners or group-managing administrators can assign group owners. Group owners aren't required to be members of the group.

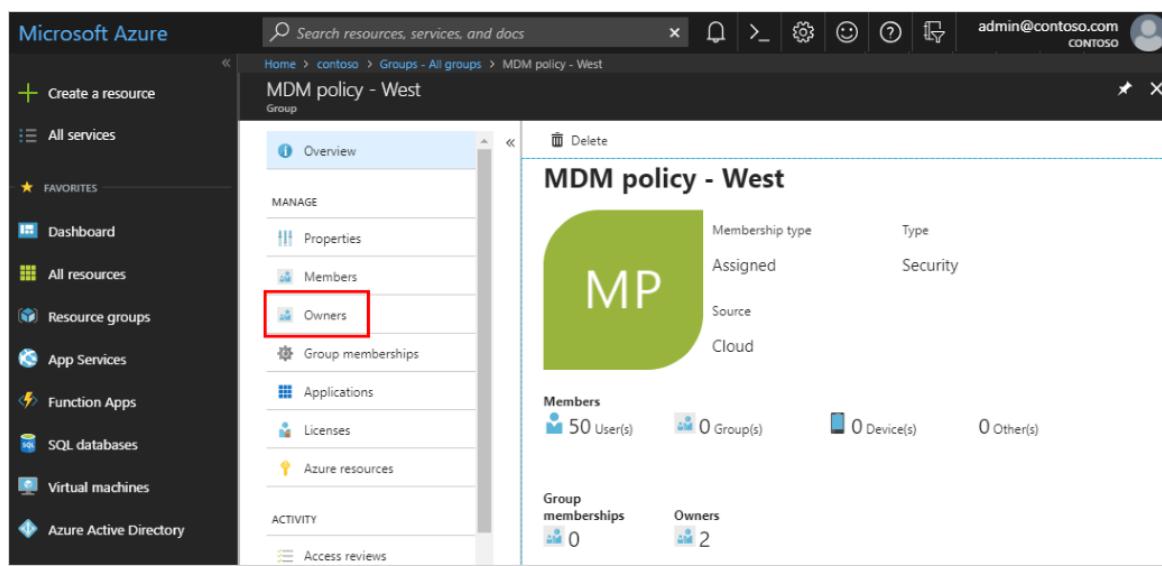
When a group has no owner, group-managing administrators are still able to manage the group. It is recommended for every group to have at least one owner. Once owners are assigned to a group, the last owner of the group cannot be removed. Please make sure to select another owner before removing the last owner from the group.

Add an owner to a group

Below are instructions for adding a user as an owner to a group using the Azure AD portal. To add a service principal as an owner of a group, follow the instructions to do so using [PowerShell](#).

To add a group owner

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, select **Groups**, and then select the group for which you want to add an owner (for this example, *MDM policy - West*).
3. On the **MDM policy - West Overview** page, select **Owners**.



The screenshot shows the Microsoft Azure portal interface. The left sidebar is dark-themed and includes links for 'Create a resource', 'All services', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', and 'Azure Active Directory'. Under 'Azure Active Directory', 'Groups' is selected. The main content area shows the 'MDM policy - West' group overview. The 'Overview' tab is selected. On the left, a 'MANAGE' sidebar lists 'Properties', 'Members', 'Owners' (which is highlighted with a red box), 'Group memberships', 'Applications', 'Licenses', and 'Azure resources'. The main panel displays the group's details: 'Membership type' is 'Assigned', 'Type' is 'Security', 'Source' is 'Cloud'. Below this, there are sections for 'Members' (50 User(s), 0 Group(s), 0 Device(s), 0 Other(s)), 'Group memberships' (0), and 'Owners' (2). The top navigation bar shows the user 'admin@contoso.com' and 'CONTOSO'.

4. On the **MDM policy - West - Owners** page, select **Add owners**, and then search for and select the user that will be the new group owner, and then choose **Select**.

The screenshot shows the 'MDM policy - West - Owners' page in the Azure portal. On the left, there's a navigation sidebar with options like Overview, Properties, Members, Owners (which is selected and highlighted in blue), Group memberships, Applications, Licenses, and Azure resources. Under Activity, there are Access reviews and Audit logs. In the main content area, there's a list of owners: Danielle McKay and Eggert Schafer. At the top right, there's a '+ Add owners' button with a red box around it. To the right of the list, there's a 'Selected owners:' section which currently says 'No owners selected'. Below that is a 'Select' button with a red box around it. The URL in the browser is 'Home > contoso > Groups - All groups > MDM policy - West - Owners'.

After you select the new owner, you can refresh the **Owners** page and see the name added to the list of owners.

Remove an owner from a group

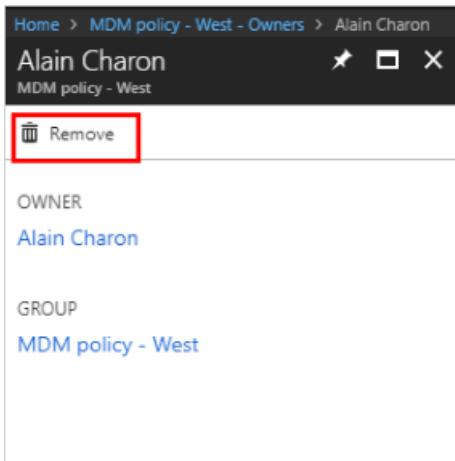
Remove an owner from a group using Azure AD.

To remove an owner

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, select **Groups**, and then select the group for which you want to remove an owner (for this example, *MDM policy - West*).
3. On the **MDM policy - West Overview** page, select **Owners**.

The screenshot shows the 'MDM policy - West' overview page in the Azure portal. On the left, there's a navigation sidebar with options like Overview, Properties, Members, Owners (which is selected and highlighted in blue), Group memberships, Applications, Licenses, and Azure resources. Under Activity, there are Access reviews and Audit logs. In the main content area, there's a large green button with 'MP' on it. To its right, there are sections for Membership type (Assigned), Type (Security), Source (Cloud), and Members (50 User(s)). Below that, there are sections for Group memberships (0) and Owners (3). The URL in the browser is 'Home > contoso > Groups - All groups > MDM policy - West'.

4. On the **MDM policy - West - Owners** page, select the user you want to remove as a group owner, choose **Remove** from the user's information page, and select **Yes** to confirm your decision.



After you remove the owner, you can return to the **Owners** page and see the name has been removed from the list of owners.

Next steps

- [Managing access to resources with Azure Active Directory groups](#)
- [Azure Active Directory cmdlets for configuring group settings](#)
- [Use groups to assign access to an integrated SaaS app](#)
- [Integrating your on-premises identities with Azure Active Directory](#)
- [Azure Active Directory cmdlets for configuring group settings](#)

Manage app and resource access using Azure Active Directory groups

4/10/2022 • 3 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) lets you use groups to manage access to your cloud-based apps, on-premises apps, and your resources. Your resources can be part of the Azure AD organization, such as permissions to manage objects through roles in Azure AD, or external to the organization, such as for Software as a Service (SaaS) apps, Azure services, SharePoint sites, and on-premises resources.

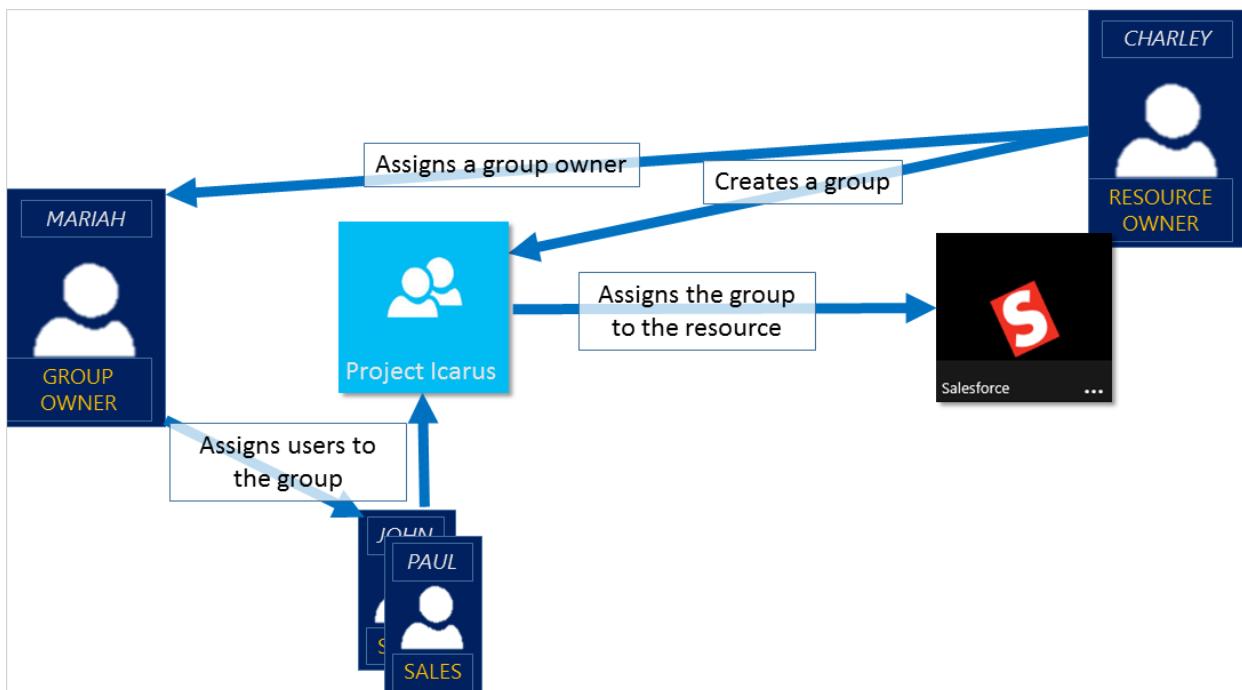
NOTE

In the Azure portal, you can see some groups whose membership and group details you can't manage in the portal:

- Groups synced from on-premises Active Directory can be managed only in on-premises Active Directory.
- Other group types such as distribution lists and mail-enabled security groups are managed only in Exchange admin center or Microsoft 365 admin center. You must sign in to Exchange admin center or Microsoft 365 admin center to manage these groups.

How access management in Azure AD works

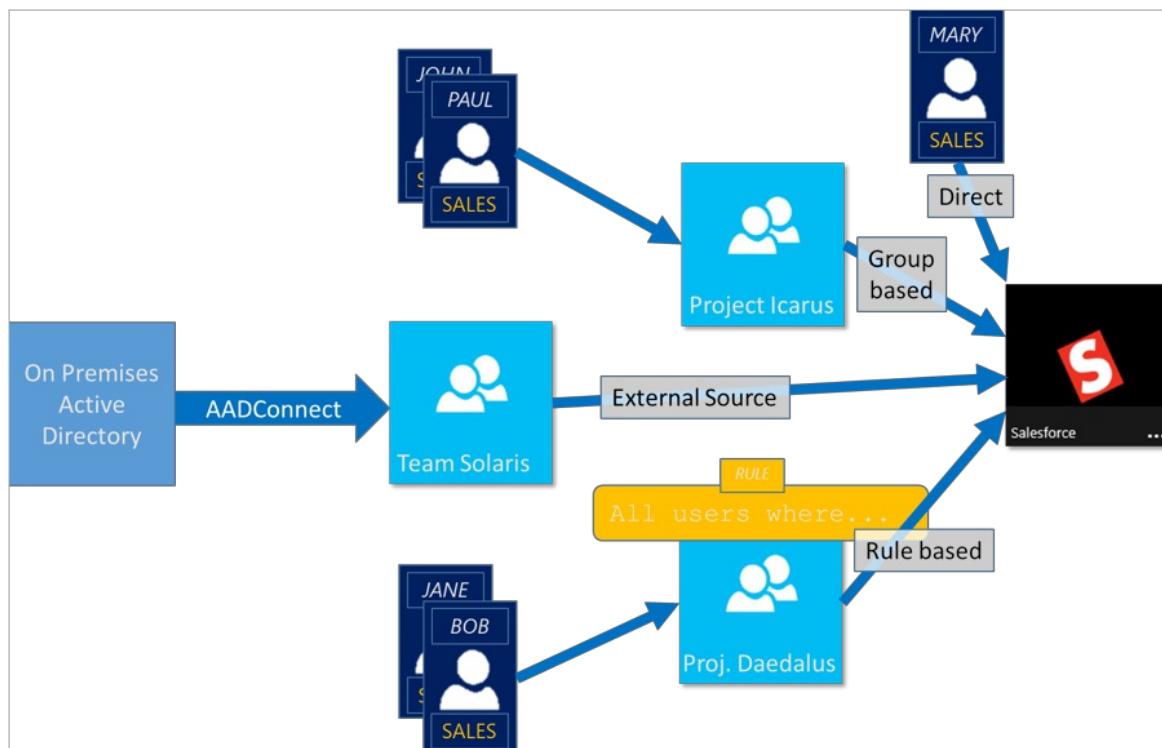
Azure AD helps you give access to your organization's resources by providing access rights to a single user or to an entire Azure AD group. Using groups lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one. The resource or directory owner can also give management rights for the member list to someone else, such as a department manager or a Helpdesk administrator, letting that person add and remove members, as needed. For more information about how to manage group owners, see [Manage group owners](#)



Ways to assign access rights

There are four ways to assign resource access rights to your users:

- **Direct assignment.** The resource owner directly assigns the user to the resource.
- **Group assignment.** The resource owner assigns an Azure AD group to the resource, which automatically gives all of the group members access to the resource. Group membership is managed by both the group owner and the resource owner, letting either owner add or remove members from the group. For more information about adding or removing group membership, see [How to: Add or remove a group from another group using the Azure Active Directory portal](#).
- **Rule-based assignment.** The resource owner creates a group and uses a rule to define which users are assigned to a specific resource. The rule is based on attributes that are assigned to individual users. The resource owner manages the rule, determining which attributes and values are required to allow access to the resource. For more information, see [Create a dynamic group and check status](#).
- **External authority assignment.** Access comes from an external source, such as an on-premises directory or a SaaS app. In this situation, the resource owner assigns a group to provide access to the resource and then the external source manages the group members.



Can users join groups without being assigned?

The group owner can let users find their own groups to join, instead of assigning them. The owner can also set up the group to automatically accept all users that join or to require approval.

After a user requests to join a group, the request is forwarded to the group owner. If it's required, the owner can approve the request and the user is notified of the group membership. However, if you have multiple owners and one of them disapproves, the user is notified, but isn't added to the group. For more information and instructions about how to let your users request to join groups, see [Set up Azure AD so users can request to join groups](#)

Next steps

Now that you have a bit of an introduction to access management using groups, you start to manage your resources and apps.

- [Create a new group using Azure Active Directory](#) or [Create and manage a new group using PowerShell cmdlets](#)

- Use groups to assign access to an integrated SaaS app
- Sync an on-premises group to Azure using Azure AD Connect

Add or deactivate custom security attributes in Azure AD (Preview)

4/10/2022 • 10 minutes to read • [Edit Online](#)

IMPORTANT

Custom security attributes are currently in PREVIEW. See the [Supplemental Terms of Use for Microsoft Azure Previews](#) for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Custom security attributes in Azure Active Directory (Azure AD) are business-specific attributes (key-value pairs) that you can define and assign to Azure AD objects. This article describes how to add, edit, or deactivate custom security attributes.

Prerequisites

To add or deactivate custom security attributes, you must have:

- Azure AD Premium P1 or P2 license
- [Attribute Definition Administrator](#)
- [AzureADPreview](#) version 2.0.2.138 or later when using PowerShell

IMPORTANT

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Add an attribute set

An attribute set is a collection of related attributes. All custom security attributes must be part of an attribute set. Attribute sets cannot be renamed or deleted.

1. Sign in to the [Azure portal](#) or [Azure AD admin center](#).
2. Click **Azure Active Directory > Custom security attributes (Preview)**.
3. Click **Add attribute set** to add a new attribute set.

If Add attribute set is disabled, make sure you are assigned the Attribute Definition Administrator role.

For more information, see [Troubleshoot custom security attributes](#).

4. Enter a name, description, and maximum number of attributes.

An attribute set name can be 32 characters with no spaces or special characters. Once you've specified a name, you can't rename it. For more information, see [Limits and constraints](#).

The screenshot shows the Azure Active Directory Custom security attributes (Preview) interface. On the left, there's a navigation sidebar with options like Overview, Preview features, Diagnose and solve problems, Recommendations (Preview), Manage (with sub-options like Users, Groups, etc.), and Custom security attributes (Preview). The main area is titled 'Contoso | Custom security attributes' and shows a list of existing attribute sets. A modal window titled 'New attribute set' is open on the right, prompting for a name ('Engineering'), description ('Attributes for engineering organization'), and maximum number of attributes (set to 25). There's also a 'Search attribute set' input field and a blue 'Add' button at the bottom.

- When finished, click **Add**.

The new attribute set appears in the list of attribute sets.

Add a custom security attribute

- Sign in to the [Azure portal](#) or [Azure AD admin center](#).
- Click **Azure Active Directory > Custom security attributes (Preview)**.
- On the Custom security attributes page, find an existing attribute set or click **Add attribute set** to add a new attribute set.

All custom security attributes must be part of an attribute set.

- Click to open the selected attribute set.
- Click **Add attribute** to add a new custom security attribute to the attribute set.

Home > Contoso > Engineering >

New attribute

Add a custom security attribute (key-value pair) to your directory that you can later assign to Azure AD objects, such as users or applications. [Learn more](#)

Attribute name *	<input type="text"/>				
Description	<input type="text"/>				
Data type *	String				
Allow multiple values to be assigned	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Only allow predefined values to be assigned	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Predefined values	<input type="button" value="Add value"/> <table border="1"> <thead> <tr> <th>Value</th> <th>Is active?</th> </tr> </thead> <tbody> <tr> <td colspan="2">No results</td> </tr> </tbody> </table>	Value	Is active?	No results	
Value	Is active?				
No results					
<input type="button" value="Save"/>					

6. In the **Attribute name** box, enter a custom security attribute name.

A custom security attribute name can be 32 characters with no spaces or special characters. Once you've specified a name, you can't rename it. For more information, see [Limits and constraints](#).

7. In the **Description** box, enter an optional description.

A description can be 128 characters long. If necessary, you can later change the description.

8. From the **Data type** list, select the data type for the custom security attribute.

DATA TYPE	DESCRIPTION
Boolean	A Boolean value that can be true, True, false, or False.
Integer	A 32-bit integer.
String	A string that can be X characters long.

9. For **Allow multiple values to be assigned**, select **Yes** or **No**.

Select **Yes** to allow multiple values to be assigned to this custom security attribute. Select **No** to only allow a single value to be assigned to this custom security attribute.

10. For **Only allow predefined values to be assigned**, select **Yes** or **No**.

Select **Yes** to require that this custom security attribute be assigned values from a predefined values list. Select **No** to allow this custom security attribute to be assigned user-defined values or potentially predefined values.

11. If **Only allow predefined values to be assigned** is **Yes**, click **Add value** to add predefined values.

An active value is available for assignment to objects. A value that is not active is defined, but not yet available for assignment.

The screenshot shows two overlapping windows. The background window is titled 'New attribute' and displays a form for creating a custom security attribute. It includes fields for 'Attribute name' (set to 'Project'), 'Description' (set to 'Active projects for user'), 'Data type' (set to 'String'), and options for allowing multiple values ('Yes') and predefined values ('Yes'). A 'Predefined values' section is present but empty. The foreground window is titled 'Add predefined value' and shows a single entry: 'Value *' set to 'Baker'. There is also an 'Is active?' checkbox which is checked.

12. When finished, click **Save**.

The new custom security attribute appears in the list of custom security attributes.

13. If you want to include predefined values, follow the steps in the next section.

Edit a custom security attribute

Once you add a new custom security attribute, you can later edit some of the properties. Some properties are immutable and cannot be changed.

1. Sign in to the [Azure portal](#) or [Azure AD admin center](#).
2. Click **Azure Active Directory > Custom security attributes (Preview)**.
3. Click the attribute set that includes the custom security attribute you want to edit.
4. In the list of custom security attributes, click the ellipsis for the custom security attribute you want to edit and then click **Edit attribute**.
5. Edit the properties that are enabled.
6. If **Only allow predefined values to be assigned** is **Yes**, click **Add value** to add predefined values.
Click an existing predefined value to change the **Is active?** setting.

The screenshot shows the Azure AD admin center interface. On the left, there's a navigation bar with 'Home > Contoso > Engineering > Project'. The main area is titled 'Project' and contains fields for 'Attribute name' (set to 'Project'), 'Description' (set to 'Active projects for user'), 'Data type' (set to 'String'), and 'Allow multiple values to be assigned' (set to 'Yes'). Below these are sections for 'Predefined values' and 'Only allow predefined values to be assigned' (also set to 'Yes'). A 'Save' button is at the bottom. On the right, a modal window titled 'Add predefined value' is open, asking to 'Add a single predefined value of the selected data type.' It has a 'Value *' field containing 'Alpine' with a checkmark, and an 'Is active?' checkbox which is checked. There's also a 'Baker' entry in the list. A blue 'Add' button is at the bottom right of the modal.

Deactivate a custom security attribute

Once you add a custom security attribute, you can't delete it. However, you can deactivate a custom security attribute.

1. Sign in to the [Azure portal](#) or [Azure AD admin center](#).
2. Click **Azure Active Directory > Custom security attributes (Preview)**.
3. Click the attribute set that includes the custom security attribute you want to deactivate.
4. In the list of custom security attributes, add a check mark next to the custom security attribute you want to deactivate.
5. Click **Deactivate attribute**.
6. In the Deactivate attribute dialog that appears, click **Yes**.

The custom security attribute is deactivated and moved to the Deactivated attributes list.

PowerShell

To manage custom security attributes in your Azure AD organization, you can also use the PowerShell. The following command can manage attribute sets and custom security attributes.

Get all attribute sets

Use the `Get-AzureADMSAttributeSet` command without any parameters to get all attribute sets.

```
Get-AzureADMSAttributeSet
```

Get an attribute set

Use the `Get-AzureADMSAttributeSet` command to get an attribute set.

- Attribute set: `Engineering`

```
Get-AzureADMSAttributeSet -Id "Engineering"
```

Add an attribute set

Use the `New-AzureADMSAttributeSet` command to add a new attribute set.

- Attribute set: `Engineering`

```
New-AzureADMSAttributeSet -Id "Engineering" -Description "Attributes for engineering team" -  
MaxAttributesPerSet 10
```

Update an attribute set

Use the [Set-AzureADMSAttributeSet](#) command to update an attribute set.

- Attribute set: `Engineering`

```
Set-AzureADMSAttributeSet -Id "Engineering" -Description "Attributes for cloud engineering team"  
Set-AzureADMSAttributeSet -Id "Engineering" -MaxAttributesPerSet 20
```

Get all custom security attributes

Use the [Get-AzureADMSCustomSecurityAttributeDefinition](#) command without any parameters to get all custom security attribute definitions.

```
Get-AzureADMSCustomSecurityAttributeDefinition
```

Get a custom security attribute

Use the [Get-AzureADMSCustomSecurityAttributeDefinition](#) command to get a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`

```
Get-AzureADMSCustomSecurityAttributeDefinition -Id "Engineering_ProjectDate"
```

Add a custom security attribute

Use the [New-AzureADMSCustomSecurityAttributeDefinition](#) command to add a new custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`
- Attribute data type: String

```
New-AzureADMSCustomSecurityAttributeDefinition -AttributeSet "Engineering" -Name "ProjectDate" -Description  
"Target completion date" -Type "String" -Status "Available" -IsCollection $false -IsSearchable $true -  
UsePreDefinedValuesOnly $true
```

Update a custom security attribute

Use the [Set-AzureADMSCustomSecurityAttributeDefinition](#) command to update a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`

```
Set-AzureADMSCustomSecurityAttributeDefinition -Id "Engineering_ProjectDate" -Description "Target completion  
date (YYYY/MM/DD)"
```

Deactivate a custom security attribute

Use the [Set-AzureADMSCustomSecurityAttributeDefinition](#) command to deactivate a custom security attribute

definition.

- Attribute set: `Engineering`
- Attribute: `Project`

```
Set-AzureADMSCustomSecurityAttributeDefinition -Id "Engineering_Project" -Status "Deprecated"
```

Get all predefined values

Use the [Get-AzureADMSCustomSecurityAttributeDefinitionAllowedValue](#) command to get all predefined values for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`

```
Get-AzureADMSCustomSecurityAttributeDefinitionAllowedValue -CustomSecurityAttributeDefinitionId "Engineering_Project"
```

Get a predefined value

Use the [Get-AzureADMSCustomSecurityAttributeDefinitionAllowedValue](#) command to get a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

```
Get-AzureADMSCustomSecurityAttributeDefinitionAllowedValue -CustomSecurityAttributeDefinitionId "Engineering_Project" -Id "Alpine"
```

Add a predefined value

Use the [Add-AzureADMScustomSecurityAttributeDefinitionAllowedValues](#) command to add a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

```
Add-AzureADMScustomSecurityAttributeDefinitionAllowedValues -CustomSecurityAttributeDefinitionId "Engineering_Project" -Id "Alpine" -IsActive $true
```

Deactivate a predefined value

Use the [Set-AzureADMSCustomSecurityAttributeDefinitionAllowedValue](#) command to deactivate a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

```
Set-AzureADMSCustomSecurityAttributeDefinitionAllowedValue -CustomSecurityAttributeDefinitionId "Engineering_Project" -Id "Alpine" -IsActive $false
```

To manage custom security attributes in your Azure AD organization, you can also use the Microsoft Graph API. The following API calls can be made to manage attribute sets and custom security attributes.

Get all attribute sets

Use the [List attributeSets](#) API to get all attribute sets.

```
GET https://graph.microsoft.com/beta/directory/attributeSets
```

Get top attribute sets

Use the [List attributeSets](#) API to get the top attribute sets.

```
GET https://graph.microsoft.com/beta/directory/attributeSets?$top=10
```

Get attribute sets in order

Use the [List attributeSets](#) API to get attribute sets in order.

```
GET https://graph.microsoft.com/beta/directory/attributeSets?$orderBy=id
```

Get an attribute set

Use the [Get attributeSet](#) API to get an attribute set.

- Attribute set: `Engineering`

```
GET https://graph.microsoft.com/beta/directory/attributeSets/Engineering
```

Add an attribute set

Use the [Create attributeSet](#) API to add a new attribute set.

- Attribute set: `Engineering`

```
POST https://graph.microsoft.com/beta/directory/attributeSets
{
    "id": "Engineering",
    "description": "Attributes for engineering team",
    "maxAttributesPerSet": 25
}
```

Update an attribute set

Use the [Update attributeSet](#) API to update an attribute set.

- Attribute set: `Engineering`

```
PATCH https://graph.microsoft.com/beta/directory/attributeSets/Engineering
{
    "description": "Attributes for engineering team",
    "maxAttributesPerSet": 20
}
```

Get all custom security attributes

Use the [List customSecurityAttributeDefinitions](#) API to get all custom security attribute definitions.

```
GET https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions
```

Filter custom security attributes

Use the [List customSecurityAttributeDefinitions](#) API to filter custom security attribute definitions.

- Filter: Attribute name eq 'Project' and status eq 'Available'

```
GET https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions?  
$filter=name+eq+'Project'%20and%20status+eq+'Available'
```

- Filter: Attribute set eq 'Engineering' and status eq 'Available' and data type eq 'String'

```
GET https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions?  
$filter=attributeSet+eq+'Engineering'%20and%20status+eq+'Available'%20and%20type+eq+'String'
```

Get a custom security attribute

Use the [Get customSecurityAttributeDefinition](#) API to get a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`

```
GET https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_ProjectDate
```

Add a custom security attribute

Use the [Create customSecurityAttributeDefinition](#) API to add a new custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`
- Attribute data type: String

```
POST https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions  
{  
    "attributeSet": "Engineering",  
    "description": "Target completion date",  
    "isCollection": false,  
    "isSearchable": true,  
    "name": "ProjectDate",  
    "status": "Available",  
    "type": "String",  
    "usePreDefinedValuesOnly": false  
}
```

Add a custom security attribute that supports multiple predefined values

Use the [Create customSecurityAttributeDefinition](#) API to add a new custom security attribute definition that supports multiple predefined values.

- Attribute set: `Engineering`
- Attribute: `Project`
- Attribute data type: Collection of Strings

```
POST https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions
{
    "attributeSet": "Engineering",
    "description": "Active projects for user",
    "isCollection": true,
    "isSearchable": true,
    "name": "Project",
    "status": "Available",
    "type": "String",
    "usePreDefinedValuesOnly": true
}
```

Add a custom security attribute with a list of predefined values

Use the [Create customSecurityAttributeDefinition](#) API to add a new custom security attribute definition with a list of predefined values.

- Attribute set: `Engineering`
- Attribute: `Project`
- Attribute data type: Collection of Strings
- Predefined values: `Alpine`, `Baker`, `Cascade`

```
POST https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions
{
    "attributeSet": "Engineering",
    "description": "Active projects for user",
    "isCollection": true,
    "isSearchable": true,
    "name": "Project",
    "status": "Available",
    "type": "String",
    "usePreDefinedValuesOnly": true,
    "allowedValues": [
        {
            "id": "Alpine",
            "isActive": true
        },
        {
            "id": "Baker",
            "isActive": true
        },
        {
            "id": "Cascade",
            "isActive": true
        }
    ]
}
```

Update a custom security attribute

Use the [Update customSecurityAttributeDefinition](#) API to update a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`

```
PATCH https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_ProjectDate
{
    "description": "Target completion date (YYYY/MM/DD)",
}
```

Update the predefined values for a custom security attribute

Use the [Update customSecurityAttributeDefinition](#) API to update the predefined values for a custom security

attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Attribute data type: Collection of Strings
- Update predefined value: `Baker`
- New predefined value: `Skagit`

NOTE

For this request, you must add the **OData-Version** header and assign it the value `4.01`.

```
PATCH https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_Project
{
    "allowedValues@delta": [
        {
            "id": "Baker",
            "isActive": false
        },
        {
            "id": "Skagit",
            "isActive": true
        }
    ]
}
```

Deactivate a custom security attribute

Use the [Update customSecurityAttributeDefinition](#) API to deactivate a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`

```
PATCH https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_Project
{
    "status": "Deprecated"
}
```

Get all predefined values

Use the [List allowedValues](#) API to get all predefined values for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`

```
GET
https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_Project/allowedValues
```

Get a predefined value

Use the [Get allowedValue](#) API to get a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

```
GET  
https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_Project/allowedValues/Alpine
```

Add a predefined value

Use the [Create allowedValue](#) API to add a predefined value for a custom security attribute definition.

You can add predefined values for custom security attributes that have `usePreDefinedValuesOnly` set to `true`.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

```
POST  
https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_Project/allowedValues  
{  
    "id":"Alpine",  
    "isActive":"true"  
}
```

Deactivate a predefined value

Use the [Update allowedValue](#) API to deactivate a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

```
PATCH  
https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions/Engineering_Project/allowedValues/Alpine  
{  
    "isActive":"false"  
}
```

Frequently asked questions

Can you delete custom security attribute definitions?

No, you can't delete custom security attribute definitions. You can only [deactivate custom security attribute definitions](#). Once you deactivate a custom security attribute, it can no longer be applied to the Azure AD objects. Custom security attribute assignments for the deactivated custom security attribute definition are not automatically removed. There is no limit to the number of deactivated custom security attributes. You can have 500 active custom security attribute definitions per tenant with 100 allowed predefined values per custom security attribute definition.

Next steps

- [Manage access to custom security attributes in Azure AD](#)
- [Assign or remove custom security attributes for a user](#)
- [Assign or remove custom security attributes for an application](#)

Manage access to custom security attributes in Azure AD (Preview)

4/10/2022 • 7 minutes to read • [Edit Online](#)

IMPORTANT

Custom security attributes are currently in PREVIEW. See the [Supplemental Terms of Use for Microsoft Azure Previews](#) for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

For people in your organization to effectively work with [custom security attributes](#), you must grant the appropriate access. Depending on the information you plan to include in custom security attributes, you might want to restrict custom security attributes or you might want to make them broadly accessible in your organization. This article describes how to manage access to custom security attributes.

Prerequisites

To manage access to custom security attributes, you must have:

- Azure AD Premium P1 or P2 license
- [Attribute Assignment Administrator](#)

IMPORTANT

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Step 1: Figure out how to organize your attributes

Every custom security attribute must be part of an attribute set. An attribute set is a way to group and manage related custom security attributes. You'll need to figure out how you want to add attributes sets for your organization. For example, you might want to add attribute sets based on departments, teams, or projects. Your ability to grant access to custom security attributes will depend on how you organize your attribute sets.

Attribute set:
Engineering



Certification={true, false}
CostCenter={1001,1002, 1003}
Project={Alpine, Baker, Cascade}
ProjectDate={}

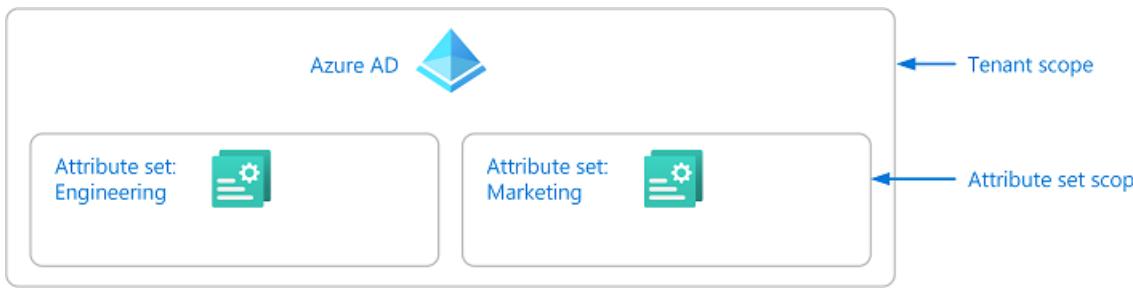
Attribute set:
Marketing



AppCountry={}
AppSensitivity={High, Medium, Low}
Level={Internal, Public, Secure}
OnlineExpansion={Global, Local, All}

Step 2: Identify the needed scope

Scope is the set of resources that the access applies to. For custom security attributes, you can assign roles at tenant scope or at attribute set scope. If you want to assign broad access, you can assign roles at tenant scope. However, if you want to limit access to particular attribute sets, you can assign roles at attribute set scope.



Azure AD role assignments are an additive model, so your effective permissions are the sum of your role assignments. For example, if you assign a user a role at tenant scope and assign the same user the same role at attribute set scope, the user will still have permissions at tenant scope.

Step 3: Review the available roles

You need to determine who needs access to work with custom security attributes in your organization. To help you manage access to custom security attributes, there are four Azure AD built-in roles. By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes. If necessary, a Global Administrator can assign these roles to themselves.

- [Attribute Definition Administrator](#)
- [Attribute Assignment Administrator](#)
- [Attribute Definition Reader](#)
- [Attribute Assignment Reader](#)

The following table provides a high-level comparison of the custom security attributes roles.

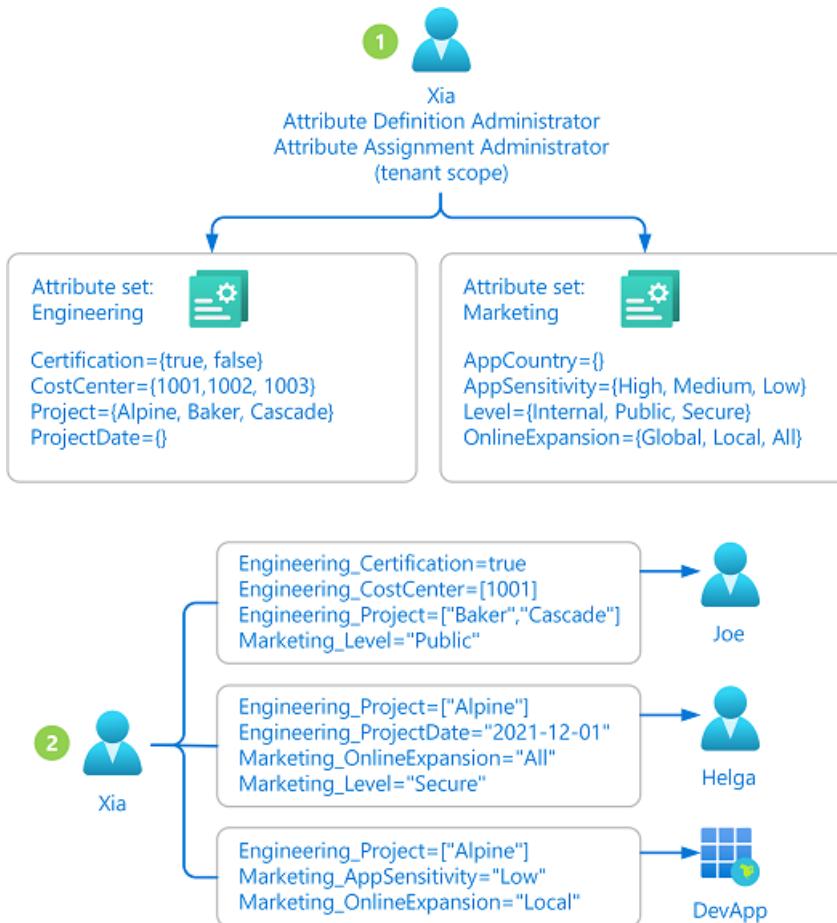
PERMISSION	GLOBAL ADMIN	ATTRIBUTE DEFINITION ADMIN	ATTRIBUTE ASSIGNMENT ADMIN	ATTRIBUTE DEFINITION READER	ATTRIBUTE ASSIGNMENT READER
Read attribute sets		✓	✓	✓	✓
Read attribute definitions		✓	✓	✓	
Read attribute assignments for users and applications (service principals)			✓		✓
Add or edit attribute sets		✓			
Add, edit, or deactivate attribute definitions		✓			
Assign attributes to users and applications (service principals)			✓		

Step 4: Determine your delegation strategy

This step describes two ways you can manage access to custom security attributes. The first way is to manage them centrally and the second way is to delegate management to others.

Manage attributes centrally

An administrator that has been assigned the Attribute Definition Administrator and Attribute Assignment Administrator roles at tenant scope can manage all aspects of custom security attributes. The following diagram shows how custom security attributes are defined and assigned by a single administrator.

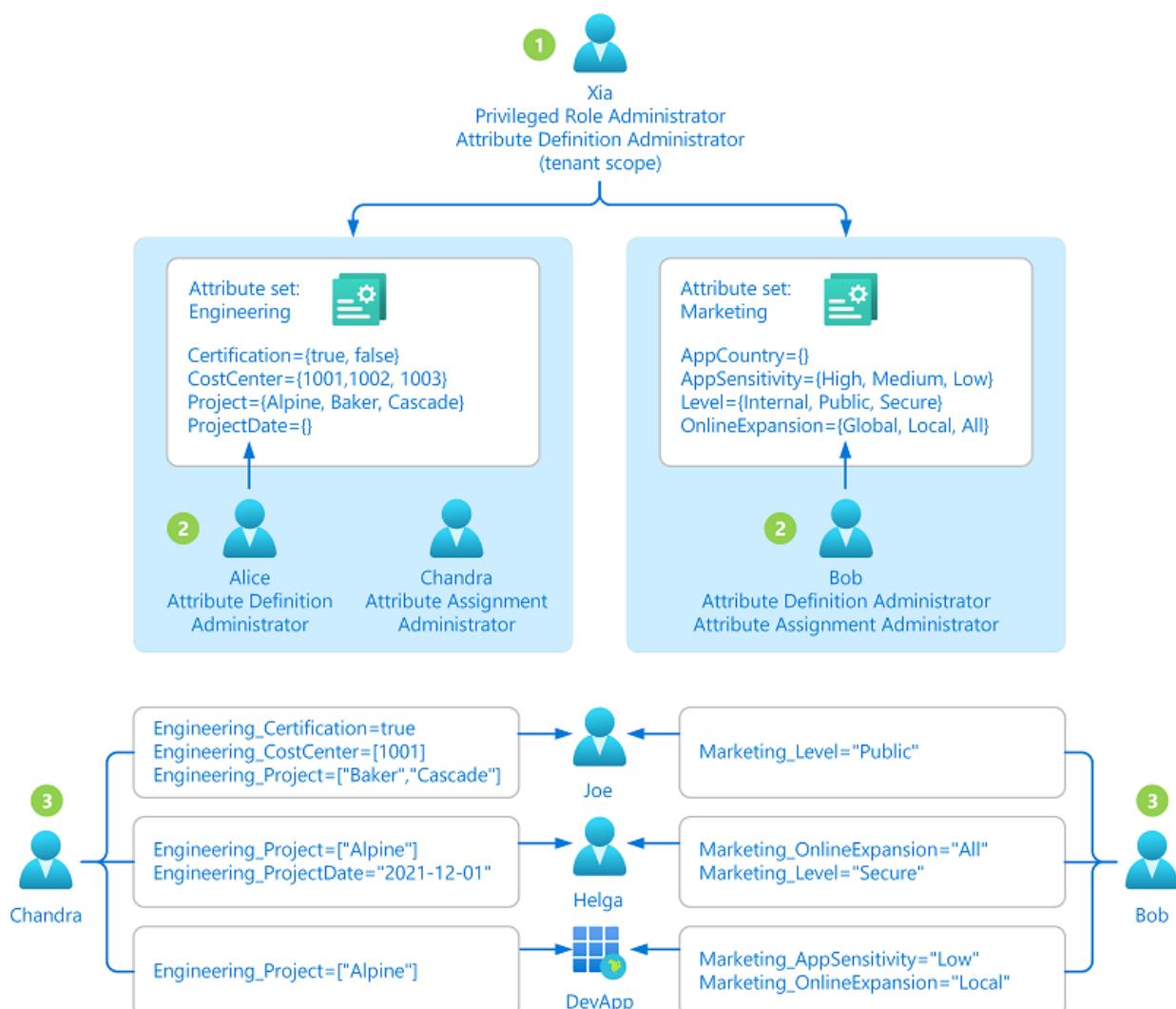


1. The administrator (Xia) has both the Attribute Definition Administrator and Attribute Assignment Administrator roles assigned at tenant scope. The administrator adds attribute sets and defines attributes.
2. The administrator assigns attributes to Azure AD objects.

Managing attributes centrally has the advantage that it can be managed by one or two administrators. The disadvantage is that the administrator might get several requests to define or assign custom security attributes. In this case, you might want to delegate management.

Manage attributes with delegation

An administrator may not know all the situations of how custom security attributes should be defined and assigned. Typically it's users within the respective departments, teams, or projects who know the most about their area. Instead of assigning one or two administrators to manage all custom security attributes, you can instead delegate the management at attribute set scope. This also follows the best practice of least privilege to grant just the permissions other administrators need to do their job and avoid unnecessary access. The following diagram shows how the management of custom security attributes can be delegated to multiple administrators.



1. The administrator (Xia) with the Attribute Definition Administrator role assigned at tenant scope adds attribute sets. The administrator also has permissions to assign roles to others (Privileged Role Administrator) and delegates who can read, define, or assign custom security attributes for each attribute set.
2. The delegated Attribute Definition Administrators (Alice and Bob) define attributes in the attribute sets they have been granted access to.
3. The delegated Attribute Assignment Administrators (Chandra and Bob) assign attributes from their attribute sets to Azure AD objects.

Step 5: Select the appropriate roles and scope

Once you have a better understanding of how your attributes will be organized and who needs access, you can select the appropriate custom security attribute roles and scope. The following table can help you with the selection.

I WANT TO GRANT THIS ACCESS	ASSIGN THIS ROLE	SCOPE
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant • Add or edit all attribute sets in a tenant • Add, edit, or deactivate all attribute definitions in a tenant 	Attribute Definition Administrator	 Tenant

I WANT TO GRANT THIS ACCESS	ASSIGN THIS ROLE	SCOPE
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Add, edit, or deactivate attribute definitions in a scoped attribute set • Cannot update the scoped attribute set • Cannot read, add, or update other attribute sets 	Attribute Definition Administrator	 Attribute set
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant • Read all attribute assignments in a tenant for users • Read all attribute assignments in a tenant for applications (service principals) • Assign all attributes in a tenant to users • Assign all attributes in a tenant to applications (service principals) • Author Azure role assignment conditions that use the Principal attribute for all attributes in a tenant 	Attribute Assignment Administrator	 Tenant
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Read attribute assignments that use attributes in a scoped attribute set for users • Read attribute assignments that use attributes in a scoped attribute set for applications (service principals) • Assign attributes in a scoped attribute set to users • Assign attributes in a scoped attribute set to applications (service principals) • Author Azure role assignment conditions that use the Principal attribute for all attributes in a scoped attribute set • Cannot read attributes in other attribute sets • Cannot read attribute assignments that use attributes in other attribute sets 	Attribute Assignment Administrator	 Attribute set

I WANT TO GRANT THIS ACCESS	ASSIGN THIS ROLE	SCOPE
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant 	Attribute Definition Reader	 Tenant
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Cannot read other attribute sets 	Attribute Definition Reader	 Attribute set
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute assignments in a tenant for users • Read all attribute assignments in a tenant for applications (service principals) 	Attribute Assignment Reader	 Tenant
<ul style="list-style-type: none"> • Read attribute assignments that use attributes in a scoped attribute set for users • Read attribute assignments that use attributes in a scoped attribute set for applications (service principals) • Cannot read attribute assignments that use attributes in other attribute sets 	Attribute Assignment Reader	 Attribute set

Step 6: Assign roles

To grant access to the appropriate people, follow these steps to assign one of the custom security attribute roles.

Assign roles at attribute set scope

1. Sign in to the [Azure portal](#) or [Azure AD admin center](#).
2. Click **Azure Active Directory**.
3. In the left navigation menu, click **Custom security attributes (Preview)**.
4. Click the attribute set you want grant access to.
5. Click **Roles and administrators**.

Microsoft Azure Search resources, services, and docs (G+)

Dashboard > Contoso > Project

Project | Roles and administrators

Active attributes | Deactivated attributes | Refresh | Preview features | Got feedback?

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

Administrative roles

Administrative roles are used for granting access for privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. [Learn more](#).

Assignable roles are roles that can be assigned here to allow managing this resource. Directory-level roles have inherited access to this resource and can only be assigned at the directory level [here](#).

Role	Description	Type
Attribute assignment administrator	Can assign attribute keys and values to Azure AD objects.	Built-in
Attribute assignment reader	Reads attribute keys and values to Azure AD objects.	Built-in
Attribute definition administrator	Can define and manage the definition of security attributes for the tenant.	Built-in
Attribute definition reader	Read the definition of security attributes for the tenant.	Built-in

6. Add assignments for the custom security attribute roles.

NOTE

If you are using Azure AD Privileged Identity Management (PIM), eligible role assignments at attribute set scope currently aren't supported. Permanent role assignments at attribute set scope are supported, but the **Assigned roles** page for a user doesn't list the role assignments.

NOTE

Users with attribute set scope role assignments currently can see other attribute sets and custom security attribute definitions.

Assign roles at tenant scope

1. Sign in to the [Azure portal](#) or [Azure AD admin center](#).
2. Click **Azure Active Directory**.
3. In the left navigation menu, click **Roles and administrators**.

Microsoft Azure Search resources, services, and docs (G+)

Dashboard > Contoso

Contoso | Roles and administrators

New custom role | Delete custom role | Refresh | Preview features | Got feedback?

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

Your Role: Global administrator and 1 other roles

Administrative roles

Administrative roles are used for granting access for privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. [Learn more](#). [Learn more](#).

Role	Description	Type
Attribute assignment administrator	Can assign attribute keys and values to Azure AD objects.	Built-in
Attribute assignment reader	Reads attribute keys and values to Azure AD objects.	Built-in
Attribute definition administrator	Can define and manage the definition of security attributes for the tenant.	Built-in
Attribute definition reader	Read the definition of security attributes for the tenant.	Built-in

4. Add assignments for the custom security attribute roles.

View audit logs for attribute changes

Sometimes you need information about custom security attribute changes, such as for auditing or troubleshooting purposes. Anytime someone makes changes to definitions or assignments, the changes get logged in the [Azure AD audit logs](#).

Here are the custom security attribute-related activities that are logged:

- Add attribute set
- Update attribute set
- Add custom security attribute definition
- Update custom security attribute definition
- Assign custom security attribute
- Remove custom security attribute

The following screenshot shows an example of the audit log. To filter the logs for custom security attribute-related activities, select the **Category** filter and then select **AttributeManagement**.

The screenshot shows the Azure Active Directory Audit logs interface. On the left, there's a sidebar with navigation links like Home, Contoso, Application proxy, Custom security attributes (Preview), Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Security, Monitoring, Sign-in logs, Audit logs (which is currently selected), and Provisioning logs. The main area displays a table of audit logs with columns for Date, Service, Category, and Status. A dropdown menu is open over the 'Category' filter, showing a list of categories: All, AdministrativeUnit, Agreement, ApplicationManagement, AttributeManagement (which is selected), Authentication, CompanyAssociation, Contact, CrossTenantAccessSettings, Device, DeviceConfiguration, and DirectoryManagement. At the bottom right of the dropdown is an 'Apply' button. The table data is as follows:

Date	Service	Category	Status
11/1/2021, 12:53:22 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:52:53 PM	Core Directory	UserManagement	Success
11/1/2021, 12:52:53 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:52:40 PM	Core Directory	UserManagement	Success
11/1/2021, 12:52:40 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:52:17 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:52:17 PM	Core Directory	UserManagement	Success
11/1/2021, 12:51:50 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:51:43 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:51:29 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:51:05 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:51:05 PM	Core Directory	AttributeManagement	Success
11/1/2021, 12:51:00 PM	Core Directory	AttributeManagement	Success

Next steps

- [Add or deactivate custom security attributes in Azure AD](#)
- [Assign or remove custom security attributes for a user](#)
- [Troubleshoot custom security attributes in Azure AD](#)

Troubleshoot custom security attributes in Azure AD (Preview)

4/10/2022 • 4 minutes to read • [Edit Online](#)

IMPORTANT

Custom security attributes are currently in PREVIEW. See the [Supplemental Terms of Use for Microsoft Azure Previews](#) for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Symptom - Custom security attributes page is disabled

When signed in to the Azure portal as Global Administrator and you try to access the **Custom security attributes** page, it is disabled.

The screenshot shows the Azure portal's 'Overview' page. On the left, there is a sidebar with various icons and links. One of the links, 'Custom security attributes (Preview)', is highlighted with a red rectangular box. The main content area on the right displays basic information about the tenant, including 'Name', 'Tenant ID', 'Primary d', 'License', and a 'My feed' section. There is also a circular icon with the letters 'RA'.

Cause

Custom security attributes requires an Azure AD Premium P1 or P2 license.

Solution

Open **Azure Active Directory > Overview** and check the license for your tenant.

Symptom - Add attribute set is disabled

When signed in to the Azure portal as Global Administrator and you try to click the **Custom security attributes > Add attribute set** option, it is disabled.

The screenshot shows the 'Contoso | Custom security attributes (Preview)' page in the Azure Active Directory portal. On the left, there's a navigation menu with various options like Overview, Preview features, Diagnose and solve problems, Recommendations (Preview), Manage, Users, Groups, etc. The 'Custom security attributes (Preview)' option is selected and highlighted with a grey background. At the top right, there are buttons for '+ Add attribute set', Refresh, and Got feedback?. Below the header, there's a section titled 'Get started with custom security attributes' with a brief description and a 'Learn more' link. To the right of this, there are three numbered steps: 1. Check permissions, 2. Add attribute sets, and 3. Manage attribute sets. Each step has a small icon and a brief description. The 'Add attribute sets' step has its own 'Add attribute set' button, which is also highlighted with a red box.

Cause

You don't have permissions to add an attribute set. To add an attribute set and custom security attributes, you must be assigned the [Attribute Definition Administrator](#) role. By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution

Make sure that you are assigned the [Attribute Definition Administrator](#) role at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Azure AD](#).

Symptom - Error when you try to assign a custom security attribute

When you try to save a custom security attribute assignment, you get the message:

```
Insufficient privileges to save custom security attributes  
This account does not have the necessary admin privileges to change custom security attributes
```

Cause

You don't have permissions to assign custom security attributes. To assign custom security attributes, you must be assigned the [Attribute Assignment Administrator](#) role. By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution

Make sure that you are assigned the [Attribute Assignment Administrator](#) role at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Azure AD](#).

Symptom - Cannot filter custom security attributes for users or applications

Cause 1

You don't have permissions to filter custom security attributes. To read and filter custom security attributes for users or enterprise applications, you must be assigned the [Attribute Assignment Reader](#) or [Attribute Assignment Administrator](#) role. By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution 1

Make sure that you are assigned one of the following Azure AD built-in roles at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Azure AD](#).

- [Attribute Assignment Administrator](#)
- [Attribute Assignment Reader](#)

Cause 2

You are assigned the Attribute Assignment Reader or Attribute Assignment Administrator role, but you have not been assigned access to an attribute set.

Solution 2

You can delegate the management of custom security attributes at the tenant scope or at the attribute set scope. Make sure you have been assigned access to an attribute set at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Azure AD](#).

Cause 3

There are no custom security attributes defined and assigned yet for your tenant.

Solution 3

Add and assign custom security attributes to users or enterprise applications. For more information, see [Add or deactivate custom security attributes in Azure AD](#), [Assign or remove custom security attributes for a user](#), or [Assign or remove custom security attributes for an application](#).

Symptom - Custom security attributes cannot be deleted

Cause

Currently, you can only activate and deactivate custom security attribute definitions. Deletion of custom security attributes is not supported. Deactivated definitions do not count towards the tenant wide 500 definition limit.

Solution

Deactivate the custom security attributes you no longer need. For more information, see [Add or deactivate custom security attributes in Azure AD](#).

Symptom - Cannot add a role assignment at an attribute set scope using PIM

When you try to add an eligible Azure AD role assignment using [Azure AD Privileged Identity Management \(PIM\)](#), you cannot set the scope to an attribute set.

Cause

PIM currently does not support adding an eligible Azure AD role assignment at an attribute set scope.

Symptom - Insufficient privileges when using Graph Explorer

When you try to use [Graph Explorer](#) to call Microsoft Graph APIs for custom security attributes, you see a message similar to the following:

```
Forbidden - 403. You need to consent to the permissions on the Modify permissions (Preview) tab  
Authorization_RequestDenied  
Insufficient privileges to complete the operation.
```

The screenshot shows the Microsoft Graph Explorer interface. At the top, there's a navigation bar with links like 'Solutions', 'Graph Explorer', 'Get Started', 'Docs', 'Changelog', 'Resources', and 'Developer Program'. Below the navigation bar, the main area is titled 'Graph Explorer' and shows a user profile with the initials 'A' and the name 'Admin'. There are tabs for 'Request body', 'Request headers', 'Modify permissions (Preview)', and 'Access token'. A 'Run query' button is located at the top right. In the center, there's a search bar with the URL 'https://graph.microsoft.com/beta/directory/customSecurityAttributeDefinitions'. Below the search bar, a red error message box displays the text: 'Forbidden - 403 - 112ms. You need to consent to the permissions on the Modify permissions (Preview) tab' and 'Authorization_RequestDenied'. 'Insufficient privileges to complete the operation.' A 'Response preview' section shows the JSON error response: { "error": { "code": "Authorization_RequestDenied", "message": "Insufficient privileges to complete the operation.", "innerError": { "date": "2022-01-14T00:09:53", "request-id": "client-request-id" } } }. To the left of the error message, there's a sidebar with sections like 'Getting Started (8)' containing various API endpoints such as 'my profile', 'my profile (beta)', 'my photo', 'my mail', and 'all the items in my drive'.

Cause 1

You have not consented to the required custom security attribute permissions to make the API call.

Solution 1

Open the Permissions panel, select the appropriate custom security attribute permission, and click **Consent**. In the Permissions requested window that appears, review the requested permissions.

Permissions

To try out different Microsoft Graph API endpoints, choose the permissions, and then click Consent.

attribute

Permission	Admin consent requir...	Status
CustomSecAttributeAssignment (1)	CustomSecAttributeAssignme...	Consented
CustomSecAttributeDefinition (1)	CustomSecAttributeDefinition....	

1 selected: CustomSecAttributeDefinition.ReadWrite.All

Consent **Cancel**

Cause 2

You are not assigned the required custom security attribute role to make the API call. By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution 2

Make sure that you are assigned the required custom security attribute role. For more information, see [Manage access to custom security attributes in Azure AD](#).

Next steps

- [Manage access to custom security attributes in Azure AD](#)
- [Troubleshoot Azure role assignment conditions](#)

How to find your Azure Active Directory tenant ID

4/10/2022 • 2 minutes to read • [Edit Online](#)

Azure subscriptions have a trust relationship with Azure Active Directory (Azure AD). Azure AD is trusted to authenticate users, services, and devices for the subscription. Each subscription has a tenant ID associated with it, and there are a few ways you can find the tenant ID for your subscription.

Find tenant ID through the Azure portal

1. Sign in to the [Azure portal](#).
2. Select **Azure Active Directory**.
3. Select **Properties**.
4. Then, scroll down to the **Tenant ID** field. Your tenant ID will be in the box.

The screenshot shows the 'First Up Consultants' tenant properties page in the Azure portal. On the left, a sidebar lists various Azure services: Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties (which is selected and highlighted in grey), and Security. The main pane displays 'Tenant properties' for the 'First Up Consultants' tenant. It includes fields for Name (set to 'First Up Consultants'), Country or region (set to 'United States'), Location (set to 'United States datacenters'), and Notification language (set to 'English'). The 'Tenant ID' field is highlighted with a red border and contains the value 'x0xx10-00x0-0x01-0xx-x0x01xx100'. Below these fields are sections for Technical contact (set to 'admin@firstupconsultants.com') and Global privacy contact (empty).

Find tenant ID with PowerShell

You can also find the tenant programmatically. To find the tenant ID with Azure PowerShell, use the cmdlet `Get-AzTenant`.

```
Connect-AzAccount  
Get-AzTenant
```

For more information, see this Azure PowerShell cmdlet reference for [Get-AzTenant](#).

Find tenant ID with CLI

If you want to use a command-line interface to find the tenant ID, you can do so with [Azure CLI](#) or [Microsoft 365 CLI](#).

For Azure CLI, use one of the commands `az login`, `az account list`, or `az account tenant list` as shown in the following example. Notice the `tenantId` property for each of your subscriptions in the output from each command.

```
az login  
az account list  
az account tenant list
```

For more information, see [az login command reference](#), [az account command reference](#), or [az account tenant command reference](#).

For Microsoft 365 CLI, use the cmdlet `tenant id get` as shown in the following example:

```
m365 tenant id get
```

For more information, see the Microsoft 365 [tenant id get command reference](#).

Next steps

- To create a new Azure AD tenant, see [Quickstart: Create a new tenant in Azure Active Directory](#).
- To learn how to associate or add a subscription to a tenant, see [Associate or add an Azure subscription to your Azure Active Directory tenant](#).
- To learn how to find the object ID, see [Find the user object ID](#).

Find help and open a support ticket for Azure Active Directory

4/10/2022 • 3 minutes to read • [Edit Online](#)

Microsoft provides global technical, pre-sales, billing, and subscription support for Azure Active Directory (Azure AD). Support is available both online and by phone for Microsoft Azure paid and trial subscriptions. Phone support and online billing support are available in additional languages.

Find help without opening a support ticket

Before creating a support ticket, check out the following resources for answers and information.

- For content such as how-to information or code samples for IT professionals and developers, see the [technical documentation at docs.microsoft.com](#).
- The [Microsoft Technical Community](#) is the place for our IT pro partners and customers to collaborate, share, and learn. The [Microsoft Technical Community Info Center](#) is used for announcements, blog posts, ask-me-anything (AMA) interactions with experts, and more. You can also [join the community to submit your ideas](#).

Open a support ticket

If you are unable to find answers by using self-help resources, you can open an online support ticket. You should open each support ticket for only a single problem, so that we can connect you to the support engineers who are subject matter experts for your problem. Also, Azure Active Directory engineering teams prioritize their work based on incidents that are generated, so you're often contributing to service improvements.

How to open a support ticket for Azure AD in the Azure portal

NOTE

- For billing or subscription issues, you must use the [Microsoft 365 admin center](#).
- If you're using Azure AD B2C, open a support ticket by first switching to an Azure AD tenant that has an Azure subscription associated with it. Typically, this is your employee tenant or the default tenant created for you when you signed up for an Azure subscription. To learn more, see [how an Azure subscription is related to Azure AD](#).

1. Sign in to [the Azure portal](#) and open Azure Active Directory.
2. Scroll down to **Troubleshooting + Support** and select **New support request**.
3. On the **Basics** blade, for **Issue type**, select **Technical**.
4. Select your **Subscription**.
5. For **Service**, select **Azure Active Directory**.
6. Create a **Summary** for the request. The summary must be under 140 characters.
7. Select a **Problem type**, and then select a category for that type. At this point, you are also offered self-help information for your problem category.
8. Add the rest of your problem information and click **Next**.

- At this point, you are offered self-help solutions and documentation in the **Solutions** blade. If none of the solutions there resolve your problem, click **Next**.
- On the **Details** blade, fill out the required details and select a **Severity**.

All services > Microsoft | New support request

Microsoft | New support request

Azure Active Directory

Search (Ctrl+ /) <>

Basics **Solutions** **Details** **Review + create**

Information provided on this tab will be used to further assess your issue and help the support engineer troubleshoot the problem. Verify the contact information before moving to the Review + Create.

PROBLEM DETAILS

When did the problem start? MM/DD/YYYY Enter in local time

* Description Provide additional information about your issue

File upload Select a file

Consent Share diagnostic information (i)

SUPPORT METHOD

Support plan Azure Support Plan - Internal

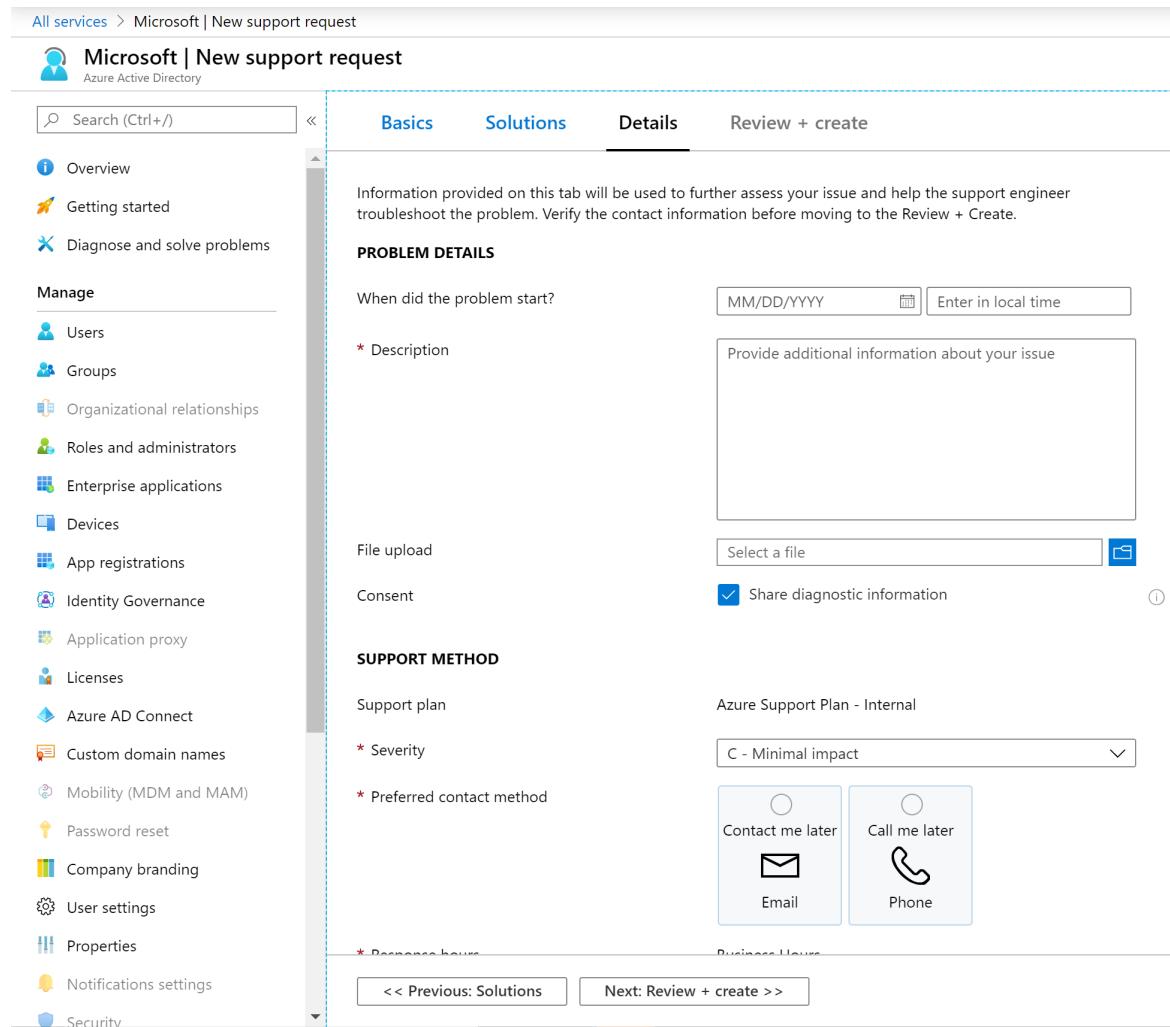
* Severity C - Minimal impact ▼

* Preferred contact method

Contact me later Call me later
 Email  Phone

* Response hours Business hours

<< Previous: Solutions Next: Review + create >>



- Provide your contact information and select **Next**.

- Provide your contact information and select **Create**.

Home >

Microsoft | New support request

Azure Active Directory

Search (Ctrl+ /) Basics Solutions Details Review + create

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

Company branding

User settings

Properties

Security

Monitoring

Sign-ins

Audit logs

Provisioning logs (Preview)

Logs

Diagnostic settings

Workbooks

Usage & insights

Troubleshooting + Support

Virtual assistant (Preview)

New support request

BASICS

Issue type	Technical
Subscription	IBIZA - Test (76cb77fa-8b17-4eab-9493-b65dace99813)
Service	Azure Active Directory App Integration and Development
Problem type	Issues Signing In to Applications
Problem subtype	On-premises apps via Azure AD application proxy
Summary	testing

TERMS, CONDITIONS AND PRIVACY POLICY

By clicking "Create" you accept the [terms and conditions](#).
View our [privacy policy](#).

DETAILS

Full Error Message:	AAD0505 - Error message
Consent	Share diagnostic information

SUPPORT METHOD

Severity	B - Moderate impact
Support plan	Azure Support Plan - Internal
Your availability	Business Hours
Support language	English
Contact method	Email

CONTACT INFO

Contact name	[REDACTED]
Email	[REDACTED]

<< Previous: Details Create

How to open a support ticket for Azure AD in the Microsoft 365 admin center

NOTE

Support for Azure AD in the [Microsoft 365 admin center](#) is offered for administrators only.

1. Sign in to the [Microsoft 365 admin center](#) with an account that has an Enterprise Mobility + Security (EMS) license.
2. On the **Support** tile, select **New service request**:
3. On the **Support Overview** page, select **Identity management** or **User and domain management**:
4. For **Feature**, select the Azure AD feature for which you want support.
5. For **Symptom**, select an appropriate symptom, summarize your issue and provide relevant details, and then select **Next**.
6. Select one of the offered self-help resources, or select **Yes, continue** or **No, cancel request**.
7. If you continue, you are asked for more details. You can attach any files you have that represent the problem, and then select **Next**.
8. Provide your contact information and select **Submit request**.

Get phone support

See the [Contact Microsoft for support](#) page to obtain support phone numbers.

Next steps

- [Microsoft Tech Community](#)
- [Technical documentation at docs.microsoft.com](#)

Support and help options for Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

If you need an answer to a question or help in solving a problem not covered in our documentation, it might be time to reach out to experts for help. Here are several suggestions for getting answers to your questions as you use Azure Active Directory (Azure AD).

Create an Azure support request

Explore the range of [Azure support options and choose the plan](#) that best fits, whether you're an IT admin managing your organization's tenant, a developer just starting your cloud journey, or a large organization deploying business-critical, strategic applications. Azure customers can create and manage support requests in the Azure portal.

- If you already have an Azure Support Plan, [open a support request here](#).
- If you're not an Azure customer, you can open a support request with [Microsoft Support for business](#).

Post a question to Microsoft Q&A



Get answers to your identity and access management questions directly from Microsoft engineers, Azure Most Valuable Professionals (MVPs), and members of our expert community.

[Microsoft Q&A](#) is Azure's recommended source of community support.

If you can't find an answer to your problem by searching Microsoft Q&A, submit a new question. Use one of following tags when you ask your [high-quality question](#):

COMPONENT/AREA	TAGS
Active Directory Authentication Library (ADAL)	[adal]
Microsoft Authentication Library (MSAL)	[msal]
Open Web Interface for .NET (OWIN) middleware	[azure-active-directory]
Azure AD B2B / External Identities	[azure-ad-b2b]
Azure AD B2C	[azure-ad-b2c]

COMPONENT/AREA	TAGS
Microsoft Graph API	[azure-ad-graph]
All other authentication and authorization areas	[azure-active-directory]

Stay informed of updates and new releases

- [Azure Updates](#): Learn about important product updates, roadmap, and announcements.
- [What's new in Azure AD](#): Get to know what's new in Azure AD including the latest release notes, known issues, bug fixes, deprecated functionality, and upcoming changes.
- [Azure Active Directory Identity Blog](#): Get news and information about Azure AD.
- [Tech Community](#): Share your experiences, engage and learn from experts.

What's new for Azure Active Directory in Microsoft 365 Government

4/10/2022 • 2 minutes to read • [Edit Online](#)

We've made some changes to Azure Active Directory (Azure AD) in the Microsoft 365 Government cloud instance, which is applicable to customers using the following services:

- Microsoft Azure Government
- Microsoft 365 Government – GCC High
- Microsoft 365 Government – DoD

This article doesn't apply to Microsoft 365 Government – GCC customers.

Changes to the initial domain name

During your organization's initial sign-up for a Microsoft 365 Government online service, you were asked to choose your organization's domain name, <your-domain-name>.onmicrosoft.com. If you already have a domain name with the .com suffix, nothing will change.

However, if you're signing up for a new Microsoft 365 Government service, you'll be asked to choose a domain name using the .us suffix. So, it will be <your-domain-name>.onmicrosoft.us.

NOTE

This change doesn't apply to any customers who are managed by cloud service providers (CSPs).

Changes to portal access

We've updated the portal endpoints for Microsoft Azure Government, Microsoft 365 Government – GCC High, and Microsoft 365 Government – DoD, as shown in the [Endpoint mapping table](#).

Previously customers could sign in using the worldwide Azure (portal.azure.com) and Office 365 (portal.office.com) portals. With this update, customers must now sign in using the specific Microsoft Azure Government, Microsoft 365 Government - GCC High, and Microsoft 365 Government - DoD portals.

Endpoint mapping

The following table shows the endpoints for all customers:

NAME	ENDPOINT DETAILS
Portals	Microsoft Azure Government: https://portal.azure.us Microsoft 365 Government – GCC High: https://portal.office365.us Microsoft 365 Government – DoD: https://portal.apps.mil
Azure Active Directory Authority Endpoint	https://login.microsoftonline.us

NAME	ENDPOINT DETAILS
Microsoft Graph API for Microsoft 365 Government - GCC High	https://graph.microsoft.us
Microsoft Graph API for Microsoft 365 Government - DoD	https://dod-graph.microsoft.us
Azure Government services endpoints	For details, see Azure Government developer guide
Microsoft 365 Government - GCC High endpoints	For details, see Office 365 U.S. Government GCC High endpoints
Microsoft 365 Government - DoD	For details, see Office 365 U.S. Government DoD endpoints

Next steps

For more information, see these articles:

- [What is Azure Government?](#)
- [Azure Government AAD Authority Endpoint Update](#)
- [Microsoft Graph endpoints in US Government cloud](#)
- [Office 365 US Government GCC High and DoD](#)

Archive for What's new in Azure Active Directory?

4/10/2022 • 298 minutes to read • [Edit Online](#)

The primary [What's new in Azure Active Directory? release notes](#) article contains updates for the last six months, while this article contains all the older information.

The What's new in Azure Active Directory? release notes provide information about:

- The latest releases
- Known issues
- Bug fixes
- Deprecated functionality
- Plans for changes

September 2021

Limits on the number of configured API permissions for an application registration will be enforced starting in October 2021

Type: Plan for change

Service category: Other

Product capability: Developer Experience

Occasionally, application developers configure their apps to require more permissions than it's possible to grant. To prevent this from happening, we're enforcing a limit on the total number of required permissions that can be configured for an app registration.

The total number of required permissions for any single application registration must not exceed 400 permissions, across all APIs. The change to enforce this limit will begin rolling out no sooner than mid-October 2021. Applications exceeding the limit can't increase the number of permissions they're configured for. The existing limit on the number of distinct APIs for which permissions are required remains unchanged and can't exceed 50 APIs.

In the Azure portal, the required permissions are listed under Azure Active Directory > Application registrations > (select an application) > API permissions. Using Microsoft Graph or Microsoft Graph PowerShell, the required permissions are listed in the requiredResourceAccess property of an application entity. [Learn more](#).

My Apps performance improvements

Type: Fixed

Service category: My Apps

Product capability: End User Experiences

The load time of My Apps has been improved. Users going to myapps.microsoft.com load My Apps directly, rather than being redirected through another service. [Learn more](#).

Single Page Apps using the `spa` redirect URI type must use a CORS enabled browser for auth

Type: Known issue

Service category: Authentications (Logins)

Product capability: Developer Experience

The modern Edge browser is now included in the requirement to provide an `Origin` header when redeeming a [single page app authorization code](#). A compatibility fix accidentally exempted the modern Edge browser from CORS controls, and that bug is being fixed during October. A subset of applications depended on CORS being disabled in the browser, which has the side effect of removing the `Origin` header from traffic. This is an unsupported configuration for using Azure AD, and these apps that depended on disabling CORS can no longer use modern Edge as a security workaround. All modern browsers must now include the `Origin` header per HTTP spec, to ensure CORS is enforced. [Learn more](#).

General availability - On the My Apps portal, users can choose to view their apps in a list

Type: New feature

Service category: My Apps

Product capability: End User Experiences

By default, My Apps displays apps in a grid view. Users can now toggle their My Apps view to display apps in a list. [Learn more](#).

General availability - New and enhanced device-related audit logs

Type: New feature

Service category: Audit

Product capability: Device Lifecycle Management

Admins can now see various new and improved device-related audit logs. The new audit logs include the create and delete passwordless credentials (Phone sign-in, FIDO2 key, and Windows Hello for Business), register/unregister device and pre-create/delete pre-create device. Additionally, there have been minor improvements to existing device-related audit logs that include adding more device details. [Learn more](#).

General availability - Azure AD users can now view and report suspicious sign-ins and manage their accounts within Microsoft Authenticator

Type: New feature

Service category: Microsoft Authenticator App

Product capability: Identity Security & Protection

This feature allows Azure AD users to manage their work or school accounts within the Microsoft Authenticator app. The management features will allow users to view sign-in history and sign-in activity. They can report any suspicious or unfamiliar activity based on the sign-in history and activity if necessary. Users also can change their Azure AD account passwords and update the account's security information. [Learn more](#).

General availability - New MS Graph APIs for role management

Type: New feature

Service category: RBAC

Product capability: Access Control

New APIs for role management to MS Graph v1.0 endpoint are generally available. Instead of old [directory roles](#), use [unifiedRoleDefinition](#) and [unifiedRoleAssignment](#).

General availability - Access Packages can expire after number of hours

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

It's now possible in entitlement management to configure an access package that will expire in a matter of hours in addition to the previous support for days or specific dates. [Learn more](#).

New provisioning connectors in the Azure AD Application Gallery - September 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [BLDNG APP](#)
- [Cato Networks](#)
- [Rouse Sales](#)
- [SchoolStream ASA](#)
- [Taskize Connect](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD Application gallery - September 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In September 2021, we have added following 44 new applications in our App gallery with Federation support

[Studybugs](#), [Yello](#), [LawVu](#), [Formate eVo Mail](#), [Revenue Grid](#), [Orbit for Office 365](#), [Upmarket](#), [Alinto Protect](#), [Cloud Concinnity](#), [Matlantis](#), [ModelGen for Visio \(MG4V\)](#), [NetRef: Classroom Management](#), [VergeSense](#), [iAuditor](#), [Secutraq](#), [Active and Thriving](#), [Inova](#), [TerraTrue](#), [Facebook Work Accounts](#), [Beyond Identity Admin Console](#), [Visult](#), [ENGAGE TAG](#), [Appaegis Isolation Access Cloud](#), [CrowdStrike Falcon Platform](#), [MY Emergency Control](#), [AlexisHR](#), [Teachme Biz](#), [Zero Networks](#), [Mavim iMprove](#), [Azumuta](#), [Frankli](#), [Amazon Managed Grafana](#), [Productive](#), [Create!Webフロー](#), [Evercate](#), [Ezra Coaching](#), [Baldwin Safety and Compliance](#), [Nulab Pass \(Backlog,Cacoo,Typetalk\)](#), [Metatask](#), [Contrast Security](#), [Animaker](#), [Traction Guest](#), [True Office Learning - LIO](#), [Qiita Team](#)

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here:

<https://aka.ms/AzureADAppRequest>

Gmail users signing in on Microsoft Teams mobile and desktop clients will sign in with device login flow starting September 30, 2021

Type: Changed feature

Service category: B2B

Product capability: B2B/B2C

Starting on September 30 2021, Azure AD B2B guests and Azure AD B2C customers signing in with their self-service signed up or redeemed Gmail accounts will have an extra login step. Users will now be prompted to enter a code in a separate browser window to finish signing in on Microsoft Teams mobile and desktop clients. If you haven't already done so, make sure to modify your apps to use the system browser for sign-in.

See [Embedded vs System Web Ulin the MSAL.NET documentation](#) for more information. All MSAL SDKs use the system web-view by default.

As the device login flow will start September 30, 2021, it may not be available in your region immediately. If it's not available yet, your end-users will be met with the error screen shown in the doc until it gets deployed to your region.) For more details on the device login flow and details on requesting extension to Google, see [Add Google as an identity provider for B2B guest users](#).

Improved Conditional Access Messaging for Non-compliant Device

Type: Changed feature

Service category: Conditional Access

Product capability: End User Experiences

The text and design on the Conditional Access blocking screen shown to users when their device is marked as non-compliant has been updated. Users will be blocked until they take the necessary actions to meet their company's device compliance policies. Additionally, we have streamlined the flow for a user to open their device management portal. These improvements apply to all conditional access supported OS platforms. [Learn more](#)

August 2021

New major version of AADConnect available

Type: Fixed

Service category: AD Connect

Product capability: Identity Lifecycle Management

We've released a new major version of Azure Active Directory Connect. This version contains several updates of foundational components to the latest versions and is recommended for all customers using Azure AD Connect. [Learn more](#).

Public Preview - Azure AD single Sign on and device-based Conditional Access support in Firefox on Windows 10

Type: New feature

Service category: Authentications (Logins)

Product capability: SSO

We now support native single sign-on (SSO) support and device-based Conditional Access to the Firefox browser on Windows 10 and Windows Server 2019. Support is available in Firefox version 91. [Learn more](#).

Public preview - beta MS Graph APIs for Azure AD access reviews returns list of contacted reviewer names

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

We've released beta MS Graph API for Azure AD access reviews. The API has methods to return a list of contacted reviewer names in addition to the reviewer type. [Learn more](#).

General Availability - "Register or join devices" user action in Conditional Access

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

The "Register or join devices" user action is generally available in Conditional access. This user action allows you to control multi-factor authentication policies for Azure Active Directory (AD) device registration. Currently, this user action only allows you to enable multi-factor authentication as a control when users register or join devices to Azure AD. Other controls that are dependent on or not applicable to Azure AD device registration continue to be disabled with this user action. [Learn more](#).

General Availability - customers can scope reviews of privileged roles to eligible or permanent assignments

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

Administrators can now create access reviews of only permanent or eligible assignments to privileged Azure AD or Azure resource roles. [Learn more](#).

General availability - assign roles to Azure Active Directory (AD) groups

Type: New feature

Service category: RBAC

Product capability: Access Control

Assigning roles to Azure AD groups is now generally available. This feature can simplify the management of role assignments in Azure AD for Global Administrators and Privileged Role Administrators. [Learn more](#).

New Federated Apps available in Azure AD Application gallery - Aug 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In August 2021, we have added following 46 new applications in our App gallery with Federation support:

Sirix Customer Dashboard, STRUXI, Autodesk Construction Cloud - Meetings, Eccentex AppBase for Azure, Bookado, FilingRamp, BenQ IAM, Rhombus Systems, CorporateExperience, TutorOcean, Bookado Device, HiFives-AD-SSO, Darzin, Simply Stakeholders, KACTUS HCM - Smart People, Five9 UC Adapter for Microsoft Teams V2, Automation Center, Cirrus Identity Bridge for Azure AD, ShiftWizard SAML, Safesend Returns, Brushup, directprint.io Cloud Print Administration, plain-x,X-point Cloud, SmartHub INFER, Fresh Relevance, FluentPro G.A. Suite, Clockwork Recruiting, WalkMe SAML2.0, Sideways 6, Kronos Workforce Dimensions, SysTrack Cloud Edition, mailworx Dynamics CRM Connector, Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service, Peripass, JobDiva, Sanebox For Office365, Tulip, HP Wolf Security, Genesys Engage cloud Email, Meta Wiki, Palo Alto Networks Cloud Identity Engine Directory Sync, Valarea, LanSchool Air, Catalyst, Webcargo

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here:

<https://aka.ms/AzureADAppRequest>

New provisioning connectors in the Azure AD Application Gallery - August 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Chatwork](#)
- [Freshservice](#)
- [InviteDesk](#)
- [Maptician](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Multifactor fraud report – new audit event

Type: Changed feature

Service category: MFA

Product capability: Identity Security & Protection

To help administrators understand that their users are blocked for multi-factor authentication as a result of fraud report, we've added a new audit event. This audit event is tracked when the user reports fraud. The audit log is available in addition to the existing information in the sign-in logs about fraud report. To learn how to get the audit report, see [multi-factor authentication Fraud alert](#).

Improved Low-Risk Detections

Type: Changed feature

Service category: Identity Protection

Product capability: Identity Security & Protection

To improve the quality of low risk alerts that Identity Protection issues, we've modified the algorithm to issue fewer low risk Risky Sign-Ins. Organizations may see a significant reduction in low risk sign-in in their environment. [Learn more](#).

Non-interactive risky sign-ins

Type: Changed feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Identity Protection now emits risky sign-ins on non-interactive sign-ins. Admins can find these risky sign-ins using the **sign-in type** filter in the risky sign-ins report. [Learn more](#).

Change from User Administrator to Identity Governance Administrator in Entitlement Management

Type: Changed feature

Service category: Roles

Product capability: Identity Governance

The permissions assignments to manage access packages and other resources in Entitlement Management are moving from the User Administrator role to the Identity Governance administrator role.

Users that have been assigned the User administrator role can longer create catalogs or manage access packages in a catalog they don't own. If users in your organization have been assigned the User administrator role to configure catalogs, access packages, or policies in entitlement management, they will need a new assignment. You should instead assign these users the Identity Governance administrator role. [Learn more](#)

Windows Azure Active Directory connector is deprecated

Type: Deprecated

Service category: Microsoft Identity Manager

Product capability: Identity Lifecycle Management

The Windows Azure AD Connector for FIM is at feature freeze and deprecated. The solution of using FIM and the Azure AD Connector has been replaced. Existing deployments should migrate to [Azure AD Connect](#), Azure AD Connect Sync, or the [Microsoft Graph Connector](#), as the internal interfaces used by the Azure AD Connector for FIM are being removed from Azure AD. [Learn more](#).

Retirement of older Azure AD Connect versions

Type: Deprecated

Service category: AD Connect

Product capability: User Management

Starting August 31 2022, all V1 versions of Azure AD Connect will be retired. If you haven't already done so, you need to update your server to Azure AD Connect V2.0. You need to make sure you're running a recent version of Azure AD Connect to receive an optimal support experience.

If you run a retired version of Azure AD Connect it may unexpectedly stop working. You may also not have the latest security fixes, performance improvements, troubleshooting, and diagnostic tools and service enhancements. Also, if you require support we can't provide you with the level of service your organization needs.

See [Azure Active Directory Connect V2.0](#), what has changed in V2.0 and how this change impacts you.

Retirement of support for installing MIM on Windows Server 2008 R2 or SQL Server 2008 R2

Type: Deprecated

Service category: Microsoft Identity Manager

Product capability: Identity Lifecycle Management

Deploying MIM Sync, Service, Portal or CM on Windows Server 2008 R2, or using SQL Server 2008 R2 as the underlying database, is deprecated as these platforms are no longer in mainstream support. Installing MIM Sync and other components on Windows Server 2016 or later, and with SQL Server 2016 or later, is recommended.

Deploying MIM for Privileged Access Management with a Windows Server 2012 R2 domain controller in the PRIV forest is deprecated. Use Windows Server 2016 or later Active Directory, with Windows Server 2016 functional level, for your PRIV forest domain. The Windows Server 2012 R2 functional level is still permitted for a CORP forest's domain. [Learn more](#).

July 2021

New Google sign-in integration for Azure AD B2C and B2B self-service sign-up and invited external users will stop working starting July 12, 2021

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

Previously we announced that [the exception for Embedded WebViews for Gmail authentication will expire in the second half of 2021](#).

On July 7, 2021, we learned from Google that some of these restrictions will apply starting **July 12, 2021**. Azure AD B2B and B2C customers who set up a new Google ID sign-in in their custom or line of business applications to invite external users or enable self-service sign-up will have the restrictions applied immediately. As a result, end-users will be met with an error screen that blocks their Gmail sign-in if the authentication is not moved to a system webview. See the docs linked below for details.

Most apps use system web-view by default, and will not be impacted by this change. This only applies to customers using embedded webviews (the non-default setting.) We advise customers to move their application's authentication to system browsers instead, prior to creating any new Google integrations. To learn how to move to system browsers for Gmail authentications, read the [Embedded vs System Web UI](#) section in the [Using web browsers \(MSAL.NET\)](#) documentation. All MSAL SDKs use the system web-view by default. [Learn more](#).

Google sign-in on embedded web-views expiring September 30, 2021

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

About two months ago we announced that the exception for Embedded WebViews for Gmail authentication will expire in the second half of 2021.

Recently, Google has specified the date to be **September 30, 2021**.

Rolling out globally beginning September 30, 2021, Azure AD B2B guests signing in with their Gmail accounts will now be prompted to enter a code in a separate browser window to finish signing in on Microsoft Teams mobile and desktop clients. This applies to invited guests and guests who signed up using Self-Service Sign-Up.

Azure AD B2C customers who have set up embedded webview Gmail authentications in their custom/line of business apps or have existing Google integrations, will no longer be able to let their users sign in with Gmail accounts. To mitigate this, make sure to modify your apps to use the system browser for sign-in. For more information, read the Embedded vs System Web UI section in the [Using web browsers \(MSAL.NET\)](#) documentation. All MSAL SDKs use the system web-view by default.

As the device login flow will start rolling out on September 30, 2021, it is likely that it may not be rolled out to your region yet (in which case, your end-users will be met with the error screen shown in the documentation until it gets deployed to your region.)

For details on known impacted scenarios and what experience your users can expect, read [Add Google as an identity provider for B2B guest users](#).

Bug fixes in My Apps

Type: Fixed

Service category: My Apps

Product capability: End User Experiences

- Previously, the presence of the banner recommending the use of collections caused content to scroll behind the header. This issue has been resolved.
- Previously, there was another issue when adding apps to a collection, the order of apps in All Apps collection would get randomly reordered. This issue has also been resolved.

For more information on My Apps, read [Sign in and start apps from the My Apps portal](#).

Public preview - Application authentication method policies

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Application authentication method policies in MS Graph which allow IT admins to enforce lifetime on application password secret credential or block the use of secrets altogether. Policies can be enforced for an entire tenant as a default configuration and it can be scoped to specific applications or service principals. [Learn more](#).

Public preview - Authentication Methods registration campaign to download Microsoft Authenticator

Type: New feature

Service category: Microsoft Authenticator App

Product capability: User Authentication

The Authenticator registration campaign helps admins to move their organizations to a more secure posture by prompting users to adopt the Microsoft Authenticator app. Prior to this feature, there was no way for an admin to push their users to set up the Authenticator app.

The registration campaign comes with the ability for an admin to scope users and groups by including and excluding them from the registration campaign to ensure a smooth adoption across the organization. [Learn more](#)

Public preview - Separation of duties check

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

In Azure AD entitlement management, an administrator can define that an access package is incompatible with another access package or with a group. Users who have the incompatible memberships will be then unable to request more access. [Learn more.](#)

Public preview - Identity Protection logs in Log Analytics, Storage Accounts, and Event Hubs

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

You can now send the risky users and risk detections logs to Azure Monitor, Storage Accounts, or Log Analytics using the Diagnostic Settings in the Azure AD blade. [Learn more.](#)

Public preview - Application Proxy API addition for backend SSL certificate validation

Type: New feature

Service category: App Proxy

Product capability: Access Control

The `onPremisesPublishing` resource type now includes the property, "isBackendCertificateValidationEnabled" which indicates whether backend SSL certificate validation is enabled for the application. For all new Application Proxy apps, the property will be set to true by default. For all existing apps, the property will be set to false. For more information, read the [onPremisesPublishing resource type](#) api.

General availability - Improved Authenticator setup experience for add Azure AD account in Microsoft Authenticator app by directly signing into the app.

Type: New feature

Service category: Microsoft Authenticator App

Product capability: User Authentication

Users can now use their existing authentication methods to directly sign into the Microsoft Authenticator app to set up their credential. Users don't need to scan a QR Code anymore and can use a Temporary Access Pass (TAP) or Password + SMS (or other authentication method) to configure their account in the Authenticator app.

This improves the user credential provisioning process for the Microsoft Authenticator app and gives the end user a self-service method to provision the app. [Learn more.](#)

General availability - Set manager as reviewer in Azure AD entitlement management access packages

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

Access packages in Azure AD entitlement management now support setting the user's manager as the reviewer for regularly occurring access reviews. [Learn more.](#)

General availability - Enable external users to self-service sign-up in Azure AD using MSA accounts

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Users can now enable external users to self-service sign-up in Azure Active Directory using Microsoft accounts. [Learn more.](#)

General availability - External Identities Self-Service Sign-Up with Email One-time Passcode

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Now users can enable external users to self-service sign-up in Azure Active Directory using their email and one-time passcode. [Learn more](#).

General availability - Anomalous token

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Anomalous token detection is now available in Identity Protection. This feature can detect that there are abnormal characteristics in the token such as time active and authentication from unfamiliar IP address. [Learn more](#).

General availability - Register or join devices in Conditional Access

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

The Register or join devices user action in Conditional access is now in general availability. This user action allows you to control multifactor authentication (MFA) policies for Azure AD device registration.

Currently, this user action only allows you to enable multifactor authentication as a control when users register or join devices to Azure AD. Other controls that are dependent on or not applicable to Azure AD device registration continue to be disabled with this user action. [Learn more](#).

New provisioning connectors in the Azure AD Application Gallery - July 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Clebex](#)
- [Exium](#)
- [SoSafe](#)
- [Talentech](#)
- [Thrive LXP](#)
- [Vonage](#)
- [Zip](#)
- [TimeClock 365](#)

For more information about how to better secure your organization by using automated user account provisioning, read [Automate user provisioning to SaaS applications with Azure AD](#).

Changes to security and Microsoft 365 group settings in Azure portal

Type: Changed feature

Service category: Group Management

Product capability: Directory

In the past, users could create security groups and Microsoft 365 groups in the Azure portal. Now users will have the ability to create groups across Azure portals, PowerShell, and API. Customers are required to verify and update the new settings have been configured for their organization. [Learn More](#).

"All Apps" collection has been renamed to "Apps"

Type: Changed feature

Service category: My Apps

Product capability: End User Experiences

In the My Apps portal, the collection that was called "All Apps" has been renamed to be called "Apps". As the product evolves, "Apps" is a more fitting name for this default collection. [Learn more](#).

June 2021

Context panes to display risk details in Identity Protection Reports

Type: Plan for change

Service category: Identity Protection

Product capability: Identity Security & Protection

For the Risky users, Risky sign-ins, and Risk detections reports in Identity Protection, the risk details of a selected entry will be shown in a context pane appearing from the right of the page July 2021. The change only impacts the user interface and won't affect any existing functionalities. To learn more about the functionality of these features, refer to [How To: Investigate risk](#).

Public preview - create Azure AD access reviews of Service Principals that are assigned to privileged roles

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

You can use Azure AD access reviews to review service principal's access to privileged Azure AD and Azure resource roles. [Learn more](#).

Public preview - group owners in Azure AD can create and manage Azure AD access reviews for their groups

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

Now group owners in Azure AD can create and manage Azure AD access reviews on their groups. This ability can be enabled by tenant administrators through Azure AD access review settings and is disabled by default. [Learn more](#).

Public preview - customers can scope access reviews of privileged roles to just users with eligible or active access

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

When admins create access reviews of assignments to privileged roles, they can scope the reviews to only eligible assigned users or only actively assigned users. [Learn more](#).

Public preview - Microsoft Graph APIs for Mobility (MDM/MAM) management policies

Type: New feature

Service category: Other

Product capability: Device Lifecycle Management

Microsoft Graph support for the Mobility (MDM/MAM) configuration in Azure AD is in public preview. Administrators can configure user scope and URLs for MDM applications like Intune using Microsoft Graph v1.0. For more information, see [mobilityManagementPolicy resource type](#)

General availability - Custom questions in access package request flow in Azure Active Directory entitlement management

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

Azure AD entitlement management now supports the creation of custom questions in the access package request flow. This feature allows you to configure custom questions in the access package policy. These questions are shown to requestors who can input their answers as part of the access request process. These answers will be displayed to approvers, giving them helpful information that empowers them to make better decisions on the access request. [Learn more](#).

General availability - Multi-geo SharePoint sites as resources in Entitlement Management Access Packages

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

Access packages in Entitlement Management now support multi-geo SharePoint sites for customers who use the multi-geo capabilities in SharePoint Online. [Learn more](#).

General availability - Knowledge Admin and Knowledge Manager built-in roles

Type: New feature

Service category: RBAC

Product capability: Access Control

Two new roles, Knowledge Administrator and Knowledge Manager are now in general availability.

- Users in the Knowledge Administrator role have full access to all Organizational knowledge settings in the Microsoft 365 admin center. They can create and manage content, like topics and acronyms. Additionally, these users can create content centers, monitor service health, and create service requests. [Learn more](#)
 - Users in the Knowledge Manager role can create and manage content and are primarily responsible for the quality and structure of knowledge. They have full rights to topic management actions to confirm a topic, approve edits, or delete a topic. This role can also manage taxonomies as part of the term store management tool and create content centers. [Learn more](#).
-

General availability - Cloud App Security Administrator built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users with this role have full permissions in Cloud App Security. They can add administrators, add Microsoft Cloud App Security (MCAS) policies and settings, upload logs, and do governance actions. [Learn more](#).

General availability - Windows Update Deployment Administrator

Type: New feature

Service category: RBAC

Product capability: Access Control

Users in this role can create and manage all aspects of Windows Update deployments through the Windows Update for Business deployment service. The deployment service enables users to define settings for when and how updates are deployed. Also, users can specify which updates are offered to groups of devices in their tenant. It also allows users to monitor the update progress. [Learn more](#).

General availability - multi-camera support for Windows Hello

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Now with the Windows 10 21H1 update, Windows Hello supports multiple cameras. The update includes defaults to use the external camera when both built-in and outside cameras are present. [Learn more](#).

General availability - Access Reviews MS Graph APIs now in v1.0

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

Azure Active Directory access reviews MS Graph APIs are now in v1.0 support fully configurable access reviews features. [Learn more](#).

New provisioning connectors in the Azure AD Application Gallery - June 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [askSpoke](#)
- [Cloud Academy - SSO](#)
- [CheckProof](#)
- [GoLinks](#)
- [Holmes Cloud](#)
- [H5mag](#)
- [LimbleCMMS](#)
- [LogMeln](#)
- [SECURE DELIVER](#)
- [Sigma Computing](#)
- [Smallstep SSH](#)
- [Tribeloo](#)
- [Twingate](#)

For more information, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD Application gallery - June 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In June 2021, we have added following 42 new applications in our App gallery with Federation support

Taksel, iDrive360, VIDA, ProProfs Classroom, WAN-Sign, Citrix Cloud SAML SSO, Fabric, DssAD, RICOH Creative Collaboration RICC, Styleflow, Chaos, Traced Connector, Squarespace, MX3 Diagnostics Connector, Ten Spot, Finvari, Mobile4ERP, WalkMe US OpenID Connect, Neustar UltraDNS, cloudtamer.io, A Cloud Guru, PetroVue, Postman, ReadCube Papers, Peklostroj, SynCloud, Polymerhq.io, Bonos, Astra Schedule, Draup, Inc, Applied Mental Health, iHASCO Training, Nexcure, XEOX, Plandisc, foundU, Standard for Success Accreditation, Penji Teams, CheckPoint Infinity Portal, Teamgo, Hopsworks.ai, HoloMeeting 2

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here:
<https://aka.ms/AzureADAppRequest>

Device code flow now includes an app verification prompt

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

The [device code flow](#) has been updated to include one extra user prompt. While signing in, the user will see a prompt asking them to validate the app they're signing into. The prompt ensures that they aren't subject to a phishing attack. [Learn more](#).

User last sign-in date and time is now available on Azure portal

Type: Changed feature

Service category: User Management

Product capability: User Management

You can now view your users' last sign-in date and time stamp on the Azure portal. The information is available for each user on the user profile page. This information helps you identify inactive users and effectively manage risky events. [Learn more](#).

MIM BHold Suite impact of end of support for Microsoft Silverlight

Type: Changed feature

Service category: Microsoft Identity Manager

Product capability: Identity Governance

Microsoft Silverlight will reach its end of support on October 12, 2021. This change only impacts customers using the Microsoft BHold Suite, and doesn't impact other Microsoft Identity Manager scenarios. For more information, see [Silverlight End of Support](#).

Users who haven't installed Microsoft Silverlight in their browser can't use the BHold Suite modules which require Silverlight. This includes the BHold Model Generator, BHold FIM Self-service integration, and BHold Analytics. Customers with an existing BHold deployment of one or more of those modules should plan to uninstall those modules from their BHold server computers by October 2021. Also, they should plan to uninstall Silverlight from any user computers that were previously interacting with that BHold deployment.

My* experiences: End of support for Internet Explorer 11

Type: Deprecated

Service category: My Apps

Product capability: End User Experiences

Microsoft 365 and other apps are ending support for Internet Explorer 11 on August 21, 2021, and this includes the My* experiences. The My*'s accessed via Internet Explorer won't receive bug fixes or any updates, which may lead to issues. These dates are being driven by the Edge team and may be subject to change. [Learn more](#).

Planned deprecation - Malware linked IP address detection in Identity Protection

Type: Deprecated

Service category: Identity Protection

Product capability: Identity Security & Protection

Starting October 1, 2021, Azure AD Identity Protection will no longer generate the "Malware linked IP address" detection. No action is required and customers will remain protected by the other detections provided by Identity Protection. To learn more about protection policies, refer to [Identity Protection policies](#).

May 2021

Public preview - Azure AD verifiable credentials

Type: New feature

Service category: Other

Product capability: User Authentication

Azure AD customers can now easily design and issue verifiable credentials. Verifiable credentials can be used to represent proof of employment, education, or any other claim while respecting privacy. Digitally validate any piece of information about anyone and any business. [Learn more](#).

Public preview - Device code flow now includes an app verification prompt

Type: New feature

Service category: User Authentication

Product capability: Authentications (Logins)

As a security improvement, the [device code flow](#) has been updated to include an another prompt, which validates that the user is signing into the app they expect. The rollout is planned to start in June and expected to be complete by June 30.

To help prevent phishing attacks where an attacker tricks the user into signing into a malicious application, the following prompt is being added: "Are you trying to sign in to [application display name]?". All users will see this prompt while signing in using the device code flow. As a security measure, it cannot be removed or bypassed.

[Learn more](#).

Public preview - build and test expressions for user provisioning

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

The expression builder allows you to create and test expressions, without having to wait for the full sync cycle.

[Learn more](#).

Public preview - enhanced audit logs for Conditional Access policy changes

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

An important aspect of managing Conditional Access is understanding changes to your policies over time. Policy changes may cause disruptions for your end users, so maintaining a log of changes and enabling admins to revert to previous policy versions is critical.

and showing who made a policy change and when, the audit logs will now also contain a modified properties value. This change gives admins greater visibility into what assignments, conditions, or controls changed. If you

want to revert to a previous version of a policy, you can copy the JSON representation of the old version and use the Conditional Access APIs to change the policy to its previous state. [Learn more](#).

Public preview - Sign-in logs include authentication methods used during sign-in

Type: New feature

Service category: MFA

Product capability: Monitoring & Reporting

Admins can now see the sequential steps users took to sign-in, including which authentication methods were used during sign-in.

To access these details, go to the Azure AD sign-in logs, select a sign-in, and then navigate to the Authentication Method Details tab. Here we have included information such as which method was used, details about the method (for example, phone number, phone name), authentication requirement satisfied, and result details.

[Learn more](#).

Public preview - PIM adds support for ABAC conditions in Azure Storage roles

Type: New feature

Service category: Privileged Identity Management

Product capability: Privileged Identity Management

Along with the public preview of attributed based access control for specific Azure RBAC role, you can also add ABAC conditions inside Privileged Identity Management for your eligible assignments. [Learn more](#).

General availability - Conditional Access and Identity Protection Reports in B2C

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

B2C now supports Conditional Access and Identity Protection for business-to-consumer (B2C) apps and users. This enables customers to protect their users with granular risk- and location-based access controls. With these features, customers can now look at the signals and create a policy to provide more security and access to your customers. [Learn more](#).

General availability - KMSI and Password reset now in next generation of user flows

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

The next generation of B2C user flows now supports [keep me signed in \(KMSI\)](#) and password reset. The KMSI functionality allows customers to extend the session lifetime for the users of their web and native applications by using a persistent cookie. This feature keeps the session active even when the user closes and reopens the browser. The session is revoked when the user signs out. Password reset allows users to reset their password from the "Forgot your password" link. This also allows the admin to force reset the user's expired password in the Azure AD B2C directory. [Learn more](#).

General availability - New Log Analytics workbook Application role assignment activity

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

A new workbook has been added for surfacing audit events for application role assignment changes. [Learn more](#).

General availability - Next generation Azure AD B2C user flows

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

The new simplified user flow experience offers feature parity with preview features and is the home for all new features. Users can enable new features within the same user flow, reducing the need to create multiple versions with every new feature release. The new, user-friendly UX also simplifies the selection and creation of user flows. Refer to [Create user flows in Azure AD B2C](#) for guidance on using this feature. [Learn more.](#)

General availability - Azure Active Directory threat intelligence for sign-in risk

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

This new detection serves as an ad-hoc method to allow our security teams to notify you and protect your users by raising their session risk to a High risk when we observe an attack happening. The detection will also mark the associated sign-ins as risky. This detection follows the existing Azure Active Directory threat intelligence for user risk detection to provide complete coverage of the various attacks observed by Microsoft security teams.

[Learn more.](#)

General availability - Conditional Access named locations improvements

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

IPv6 support in named locations is now generally available. Updates include:

- Added the capability to define IPv6 address ranges
- Increased limit of named locations from 90 to 195
- Increased limit of IP ranges per named location from 1200 to 2000
- Added capabilities to search and sort named locations and filter by location type and trust type
- Added named locations a sign-in belonged to in the sign-in logs

Additionally, to prevent admins from defining problematically named locations, extra checks have been added to reduce the chance of misconfiguration. [Learn more.](#)

General availability - Restricted guest access permissions in Azure AD

Type: New feature

Service category: User Management

Product capability: Directory

Directory level permissions for guest users have been updated. These permissions allow administrators to require extra restrictions and controls on external guest user access.

Admins can now add more restrictions for external guests' access to user and groups' profile and membership information. Also, customers can manage external user access at scale by hiding group memberships, including restricting guest users from seeing memberships of the group(s) they are in. To learn more, see [Restrict guest access permissions in Azure Active Directory](#).

New Federated Apps available in Azure AD Application gallery - May 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [AuditBoard](#)
- [Cisco Umbrella User Management](#)
- [Insite LMS](#)
- [kpifire](#)
- [UNIFI](#)

For more information about how to better secure your organization using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD Application gallery - May 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In May 2021, we have added following 29 new applications in our App gallery with Federation support

[InviteDesk](#), [Webrecruit ATS](#), [Workshop](#), [Gravity Sketch](#), [JustLogin](#), [Custellence](#), [WEVO](#), [AppTec360 MDM](#), [Filemail](#), [Ardoq](#), [Leadfamly](#), [Documo](#), [Autodesk SSO](#), [Check Point Harmony Connect](#), [BrightHire](#), [Rescana](#), [Bluewhale](#), [AlacrityLaw](#), [Equisolve](#), [Zip](#), [Cognician](#), [Acra](#), [VaultMe](#), [TAP App Security](#), [Cavelo Office365 Cloud Connector](#), [Clebex](#), [Banyan Command Center](#), [Check Point Remote Access VPN](#), [LogMeln](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here

<https://aka.ms/AzureADAppRequest>

Improved Conditional Access Messaging for Android and iOS

Type: Changed feature

Service category: Device Registration and Management

Product capability: End User Experiences

We've updated the wording on the Conditional Access screen shown to users when they're blocked from accessing corporate resources. They'll be blocked until they enroll their device in Mobile Device Management. These improvements apply to the Android and iOS/iPadOS platforms. The following have been changed:

- "Help us keep your device secure" has changed to "Set up your device to get access"
- "Your sign-in was successful but your admin requires your device to be managed by Microsoft to access this resource." to "[Organization's name] requires you to secure this device before you can access [organization's name] email, files, and data."
- "Enroll Now" to "Continue"

The information in [Enroll your Android enterprise device](#) is out of date.

Azure Information Protection service will begin asking for consent

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

The Azure Information Protection service signs users into the tenant that encrypted the document as part of providing access to the document. Starting June, Azure AD will begin prompting the user for consent when this

access is given across organizations. This ensures that the user understands that the organization that owns the document will collect some information about the user as part of the document access. [Learn more](#).

Provisioning logs schema change impacting Graph API and Azure Monitor integration

Type: Changed feature

Service category: App Provisioning

Product capability: Monitoring & Reporting

The attributes "Action" and "statusInfo" will be changed to "provisioningAction" and "provisoiningStatusInfo." Update any scripts that you have created using the [provisioning logs Graph API](#) or [Azure Monitor integrations](#).

New ARM API to manage PIM for Azure Resources and Azure AD roles

Type: Changed feature

Service category: Privileged Identity Management

Product capability: Privileged Identity Management

An updated version of the PIM API for Azure Resource role and Azure AD role has been released. The PIM API for Azure Resource role is now released under the ARM API standard, which aligns with the role management API for regular Azure role assignment. On the other hand, the PIM API for Azure AD roles is also released under graph API aligned with the unifiedRoleManagement APIs. Some of the benefits of this change include:

- Alignment of the PIM API with objects in ARM and Graph for role managementReducing the need to call PIM to onboard new Azure resources.
- All Azure resources automatically work with new PIM API.
- Reducing the need to call PIM for role definition or keeping a PIM resource ID
- Supporting app-only API permissions in PIM for both Azure AD and Azure Resource roles

A previous version of the PIM API under `/privilegedaccess` will continue to function but we recommend you to move to this new API going forward. [Learn more](#).

Revision of roles in Azure AD entitlement management

Type: Changed feature

Service category: Roles

Product capability: Entitlement Management

A new role, Identity Governance Administrator, has recently been introduced. This role will be the replacement for the User Administrator role in managing catalogs and access packages in Azure AD entitlement management. If you have assigned administrators to the User Administrator role or have them activate this role to manage access packages in Azure AD entitlement management, switch to the Identity Governance Administrator role instead. The User Administrator role will no longer be providing administrative rights to catalogs or access packages. [Learn more](#).

April 2021

Bug fixed - Azure AD will no longer double-encode the state parameter in responses

Type: Fixed

Service category: Authentications (Logins)

Product capability: User Authentication

Azure AD has identified, tested, and released a fix for a bug in the `/authorize` response to a client application. Azure AD was incorrectly URL encoding the `state` parameter twice when sending responses back to the client. This can cause a client application to reject the request, due to a mismatch in state parameters. [Learn more](#).

Users can only create security and Microsoft 365 groups in Azure portal being deprecated

Type: Plan for change

Service category: Group Management

Product capability: Directory

Users will no longer be limited to create security and Microsoft 365 groups only in the Azure portal. The new setting will allow users to create security groups in the Azure portal, PowerShell, and API. Users will be required to verify and update the new setting. [Learn more](#).

Public preview - External Identities Self-Service Sign-up in Azure AD using Email One-Time Passcode accounts

Type: New feature

Service category: B2B

Product capability: B2B/B2C

External users can now use Email One-Time Passcode accounts to sign up or sign in to Azure AD 1st party and line-of-business applications. [Learn more](#).

General availability - External Identities Self-Service Sign Up

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Self-service sign-up for external users is now in general availability. With this new feature, external users can now self-service sign up to an application.

You can create customized experiences for these external users, including collecting information about your users during the registration process and allowing external identity providers like Facebook and Google. You can also integrate with third-party cloud providers for various functionalities like identity verification or approval of users. [Learn more](#).

General availability - Azure AD B2C Phone Sign-up and Sign-in using Built-in Policy

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

B2C Phone Sign-up and Sign-in using a built-in policy enable IT administrators and developers of organizations to allow their end-users to sign in and sign-up using a phone number in user flows. With this feature, disclaimer links such as privacy policy and terms of use can be customized and shown on the page before the end-user proceeds to receive the one-time passcode via text message. [Learn more](#).

New Federated Apps available in Azure AD Application gallery - April 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In April 2021, we have added following 31 new applications in our App gallery with Federation support

Zii Travel Azure AD Connect, Cerby, Selflessly, Apollo CX, Pedagoo, Measureup, Wistec Education, ProcessUnity, Cisco Intersight, Codility, H5mag, Check Point Identity Awareness, Jarvis, desknet's NEO, SDS & Chemical Information Management, Wúru App, Holmes, Tide Multi Tenant, Telenor, Yooz US, Mooncamp, inwise SSO, Ecolab Digital Solutions, Taguchi Digital Marketing System, XpressDox EU Cloud, EZSSH, EZSSH Client, Verto 365, KPN Grip, AddressLook, Cornerstone Single Sign-On

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here:

<https://aka.ms/AzureADAppRequest>

New provisioning connectors in the Azure AD Application Gallery - April 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Bentley - Automatic User Provisioning](#)
- [Boxcryptor](#)
- [BrowserStack Single Sign-on](#)
- [Eletive](#)
- [Jostle](#)
- [Olfeo SAAS](#)
- [Proware](#)
- [Segment](#)

For more information about how to better secure your organization with automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Introducing new versions of page layouts for B2C

Type: Changed feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

The [page layouts](#) for B2C scenarios on the Azure AD B2C has been updated to reduce security risks by introducing the new versions of jQuery and Handlebars JS.

Updates to Sign-in Diagnostic

Type: Changed feature

Service category: Reporting

Product capability: Monitoring & Reporting

The scenario coverage of the Sign-in Diagnostic tool has increased.

With this update, the following event-related scenarios will now be included in the sign-in diagnosis results:

- Enterprise Applications configuration problem events.
- Enterprise Applications service provider (application-side) events.
- Incorrect credentials events.

These results will show contextual and relevant details about the event and actions to take to resolve these problems. Also, for scenarios where we don't have deep contextual diagnostics, Sign-in Diagnostic will present more descriptive content about the error event.

For more information, see [What is sign-in diagnostic in Azure AD?](#)

Azure AD Connect cloud sync general availability refresh

Type: Changed feature

Service category: Azure AD Connect Cloud Sync **Product capability:** Directory

Azure AD connect cloud sync now has an updated agent (version# - 1.1.359). For more details on agent updates, including bug fixes, check out the [version history](#). With the updated agent, cloud sync customers can use GMSA cmdlets to set and reset their gMSA permission at a granular level. In addition that, we have changed the limit of syncing members using group scope filtering from 1499 to 50,000 (50K) members.

Check out the newly available [expression builder](#) for cloud sync, which, helps you build complex expressions as well as simple expressions when you do transformations of attribute values from AD to Azure AD using attribute mapping.

March 2021

Guidance on how to enable support for TLS 1.2 in your environment, in preparation for upcoming Azure AD TLS 1.0/1.1 deprecation

Type: Plan for change

Service category: N/A

Product capability: Standards

Azure Active Directory will deprecate the following protocols in Azure Active Directory worldwide regions starting June 30, 2021:

- TLS 1.0
- TLS 1.1
- 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

Affected environments include:

- Azure Commercial Cloud
- Office 365 GCC and WW

For more information, see [Enable support for TLS 1.2 in your environment for Azure AD TLS 1.1 and 1.0 deprecation](#).

Public preview - Azure AD Entitlement management now supports multi-geo SharePoint Online

Type: New feature

Service category: Other

Product capability: Entitlement Management

For organizations using multi-geo SharePoint Online, you can now include sites from specific multi-geo environments to your Entitlement management access packages. [Learn more](#).

Public preview - Restore deleted apps from App registrations

Type: New feature

Service category: Other

Product capability: Developer Experience

Customers can now view, restore, and permanently remove deleted app registrations from the Azure portal. This applies only to applications associated to a directory, not applications from a personal Microsoft account. [Learn more](#).

Public preview - New "User action" in Conditional Access for registering or joining devices

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

A new user action called "Register or join devices" in Conditional access is available. This user action allows you to control Azure Active Directory Multi-Factor Authentication (MFA) policies for Azure AD device registration.

Currently, this user action only allows you to enable Azure AD MFA as a control when users register or join devices to Azure AD. Other controls that are dependent on or not applicable to Azure AD device registration are disabled with this user action. [Learn more](#).

Public preview - Optimize connector groups to use the closest Application Proxy cloud service

Type: New feature

Service category: App Proxy

Product capability: Access Control

With this new capability, connector groups can be assigned to the closest regional Application Proxy service an application is hosted in. This can improve app performance in scenarios where apps are hosted in regions other than the home tenant's region. [Learn more](#).

Public preview - External Identities Self-Service Sign-up in Azure AD using Email One-Time Passcode accounts

Type: New feature

Service category: B2B

Product capability: B2B/B2C

External users will now be able to use Email One-Time Passcode accounts to sign up in to Azure AD 1st party and LOB apps. [Learn more](#).

Public preview - Availability of AD FS Sign-Ins in Azure AD

Type: New feature

Service category: Authentications (Logins)

Product capability: Monitoring & Reporting

AD FS sign-in activity can now be integrated with Azure AD activity reporting, providing a unified view of hybrid identity infrastructure. Using the Azure AD Sign-Ins report, Log Analytics, and Azure Monitor Workbooks, it's possible to do in-depth analysis for both Azure AD and AD FS sign-in scenarios such as AD FS account lockouts, bad password attempts, and spikes of unexpected sign-in attempts.

To learn more, visit [AD FS sign-ins in Azure AD with Connect Health](#).

General availability - Staged rollout to cloud authentication

Type: New feature

Service category: AD Connect

Product capability: User Authentication

Staged rollout to cloud authentication is now generally available. The staged rollout feature allows you to selectively test groups of users with cloud authentication methods, such as Passthrough Authentication (PTA) or Password Hash Sync (PHS). Meanwhile, all other users in the federated domains continue to use federation services, such as AD FS or any other federation services to authenticate users. [Learn more](#).

General availability - User Type attribute can now be updated in the Azure admin portal

Type: New feature

Service category: User Experience and Management

Product capability: User Management

Customers can now update the user type of Azure AD users when they update their user profile information

from the Azure admin portal. The user type can be updated from Microsoft Graph also. To learn more, see [Add or update user profile information](#).

General availability - Replica Sets for Azure Active Directory Domain Services

Type: New feature

Service category: Azure AD Domain Services

Product capability: Azure AD Domain Services

The capability of replica sets in Azure AD DS is now generally available. [Learn more](#).

General availability - Collaborate with your partners using Email One-Time Passcode in the Azure Government cloud

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Organizations in the Microsoft Azure Government cloud can now enable their guests to redeem invitations with Email One-Time Passcode. This ensures that any guest users with no Azure AD, Microsoft, or Gmail accounts in the Azure Government cloud can still collaborate with their partners by requesting and entering a temporary code to sign in to shared resources. [Learn more](#).

New Federated Apps available in Azure AD Application gallery - March 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In March 2021 we have added following 37 new applications in our App gallery with Federation support:

Bambuser Live Video Shopping, DeepDye Inc, Moqups, RICOH Spaces Mobile, Flipgrid, hCaptcha Enterprise, SchoolStream ASA, TransPerfect GlobalLink Dashboard, SimplificaCI, Thrive LXP, Lexonis TalentScape, Exium, Sapient, TrueChoice, RICOH Spaces, Saba Cloud, Acunetix 360, Exceed.ai, GitHub Enterprise Managed User, Enterprise Vault.cloud for Outlook, Smartlook, Accenture Academy, Onshape, Tradeshift, JuriBlox, SecurityStudio, ClicData, Evergreen, Patchdeck, FAX.PLUS, ValidSign, AWS Single Sign-on, Nura Space, Broadcom DX SaaS, Interplay Learning, SendPro Enterprise, FortiSASE SIA

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here:

<https://aka.ms/AzureADAppRequest>

New provisioning connectors in the Azure AD Application Gallery - March 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [AWS Single Sign-on](#)
- [Bpanda](#)
- [Britive](#)
- [GitHub Enterprise Managed User](#)
- [Grammarly](#)
- [LogicGate](#)

- [SecureLogin](#)
- [TravelPerk](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Introducing MS Graph API for Company Branding

Type: Changed feature

Service category: MS Graph

Product capability: B2B/B2C

[MS Graph API for the Company Branding](#) is available for the Azure AD or Microsoft 365 login experience to allow the management of the branding parameters programmatically.

General availability - Header-based authentication SSO with Application Proxy

Type: Changed feature

Service category: App Proxy

Product capability: Access Control

Azure AD Application Proxy native support for header-based authentication is now in general availability. With this feature, you can configure the user attributes required as HTTP headers for the application without additional components needed to deploy. [Learn more](#).

Two-way SMS for MFA Server is no longer supported

Type: Deprecated

Service category: MFA

Product capability: Identity Security & Protection

Two-way SMS for MFA Server was originally deprecated in 2018, and will not be supported after February 24, 2021. Administrators should enable another method for users who still use two-way SMS.

Email notifications and Azure portal Service Health notifications were sent to affected admins on December 8, 2020 and January 28, 2021. The alerts went to the Owner, Co-Owner, Admin, and Service Admin RBAC roles tied to the subscriptions. [Learn more](#).

February 2021

Email one-time passcode authentication on by default starting October 2021

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

Starting October 31, 2021, Microsoft Azure Active Directory [email one-time passcode authentication](#) will become the default method for inviting accounts and tenants for B2B collaboration scenarios. At this time, Microsoft will no longer allow the redemption of invitations using unmanaged Azure Active Directory accounts.

Unrequested but consented permissions will no longer be added to tokens if they would trigger Conditional Access

Type: Plan for change

Service category: Authentications (Logins)

Product capability: Platform

Currently, applications using [dynamic permissions](#) are given all of the permissions they're consented to access.

This includes applications that are unrequested and even if they trigger conditional access. For example, this can cause an app requesting only `user.read` that also has consent for `files.read`, to be forced to pass the Conditional Access assigned for the `files.read` permission.

To reduce the number of unnecessary Conditional Access prompts, Azure AD is changing the way that unrequested scopes are provided to applications. Apps will only trigger conditional access for permission they explicitly request. For more information, read [What's new in authentication](#).

Public preview - Use a Temporary Access Pass to register Passwordless credentials

Type: New feature

Service category: MFA

Product capability: Identity Security & Protection

Temporary Access Pass is a time-limited passcode that serves as strong credentials and allows onboarding of Passwordless credentials and recovery when a user has lost or forgotten their strong authentication factor (for example, FIDO2 security key or Microsoft Authenticator) app and needs to sign in to register new strong authentication methods. [Learn more](#).

Public preview - Keep me signed in (KMSI) in next generation of user flows

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

The next generation of B2C user flows now supports the [keep me signed in \(KMSI\)](#) functionality that allows customers to extend the session lifetime for the users of their web and native applications by using a persistent cookie. feature keeps the session active even when the user closes and reopens the browser, and is revoked when the user signs out.

Public preview - Reset redemption status for a guest user

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Customers can now reinvite existing external guest users to reset their redemption status, which allows the guest user account to remain without them losing any access. [Learn more](#).

Public preview - /synchronization (provisioning) APIs now support application permissions

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

Customers can now use `application.readwrite.ownedby` as an application permission to call the synchronization APIs. Note this is only supported for provisioning from Azure AD out into third-party applications (for example, AWS, Data Bricks, etc.). It is currently not supported for HR-provisioning (Workday / Successfactors) or Cloud Sync (AD to Azure AD). [Learn more](#).

General availability - Authentication Policy Administrator built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users with this role can configure the authentication methods policy, tenant-wide MFA settings, and password protection policy. This role grants permission to manage Password Protection settings: smart lockout

configurations and updating the custom banned passwords list. [Learn more](#).

General availability - User collections on My Apps are available now!

Type: New feature

Service category: My Apps

Product capability: End User Experiences

Users can now create their own groupings of apps on the My Apps app launcher. They can also reorder and hide collections shared with them by their administrator. [Learn more](#).

General availability - Autofill in Authenticator

Type: New feature

Service category: Microsoft Authenticator App

Product capability: Identity Security & Protection

Microsoft Authenticator provides multifactor authentication and account management capabilities, and now also will autofill passwords on sites and apps users visit on their mobile (iOS and Android).

To use autofill on Authenticator, users need to add their personal Microsoft account to Authenticator and use it to sync their passwords. Work or school accounts cannot be used to sync passwords at this time. [Learn more](#).

General availability - Invite internal users to B2B collaboration

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Customers can now invite internal guests to use B2B collaboration instead of sending an invitation to an existing internal account. This allows customers to keep that user's object ID, UPN, group memberships, and app assignments. [Learn more](#).

General availability - Domain Name Administrator built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users with this role can manage (read, add, verify, update, and delete) domain names. They can also read directory information about users, groups, and applications, as these objects have domain dependencies.

For on-premises environments, users with this role can configure domain names for federation so that associated users are always authenticated on-premises. These users can then sign into Azure AD-based services with their on-premises passwords via single sign-on. Federation settings need to be synced via Azure AD Connect, so users also have permissions to manage Azure AD Connect. [Learn more](#).

New Federated Apps available in Azure AD Application gallery - February 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In February 2021 we have added following 37 new applications in our App gallery with Federation support:

[Loop Messenger Extension](#), [Silverfort Azure AD Adapter](#), [Interplay Learning](#), [Nura Space](#), [Yooz EU](#), [UXPressia](#), [introDus Pre- and Onboarding Platform](#), [Happybot](#), [LeaksID](#), [ShiftWizard](#), [PingFlow SSO](#), [Swiftlane](#), [Quasydoc SSO](#), [Fenwick Gold Account](#), [SeamlessDesk](#), [Learnsoft LMS & TMS](#), [P-TH+](#), [myViewBoard](#), [Tartabit IoT Bridge](#), [AKASHI](#), [Rewatch](#), [Zuddl](#), [Parkalot - Car park management](#), [HSB ThoughtSpot](#), [IBMid](#), [SharingCloud](#), [PoolParty](#)

Semantic Suite, GlobeSmart, Samsung Knox and Business Services, Penji, Kendis- Scaling Agile Platform, Maptician, Olfeo SAAS, Sigma Computing, CloudKnox Permissions Management Platform, Klaxoon SAML, Enablon

You can also find the documentation of all the applications here: <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here:

<https://aka.ms/AzureADAppRequest>

New provisioning connectors in the Azure AD Application Gallery - February 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Atea](#)
- [Getabstract](#)
- [HelloID](#)
- [Hoxhunt](#)
- [Iris Intranet](#)
- [Preciate](#)

For more information, read [Automate user provisioning to SaaS applications with Azure AD](#).

General availability - 10 Azure Active Directory roles now renamed

Type: Changed feature

Service category: RBAC

Product capability: Access Control

10 Azure AD built-in roles have been renamed so that they're aligned across the [Microsoft 365 admin center](#), [Azure AD portal](#), and [Microsoft Graph](#). To learn more about the new roles, refer to [Administrator role permissions in Azure Active Directory](#).

Role names in MS Graph API	Role name in Azure portal	Proposed final name across API, Azure Portal and MAC
Company Administrator	Global administrator	Global Administrator
CRM Service Administrator	Dynamics 365 administrator	Dynamics 365 Administrator
Device Administrator	<i>Not shown</i>	Azure AD Joined Device Local Administrator
Exchange Service Administrator	Exchange administrator	Exchange Administrator
Intune Service Administrator	Intune administrator	Intune Administrator
Lync Service Administrator	Skype for Business administrator	Skype for Business Administrator
Power BI Service Administrator	Power BI administrator	Power BI Administrator
SharePoint Service Administrator	SharePoint administrator	SharePoint Administrator
User Account Administrator	User administrator	User Administrator
Teams Service Administrator	Teams Service Administrator	Teams Administrator

New Company Branding in multifactor authentication (MFA)/SSPR Combined Registration

Type: Changed feature

Service category: User Experience and Management

Product capability: End User Experiences

In the past, company logos weren't used on Azure Active Directory sign-in pages. Company branding is now located to the top left of multifactor authentication (MFA)/SSPR Combined Registration. Company branding is also included on My Sign-Ins and the Security Info page. [Learn more](#).

General availability - Second level manager can be set as alternate approver

Type: Changed feature

Service category: User Access Management

Product capability: Entitlement Management

An extra option when you select approvers is now available in Entitlement Management. If you select "Manager as approver" for the First Approver, you will have another option, "Second level manager as alternate approver", available to choose in the alternate approver field. If you select this option, you need to add a fallback approver to forward the request to in case the system can't find the second level manager. [Learn more](#).

Authentication Methods Activity Dashboard

Type: Changed feature

Service category: Reporting

Product capability: Monitoring & Reporting

The refreshed Authentication Methods Activity dashboard gives admins an overview of authentication method registration and usage activity in their tenant. The report summarizes the number of users registered for each method, and also which methods are used during sign-in and password reset. [Learn more](#).

Refresh and session token lifetimes configurability in Configurable Token Lifetime (CTL) are retired

Type: Deprecated

Service category: Other

Product capability: User Authentication

Refresh and session token lifetimes configurability in CTL are retired. Azure Active Directory no longer honors refresh and session token configuration in existing policies. [Learn more](#).

January 2021

Secret token will be a mandatory field when configuring provisioning

Type: Plan for change

Service category: App Provisioning

Product capability: Identity Lifecycle Management

In the past, the secret token field could be kept empty when setting up provisioning on the custom / BYOA application. This function was intended to solely be used for testing. We'll update the UI to make the field required.

Customers can work around this requirement for testing purposes by using a feature flag in the browser URL. [Learn more](#).

Public Preview - Customize and configure Android shared devices for frontline workers at scale

Type: New feature

Service category: Device Registration and Management

Product capability: Identity Security & Protection

Azure AD and Microsoft Endpoint Manager teams have combined to bring the capability to customize, scale, and secure your frontline worker devices.

The following preview capabilities will allow you to:

- Provision Android shared devices at scale with Microsoft Endpoint Manager
- Secure your access for shift workers using device-based conditional access
- Customize sign-in experiences for the shift workers with Managed Home Screen

To learn more, refer to [Customize and configure shared devices for frontline workers at scale](#).

Public preview - Provisioning logs can now be downloaded as a CSV or JSON

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

Customers can download the provisioning logs as a CSV or JSON file through the UI and via graph API. To learn more, refer to [Provisioning reports in the Azure Active Directory portal](#).

Public preview - Assign cloud groups to Azure AD custom roles and admin unit scoped roles

Type: New feature

Service category: RBAC

Product capability: Access Control

Customers can assign a cloud group to Azure AD custom roles or an admin unit scoped role. To learn how to use this feature, refer to [Use cloud groups to manage role assignments in Azure Active Directory](#).

General Availability - Azure AD Connect cloud sync (previously known as cloud provisioning)

Type: New feature

Service category: Azure AD Connect cloud sync

Product capability: Identity Lifecycle Management

Azure AD Connect cloud sync is now generally available to all customers.

Azure AD Connect cloud moves the heavy lifting of transform logic to the cloud, reducing your on-premises footprint. Additionally, multiple light-weight agent deployments are available for higher sync availability. [Learn more.](#)

General Availability - Attack Simulation Administrator and Attack Payload Author built-in roles

Type: New feature

Service category: RBAC

Product capability: Access Control

Two new roles in Role-Based Access Control are available to assign to users, Attack simulation Administrator and Attack Payload author.

Users in the [Attack Simulation Administrator](#) role have access for all simulations in the tenant and can:

- create and manage all aspects of attack simulation creation
- launch/scheduling of a simulation
- review simulation results.

Users in the [Attack Payload Author](#) role can create attack payloads but not actually launch or schedule them. Attack payloads are then available to all administrators in the tenant who can use them to create a simulation.

General Availability - Usage Summary Reports Reader built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users with the Usage Summary Reports Reader role can access tenant level aggregated data and associated insights in Microsoft 365 Admin Center for Usage and Productivity Score. However, they can't access any user level details or insights.

In the Microsoft 365 Admin Center for the two reports, we differentiate between tenant level aggregated data and user level details. This role adds an extra layer of protection to individual user identifiable data. [Learn more.](#)

General availability - Require App protection policy grant in Azure AD Conditional Access

Type: New Feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Azure AD Conditional Access grant for "Require App Protection policy" is now GA.

The policy provides the following capabilities:

- Allows access only when using a mobile application that supports Intune App protection
- Allows access only when a user has an Intune app protection policy delivered to the mobile application

Learn more on how to set up a conditional access policy for app protection [here](#).

General availability - Email One-Time Passcode

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Email OTP enables organizations around the world to collaborate with anyone by sending a link or invitation via email. Invited users can verify their identity with the one-time passcode sent to their email to access their partner's resources. [Learn more](#).

New provisioning connectors in the Azure AD Application Gallery - January 2021

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Forte Change Cloud](#)
- [Gtmhub](#)
- [monday.com](#)
- [Splashtop](#)
- [Templafy OpenID Connect](#)
- [WEDO](#)

For more information, see [What is automated SaaS app user provisioning in Azure AD?](#)

New Federated Apps available in Azure AD Application gallery - January 2021

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In January 2021 we have added following 29 new applications in our App gallery with Federation support:

[mySCView](#), [Talentech](#), [Bipsync](#), [OroTimesheet](#), [Mio](#), [Sovelto Easy](#), [Supportbench](#), [Bienvenue Formation](#), [AIDA Healthcare SSO](#), [International SOS Assistance Products](#), [NAVEX One](#), [LabLog](#), [Oktopost SAML](#), [EPHOTO DAM](#), [Notion](#), [Syndio](#), [Yello Enterprise](#), [Timeclock 365 SAML](#), [Nalco E-data](#), [Vacancy Filler](#), [Synerise AI Growth Ecosystem](#), [Imperva Data Security](#), [Illusive Networks](#), [Proware](#), [Splan Visitor](#), [Aruba User Experience Insight](#), [Contentsquare SSO](#), [Perimeter 81](#), [Burp Suite Enterprise Edition](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here

<https://aka.ms/AzureADAppRequest>

Public preview - Second level manager can be set as alternate approver

Type: Changed feature

Service category: User Access Management

Product capability: Entitlement Management

An extra option when you select approvers is now available in Entitlement Management. If you select "Manager as approver" for the First Approver, you will have another option, "Second level manager as alternate approver", available to choose in the alternate approver field. If you select this option, you need to add a fallback approver to forward the request to in case the system can't find the second level manager. [Learn more](#)

General availability - Navigate to Teams directly from My Access portal

Type: Changed feature

Service category: User Access Management

Product capability: Entitlement Management

You can now launch Teams directly from the My Access portal.

To do so, sign-in to My Access (<https://myaccess.microsoft.com/>), navigate to "Access packages", then go to the "Active" tab to see all of the access packages you already have access to. When you expand the selected access package and hover on Teams, you can launch it by clicking on the "Open" button. [Learn more](#).

Improved Logging & End-User Prompts for Risky Guest Users

Type: Changed feature

Service category: Identity Protection

Product capability: Identity Security & Protection

The Logging and End-User Prompts for Risky Guest Users have been updated. Learn more in [Identity Protection and B2B users](#).

December 2020

Public preview - Azure AD B2C Phone Sign-up and Sign-in using Built-in Policy

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

B2C Phone Sign-up and Sign-in using Built-in Policy enable IT administrators and developers of organizations to allow their end-users to sign in and sign up using a phone number in user flows. Read [Set up phone sign-up and sign-in for user flows \(preview\)](#) to learn more.

General Availability - Security Defaults now enabled for all new tenants by default

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

To protect user accounts, all new tenants created on or after November 12, 2020, will come with Security Defaults enabled. Security Defaults enforces multiple policies including:

- Requires all users and admins to register for multifactor authentication (MFA) using the Microsoft Authenticator App
- Requires critical admin roles to use multifactor authentication (MFA) every single time they sign-in. All other users will be prompted for multifactor authentication (MFA) whenever necessary.
- Legacy authentication will be blocked tenant wide.

For more information, read [What are security defaults?](#)

General availability - Support for groups with up to 250K members in AADConnect

Type: Changed feature

Service category: AD Connect

Product capability: Identity Lifecycle Management

Microsoft has deployed a new endpoint (API) for Azure AD Connect that improves the performance of the synchronization service operations to Azure Active Directory. When you use the new [V2 endpoint](#), you'll experience noticeable performance gains on export and import to Azure AD. This new endpoint supports the following scenarios:

- Syncing groups with up to 250k members

- Performance gains on export and import to Azure AD
-

General availability - Entitlement Management available for tenants in Azure China cloud

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

The capabilities of Entitlement Management are now available for all tenants in the Azure China cloud. For information, visit our [Identity governance documentation](#) site.

New provisioning connectors in the Azure AD Application Gallery - December 2020

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Bizagi Studio for Digital Process Automation](#)
- [CybSafe](#)
- [GroupTalk](#)
- [PaperCut Cloud Print Management](#)
- [Parable](#)
- [Shopify Plus](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD Application gallery - December 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In December 2020 we have added following 18 new applications in our App gallery with Federation support:

[AwareGo](#), [HowNow SSO](#), [ZyLAB ONE Legal Hold](#), [Guider](#), [Softcrisis](#), [Pims 365](#), [InformaCast](#), [RetrieverMediaDatabase](#), [vonage](#), [Count Me In - Operations Dashboard](#), [ProProfs Knowledge Base](#), [RightCrowd Workforce Management](#), [JLL TRIRIGA](#), [Shutterstock](#), [FortiWeb Web Application Firewall](#), [LinkedIn Talent Solutions](#), [Equinix Federation App](#), [KFAdvance](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here

<https://aka.ms/AzureADAppRequest>

Navigate to Teams directly from My Access portal

Type: Changed feature

Service category: User Access Management **Product capability:** Entitlement Management

You can now launch Teams directly from My Access portal. To do so, sign-in to [My Access](#), navigate to **Access packages**, then go to the **Active Tab** to see all access packages you already have access to. When you expand the access package and hover on Teams, you can launch it by clicking on the **Open** button.

To learn more about using the My Access portal, go to [Request access to an access package in Azure AD entitlement management](#).

Public preview - Second level manager can be set as alternate approver

Type: Changed feature

Service category: User Access Management

Product capability: Entitlement Management

An extra option is now available in the approval process in Entitlement Management. If you select Manager as approver for the First Approver, you'll have another option, Second level manager as alternate approver, available to choose in the alternate approver field. When you select this option, you need to add a fallback approver to forward the request to in case the system can't find the second level manager.

For more information, go to [Change approval settings for an access package in Azure AD entitlement management](#).

November 2020

Azure Active Directory TLS 1.0, TLS 1.1, and 3DES deprecation

Type: Plan for change

Service category: All Azure AD applications

Product capability: Standards

Azure Active Directory will deprecate the following protocols in Azure Active Directory worldwide regions starting June 30, 2021:

- TLS 1.0
- TLS 1.1
- 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

Affected environments are:

- Azure Commercial Cloud
- Office 365 GCC and WW

For guidance to remove deprecating protocols dependencies, please refer to [Enable support for TLS 1.2 in your environment, in preparation for upcoming Azure AD TLS 1.0/1.1 deprecation](#).

New Federated Apps available in Azure AD Application gallery - November 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In November 2020 we have added following 52 new applications in our App gallery with Federation support:

[Travel & Expense Management](#), [Tribeloo](#), [Itslearning](#) File Picker, [Crises Control](#), [CourtAlert](#), [StealthMail](#), [Edmentum - Study Island](#), [Virtual Risk Manager](#), [TIMU](#), [Looker Analytics Platform](#), [Talview - Recruit](#), [Real Time Translator](#), [Klaxoon](#), [Podbean](#), [zcal](#), [expensemanger](#), [Netsparker Enterprise](#), [En-trak Tenant Experience Platform](#), [Appian](#), [Panorays](#), [Builterra](#), [EVA Check-in](#), [HowNow WebApp SSO](#), [Coupa Risk Assess](#), [Lucid \(All Products\)](#), [GoBright](#), [SailPoint IdentityNow](#), [Resource Central](#), [UiPathStudioO365App](#), [Jedox](#), [Cequence Application Security](#), [PerimeterX](#), [TrendMiner](#), [Lexion](#), [WorkWare](#), [ProdPad](#), [AWS ClientVPN](#), [AppSec Flow SSO](#), [Luum](#), [Freight Measure](#), [Terraform Cloud](#), [Nature Research](#), [Play Digital Signage](#), [RemotePC](#), [Prolorus](#), [Hirebridge ATS](#), [Teamgage](#), [Roadmunk](#), [Sunrise Software Relations CRM](#), [Procaire](#), [Mentor® by eDriving: Business](#), [Gradle Enterprise](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here

Public preview - Custom roles for enterprise apps

Type: New feature

Service category: RBAC

Product capability: Access Control

[Custom RBAC roles for delegated enterprise application management](#) is now in public preview. These new permissions build on the custom roles for app registration management, which allows fine-grained control over what access your admins have. Over time, additional permissions to delegate management of Azure AD will be released.

Some common delegation scenarios:

- assignment of user and groups that can access SAML based single sign-on applications
- the creation of Azure AD Gallery applications
- update and read of basic SAML Configurations for SAML based single sign-on applications
- management of signing certificates for SAML based single sign-on applications
- update of expiring sign in certificates notification email addresses for SAML based single sign-on applications
- update of the SAML token signature and sign-in algorithm for SAML based single sign-on applications
- create, delete, and update of user attributes and claims for SAML-based single sign-on applications
- ability to turn on, off, and restart provisioning jobs
- updates to attribute mapping
- ability to read provisioning settings associated with the object
- ability to read provisioning settings associated with your service principal
- ability to authorize application access for provisioning

Public preview - Azure AD Application Proxy natively supports single sign-on access to applications that use headers for authentication

Type: New feature

Service category: App Proxy

Product capability: Access Control

Azure Active Directory (Azure AD) Application Proxy natively supports single sign-on access to applications that use headers for authentication. You can configure header values required by your application in Azure AD. The header values will be sent down to the application via Application Proxy. To learn more, see [Header-based single sign-on for on-premises apps with Azure AD App Proxy](#)

General Availability - Azure AD B2C Phone Sign-up and Sign-in using Custom Policy

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

With phone number sign-up and sign-in, developers and enterprises can allow their customers to sign up and sign in using a one-time password sent to the user's phone number via SMS. This feature also lets the customer change their phone number if they lose access to their phone. With the power of custom policies, allow developers and enterprises to communicate their brand through page customization. Find out how to [set up phone sign-up and sign-in with custom policies in Azure AD B2C](#).

New provisioning connectors in the Azure AD Application Gallery - November 2020

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Adobe Identity Management](#)
- [Blogin](#)
- [Clarizen One](#)
- [Contentful](#)
- [GitHub AE](#)
- [Playvox](#)
- [PrinterLogic SaaS](#)
- [Tic - Tac Mobile](#)
- [Visibly](#)

For more information, see [Automate user provisioning to SaaS applications with Azure AD](#).

Public Preview - Email Sign-In with ProxyAddresses now deployable via Staged Rollout

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Tenant administrators can now use Staged Rollout to deploy Email Sign-In with ProxyAddresses to specific Azure AD groups. This can help while trying out the feature before deploying it to the entire tenant via the Home Realm Discovery policy. Instructions for deploying Email Sign-In with ProxyAddresses via Staged Rollout are in the [documentation](#).

Limited Preview - Sign-in Diagnostic

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

With the initial preview release of the Sign-in Diagnostic, admins can now review user sign-ins. Admins can receive contextual, specific, and relevant details and guidance on what happened during a sign-in and how to fix problems. The diagnostic is available in both the Azure AD level, and Conditional Access Diagnose and Solve blades. The diagnostic scenarios covered in this release are Conditional Access, Azure Active Directory Multi-Factor Authentication, and successful sign-in.

For more information, see [What is sign-in diagnostic in Azure AD?](#).

Improved Unfamiliar Sign-in Properties

Type: Changed feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Unfamiliar sign-in properties detections has been updated. Customers may notice more high-risk unfamiliar sign-in properties detections. For more information, see [What is risk?](#)

Public Preview refresh of Cloud Provisioning agent now available (Version: 1.1.281.0)

Type: Changed feature

Service category: Azure AD Cloud Provisioning

Product capability: Identity Lifecycle Management

Cloud provisioning agent has been released in public preview and is now available through the portal. This release contains several improvements including, support for GMSA for your domains, which provides better security, improved initial sync cycles, and support for large groups. Check out the release version [history](#) for more details.

BitLocker recovery key API endpoint now under /informationProtection

Type: Changed feature

Service category: Device Access Management

Product capability: Device Lifecycle Management

Previously, you could recover BitLocker keys via the /bitlocker endpoint. We'll eventually be deprecating this endpoint, and customers should begin consuming the API that now falls under /informationProtection.

See [BitLocker recovery API](#) for updates to the documentation to reflect these changes.

General Availability of Application Proxy support for Remote Desktop Services HTML5 Web Client

Type: Changed feature

Service category: App Proxy

Product capability: Access Control

Azure AD Application Proxy support for Remote Desktop Services (RDS) Web Client is now in General Availability. The RDS web client allows users to access Remote Desktop infrastructure through any HTML5-capable browser such as Microsoft Edge, Internet Explorer 11, Google Chrome, and so on. Users can interact with remote apps or desktops like they would with a local device from anywhere.

By using Azure AD Application Proxy, you can increase the security of your RDS deployment by enforcing pre-authentication and Conditional Access policies for all types of rich client apps. To learn more, see [Publish Remote Desktop with Azure AD Application Proxy](#)

New enhanced Dynamic Group service is in Public Preview

Type: Changed feature

Service category: Group Management

Product capability: Collaboration

Enhanced dynamic group service is now in Public Preview. New customers that create dynamic groups in their tenants will be using the new service. The time required to create a dynamic group will be proportional to the size of the group that is being created instead of the size of the tenant. This update will improve performance for large tenants significantly when customers create smaller groups.

The new service also aims to complete member addition and removal because of attribute changes within a few minutes. Also, single processing failures won't block tenant processing. To learn more about creating dynamic groups, see our [documentation](#).

October 2020

Azure AD On-Premises Hybrid Agents Impacted by Azure TLS Certificate Changes

Type: Plan for change

Service category: N/A

Product capability: Platform

Microsoft is updating Azure services to use TLS certificates from a different set of Root Certificate Authorities (CAs). This update is due to the current CA certificates not complying with one of the CA/Browser Forum Baseline requirements. This change will impact Azure AD hybrid agents installed on-premises that have

hardened environments with a fixed list of root certificates and will need to be updated to trust the new certificate issuers.

This change will result in disruption of service if you don't take action immediately. These agents include [Application Proxy connectors](#) for remote access to on-premises, [Passthrough Authentication](#) agents that allow your users to sign in to applications using the same passwords, and [Cloud Provisioning Preview](#) agents that perform AD to Azure AD sync.

If you have an environment with firewall rules set to allow outbound calls to only specific Certificate Revocation List (CRL) download, you will need to allow the following CRL and OCSP URLs. For full details on the change and the CRL and OCSP URLs to enable access to, see [Azure TLS certificate changes](#).

Provisioning events will be removed from audit logs and published solely to provisioning logs

Type: Plan for change

Service category: Reporting

Product capability: Monitoring & Reporting

Activity by the SCIM [provisioning service](#) is logged in both the audit logs and provisioning logs. This includes activity such as the creation of a user in ServiceNow, group in GSuite, or import of a role from AWS. In the future, these events will only be published in the provisioning logs. This change is being implemented to avoid duplicate events across logs, and additional costs incurred by customers consuming the logs in log analytics.

We'll provide an update when a date is completed. This deprecation isn't planned for the calendar year 2020.

NOTE

This does not impact any events in the audit logs outside of the synchronization events emitted by the provisioning service. Events such as the creation of an application, conditional access policy, a user in the directory, etc. will continue to be emitted in the audit logs. [Learn more](#).

Azure AD On-Premises Hybrid Agents Impacted by Azure Transport Layer Security (TLS) Certificate Changes

Type: Plan for change

Service category: N/A

Product capability: Platform

Microsoft is updating Azure services to use TLS certificates from a different set of Root Certificate Authorities (CAs). There will be an update because of the current CA certificates not following one of the CA/Browser Forum Baseline requirements. This change will impact Azure AD hybrid agents installed on-premises that have hardened environments with a fixed list of root certificates. These agents will need to be updated to trust the new certificate issuers.

This change will result in disruption of service if you don't take action immediately. These agents include:

- [Application Proxy connectors](#) for remote access to on-premises
- [Passthrough Authentication](#) agents that allow your users to sign in to applications using the same passwords
- [Cloud Provisioning Preview](#) agents that do AD to Azure AD sync.

If you have an environment with firewall rules set to allow outbound calls to only specific Certificate Revocation List (CRL) download, you'll need to allow CRL and OCSP URLs. For full details on the change and the CRL and OCSP URLs to enable access to, see [Azure TLS certificate changes](#).

[1305958](#)

Azure Active Directory TLS 1.0 & 1.1, and 3DES Cipher Suite Deprecation

Type: Plan for change

Service category: N/A

Product capability: Standards

Azure Active Directory will deprecate the following protocols in Azure Active Directory worldwide regions starting on January 31, 2022 (This date has been postponed from 30th June 2021 to 31st Jan 2022, to give Administrators more time to remove the dependency on legacy TLS protocols and ciphers (TLS 1.0,1.1 and 3DES)):

- TLS 1.0
- TLS 1.1
- 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

Affected environments are:

- Azure Commercial Cloud
- Office 365 GCC and WW

Users, services, and applications that interact with Azure Active Directory and Microsoft Graph, should use TLS 1.2 and modern cipher suites to maintain a secure connection to Azure Active Directory for Azure, Office 365, and Microsoft 365 services. For additional guidance, refer to [Enable support for TLS 1.2 in your environment, in preparation for upcoming deprecation of Azure AD TLS 1.0/1.1.](#)

Azure Active Directory TLS 1.0, TLS 1.1, and 3DES Deprecation in US Gov Cloud

Type: Plan for change

Service category: All Azure AD applications

Product capability: Standards

Azure Active Directory will deprecate the following protocols starting March 31, 2021:

- TLS 1.0
- TLS 1.1
- 3DES cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA)

All client-server and browser-server combinations should use TLS 1.2 and modern cipher suites to maintain a secure connection to Azure Active Directory for Azure, Office 365, and Microsoft 365 services.

Affected environments are:

- Azure US Gov
- [Office 365 GCC High & DoD](#)

For guidance to remove deprecating protocols dependencies, please refer to [Enable support for TLS 1.2 in your environment for Azure AD TLS 1.1 and 1.0 deprecation.](#)

Assign applications to roles on administrative unit and object scope

Type: New feature

Service category: RBAC

Product capability: Access Control

This feature enables the ability to assign an application (SPN) to an administrator role on the administrative unit scope. To learn more, refer to [Assign scoped roles to an administrative unit.](#)

Now you can disable and delete guest users when they're denied access to a resource

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

Disable and delete is an advanced control in Azure AD Access Reviews to help organizations better manage external guests in Groups and Apps. If guests are denied in an access review, **disable and delete** will automatically block them from signing in for 30 days. After 30 days, then they'll be removed from the tenant altogether.

For more information about this feature, see [Disable and delete external identities with Azure AD Access Reviews](#).

Access Review creators can add custom messages in emails to reviewers

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

In Azure AD access reviews, administrators creating reviews can now write a custom message to the reviewers. Reviewers will see the message in the email they receive that prompts them to complete the review. To learn more about using this feature, see step 14 of the [Create a single-stage review](#) section.

New provisioning connectors in the Azure AD Application Gallery - October 2020

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Apple Business Manager](#)
- [Apple School Manager](#)
- [Code42](#)
- [AlertMedia](#)
- [OpenText Directory Services](#)
- [Cinode](#)
- [Global Relay Identity Sync](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Integration assistant for Azure AD B2C

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

The Integration Assistant (preview) experience is now available for Azure AD B2C App registrations. This experience helps guide you in configuring your application for common scenarios.. Learn more about [Microsoft identity platform best practices and recommendations](#).

View role template ID in Azure portal UI

Type: New feature

Service category: Azure roles

Product capability: Access Control

You can now view the template ID of each Azure AD role in the Azure portal. In Azure AD, select **description** of

the selected role.

It's recommended that customers use role template IDs in their PowerShell script and code, instead of the display name. Role template ID is supported for use to [directoryRoles](#) and [roleDefinition](#) objects. For more information on role template IDs, see [Azure AD built-in roles](#).

API connectors for Azure AD B2C sign-up user flows is now in public preview

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

API connectors are now available for use with Azure Active Directory B2C. API connectors enable you to use web APIs to customize your sign-up user flows and integrate with external cloud systems. You can use API connectors to:

- Integrate with custom approval workflows
- Validate user input data
- Overwrite user attributes
- Run custom business logic

Visit the [Use API connectors to customize and extend sign-up](#) documentation to learn more.

State property for connected organizations in entitlement management

Type: New feature

Service category: Directory Management **Product capability:** Entitlement Management

All connected organizations will now have an additional property called "State". The state will control how the connected organization will be used in policies that refer to "all configured connected organizations". The value will be either "configured" (meaning the organization is in the scope of policies that use the "all" clause) or "proposed" (meaning that the organization isn't in scope).

Manually created connected organizations will have a default setting of "configured". Meanwhile, automatically created ones (created via policies that allow any user from the internet to request access) will default to "proposed." Any connected organizations created before September 9 2020 will be set to "configured." Admins can update this property as needed. [Learn more](#).

Azure Active Directory External Identities now has premium advanced security settings for B2C

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

Risk-based Conditional Access and risk detection features of Identity Protection are now available in [Azure AD B2C](#). With these advanced security features, customers can now:

- Leverage intelligent insights to assess risk with B2C apps and end user accounts. Detections include atypical travel, anonymous IP addresses, malware-linked IP addresses, and Azure AD threat intelligence. Portal and API-based reports are also available.
- Automatically address risks by configuring adaptive authentication policies for B2C users. App developers and administrators can mitigate real-time risk by requiring Azure Active Directory Multi-Factor Authentication (MFA) or blocking access depending on the user risk level detected, with additional controls available based on location, group, and app.
- Integrate with Azure AD B2C user flows and custom policies. Conditions can be triggered from built-in user flows in Azure AD B2C or can be incorporated into B2C custom policies. As with other aspects of the B2C user flow, end user experience messaging can be customized. Customization is according to the

organization's voice, brand, and mitigation alternatives.

New Federated Apps available in Azure AD Application gallery - October 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In October 2020 we have added following 27 new applications in our App gallery with Federation support:

Sentry, Bumblebee - Productivity Superapp, ABBYY FlexiCapture Cloud, EAComposer, Genesys Cloud Integration for Azure, Zone Technologies Portal, Beautiful.ai, Datawiza Access Broker, ZOKRI, CheckProof, Ecochallenge.org, atSpoke, Appointment Reminder, Cloud.Market, TravelPerk, Greetly, OrgVitality SSO, Web Cargo Air, Loop Flow CRM, Starmind, Workstem, Retail Zipline, Hoxhunt, MEVISIO, Samsara, Nimbus, Pulse Secure virtual Traffic Manager

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here

<https://aka.ms/AzureADAppRequest>

Provisioning logs can now be streamed to log analytics

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Publish your provisioning logs to log analytics in order to:

- Store provisioning logs for more than 30 days
- Define custom alerts and notifications
- Build dashboards to visualize the logs
- Execute complex queries to analyze the logs

To learn how to use the feature, see [Understand how provisioning integrates with Azure Monitor logs](#).

Provisioning logs can now be viewed by application owners

Type: Changed feature

Service category: Reporting

Product capability: Monitoring & Reporting

You can now allow application owners to monitor activity by the provisioning service and troubleshoot issues without providing them a privileged role or making IT a bottleneck. [Learn more](#).

Renaming 10 Azure Active Directory roles

Type: Changed feature

Service category: Azure roles

Product capability: Access Control

Some Azure Active Directory (AD) built-in roles have names that differ from those that appear in Microsoft 365 admin center, the Azure AD portal, and Microsoft Graph. This inconsistency can cause problems in automated processes. With this update, we're renaming 10 role names to make them consistent. The following table has the new role names:

Role name in MS Graph API	Role name in Azure portal	Proposed new role name in M365 Admin Center, Azure Portal and API
CRM Service Administrator	Dynamics 365 administrator	Dynamics 365 Administrator
Company Administrator	Global administrator	Global Administrator
Exchange Service Administrator	Exchange administrator	Exchange Administrator
Intune Service Administrator	Intune administrator	Intune Administrator
Lync Service Administrator	Skype for Business administrator	Skype for Business Administrator
Power BI Service Administrator	Power BI administrator	Power BI Administrator
SharePoint Service Administrator	SharePoint administrator	SharePoint Administrator
Teams Service Administrator	Teams Service Administrator	Teams Administrator
User Account Administrator	User administrator	User Administrator
Device Administrator	<i>Not shown</i>	Azure AD Joined Device Local Admin

Azure AD B2C support for auth code flow for SPAs using MSAL JS 2.x

Type: Changed feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

MSAL.js version 2.x now includes support for the authorization code flow for single-page web apps (SPAs).

Azure AD B2C will now support the use of the SPA app type on the Azure portal and the use of MSAL.js authorization code flow with PKCE for single-page apps. This will allow SPAs using Azure AD B2C to maintain SSO with newer browsers and abide by newer authentication protocol recommendations. Get started with the [Register a single-page application \(SPA\) in Azure Active Directory B2C](#) tutorial.

Updates to Remember Azure Active Directory Multi-Factor Authentication (MFA) on a trusted device setting

Type: Changed feature

Service category: MFA

Product capability: Identity Security & Protection

We've recently updated the [remember Azure Active Directory Multi-Factor Authentication \(MFA\)](#) on a trusted device feature to extend authentication for up to 365 days. Azure Active Directory (Azure AD) Premium licenses, can also use the [Conditional Access – Sign-in Frequency policy](#) that provides more flexibility for reauthentication settings.

For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to remember multifactor authentication (MFA) on a trusted device setting. To get started, review our [latest guidance on optimizing the reauthentication experience](#).

September 2020

New provisioning connectors in the Azure AD Application Gallery - September 2020

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Coda](#)
- [Cofense Recipient Sync](#)
- [InVision](#)
- [myday](#)
- [SAP Analytics Cloud](#)
- [Webroot Security Awareness](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Cloud Provisioning Public Preview Refresh

Type: New feature

Service category: Azure AD Cloud Provisioning **Product capability:** Identity Lifecycle Management

Azure AD Connect Cloud Provisioning public preview refresh features two major enhancements developed from customer feedback:

- Attribute Mapping Experience through Azure portal

With this feature, IT Admins can map user, group, or contact attributes from AD to Azure AD using various mapping types present today. Attribute mapping is a feature used for standardizing the values of the attributes that flow from Active Directory to Azure Active Directory. One can determine whether to directly map the attribute value as it is from AD to Azure AD or use expressions to transform the attribute values when provisioning users. [Learn more](#)

- On-demand Provisioning or Test User experience

Once you have setup your configuration, you might want to test to see if the user transformation is working as expected before applying it to all your users in scope. With on-demand provisioning, IT Admins can enter the Distinguished Name (DN) of an AD user and see if they're getting synced as expected. On-demand provisioning provides a great way to ensure that the attribute mappings you did previously work as expected. [Learn More](#)

Audited BitLocker Recovery in Azure AD - Public Preview

Type: New feature

Service category: Device Access Management

Product capability: Device Lifecycle Management

When IT admins or end users read BitLocker recovery key(s) they have access to, Azure Active Directory now generates an audit log that captures who accessed the recovery key. The same audit provides details of the device the BitLocker key was associated with.

End users can [access their recovery keys via My Account](#). IT admins can access recovery keys via the [BitLocker recovery key API](#) or via the Azure AD Portal. To learn more, see [View or copy BitLocker keys in the Azure AD Portal](#).

Teams Devices Administrator built-in role

Type: New feature

Service category: RBAC

Product capability: Access Control

Users with the [Teams Devices Administrator](#) role can manage [Teams-certified devices](#) from the Teams Admin Center.

This role allows the user to view all devices at single glance, with the ability to search and filter devices. The user can also check the details of each device including logged-in account and the make and model of the device. The user can change the settings on the device and update the software versions. This role doesn't grant permissions to check Teams activity and call quality of the device.

Advanced query capabilities for Directory Objects

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

All the new query capabilities introduced for Directory Objects in Azure AD APIs are now available in the v1.0 endpoint and production-ready. Developers can Count, Search, Filter, and Sort Directory Objects and related links using the standard OData operators.

To learn more, see the documentation [here](#), and you can also send feedback with this [brief survey](#).

Public preview: continuous access evaluation for tenants who configured Conditional Access policies

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Security & Protection

Continuous access evaluation (CAE) is now available in public preview for Azure AD tenants with Conditional Access policies. With CAE, critical security events and policies are evaluated in real time. This includes account disable, password reset, and location change. To learn more, see [Continuous access evaluation](#).

Public preview: ask users requesting an access package additional questions to improve approval decisions

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

Administrators can now require that users requesting an access package answer additional questions beyond just business justification in Azure AD Entitlement management's My Access portal. The users' answers will then be shown to the approvers to help them make a more accurate access approval decision. To learn more, see [Collect additional requestor information for approval](#).

Public preview: Enhanced user management

Type: New feature

Service category: User Management

Product capability: User Management

The Azure AD portal has been updated to make it easier to find users in the All users and Deleted users pages. Changes in the preview include:

- More visible user properties including object ID, directory sync status, creation type, and identity issuer.
- Search now allows combined search of names, emails, and object IDs.
- Enhanced filtering by user type (member, guest, and none), directory sync status, creation type, company name, and domain name.
- New sorting capabilities on properties like name, user principal name and deletion date.
- A new total users count that updates with any searches or filters.

For more information, please see [User management enhancements \(preview\) in Azure Active Directory](#).

New notes field for Enterprise applications

Type: New feature

Service category: Enterprise Apps **Product capability:** SSO

You can add free text notes to Enterprise applications. You can add any relevant information that will help you manage applications under Enterprise applications. For more information, see [Quickstart: Configure properties for an application in your Azure Active Directory \(Azure AD\) tenant](#).

New Federated Apps available in Azure AD Application gallery - September 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In September 2020 we have added following 34 new applications in our App gallery with Federation support:

[VMware Horizon - Unified Access Gateway](#), [Pulse Secure PCS](#), [Inventory360](#), [Frontitude](#), [BookWidgets](#), [ZVD_Server](#), [HashData for Business](#), [SecureLogin](#), [CyberSolutions MAILBASEΣ/CMSS](#), [CyberSolutions CYBERMAILΣ](#), [LimbleCMMS](#), [Glint Inc](#), [zeroheight](#), [Gender Fitness](#), [Ceo Portal](#), [Grammarly](#), [Fivetran](#), [Kumulus](#), [RSA Archer Suite](#), [TeamzSkill](#), [raumfürraum](#), [Saviynt](#), [BizMerlinHR](#), [Mobile Locker](#), [Zengine](#), [CloudCADI](#), [Simfoni Analytics](#), [Priva Identity & Access Management](#), [Nitro Pro](#), [Eventfinity](#), [Fexa](#), [Secured Signing Enterprise Portal](#), [Secured Signing Enterprise Portal AAD Setup](#), [Wistec Online](#), [Oracle PeopleSoft - Protected by F5 BIG-IP APM](#)

You can also find the documentation of all the applications from here: <https://aka.ms/AppsTutorial>.

For listing your application in the Azure AD app gallery, read the details here:

<https://aka.ms/AzureADAppRequest>.

New delegation role in Azure AD entitlement management: Access package assignment manager

Type: New feature

Service category: User Access Management

Product capability: Entitlement Management

A new Access Package Assignment Manager role has been added in Azure AD entitlement management to provide granular permissions to manage assignments. You can now delegate tasks to a user in this role, who can delegate assignments management of an access package to a business owner. However, an Access Package Assignment Manager can't alter the access package policies or other properties that are set by the administrators.

With this new role, you benefit from the least privileges needed to delegate management of assignments and maintain administrative control on all other access package configurations. To learn more, see [Entitlement management roles](#).

Changes to Privileged Identity Management's onboarding flow

Type: Changed feature

Service category: Privileged Identity Management

Product capability: Privileged Identity Management

Previously, onboarding to Privileged Identity Management (PIM) required user consent and an onboarding flow in PIM's blade that included enrollment in Azure Active Directory Multi-Factor Authentication (MFA). With the recent integration of PIM experience into the Azure AD roles and administrators blade, we are removing this experience. Any tenant with valid P2 license will be auto-onboarded to PIM.

Onboarding to PIM does not have any direct adverse effect on your tenant. You can expect the following changes:

- Additional assignment options such as active vs. eligible with start and end time when you make an

assignment in either PIM or Azure AD roles and administrators blade.

- Additional scoping mechanisms, like Administrative Units and custom roles, introduced directly into the assignment experience.
- If you are a global administrator or privileged role administrator, you may start getting a few additional emails like the PIM weekly digest.
- You might also see ms-pim service principal in the audit log related to role assignment. This expected change shouldn't affect your regular workflow.

For more information, see [Start using Privileged Identity Management](#).

Azure AD Entitlement Management: The Select pane of access package resources now shows by default the resources currently in the selected catalog

Type: Changed feature

Service category: User Access Management

Product capability: Entitlement Management

In the access package creation flow, under the Resource roles tab, the Select pane behavior is changing. Currently, the default behavior is to show all resources that are owned by the user and resources added to the selected catalog.

This experience will be changed to display only the resources currently added in the catalog by default, so that users can easily pick resources from the catalog. The update will help with discoverability of the resources to add to access packages, and reduce risk of inadvertently adding resources owned by the user that aren't part of the catalog. To learn more, see [Create a new access package in Azure AD entitlement management](#).

August 2020

Updates to Azure Active Directory Multi-Factor Authentication Server firewall requirements

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

Starting 1 October 2020, Azure AD Multi-Factor Authentication (MFA) Server firewall requirements will require additional IP ranges.

If you have outbound firewall rules in your organization, update the rules so that your multifactor authentication (MFA) servers can communicate with all the necessary IP ranges. The IP ranges are documented in [Azure Active Directory Multi-Factor Authentication Server firewall requirements](#).

Upcoming changes to user experience in Identity Secure Score

Type: Plan for change

Service category: Identity Protection **Product capability:** Identity Security & Protection

We're updating the Identity Secure Score portal to align with the changes introduced in Microsoft Secure Score's [new release](#).

The preview version with the changes will be available at the beginning of September. The changes in the preview version include:

- "Identity Secure Score" renamed to "Secure Score for Identity" for brand alignment with Microsoft Secure Score
- Points normalized to standard scale and reported in percentages instead of points

In this preview, customers can toggle between the existing experience and the new experience. This preview will

last until the end of November 2020. After the preview, the customers will automatically be directed to the new UX experience.

New Restricted Guest Access Permissions in Azure AD - Public Preview

Type: New feature

Service category: Access Control

Product capability: User Management

We've updated directory level permissions for guest users. These permissions allow administrators to require additional restrictions and controls on external guest user access. Admins can now add additional restrictions for external guests' access to user and groups' profile and membership information. With this public preview feature, customers can manage external user access at scale by obfuscating group memberships, including restricting guest users from seeing memberships of the group(s) they are in.

To learn more, see [Restricted Guest Access Permissions](#) and [Users Default Permissions](#).

General availability of delta queries for service principals

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Microsoft Graph Delta Query now supports the resource type in v1.0:

- Service Principal

Now clients can track changes to those resources efficiently and provides the best solution to synchronize changes to those resources with a local data store. To learn how to configure these resources in a query, see [Use delta query to track changes in Microsoft Graph data](#).

General availability of delta queries for oAuth2PermissionGrant

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Microsoft Graph Delta Query now supports the resource type in v1.0:

- OAuth2PermissionGrant

Clients can now track changes to those resources efficiently and provides the best solution to synchronize changes to those resources with a local data store. To learn how to configure these resources in a query, see [Use delta query to track changes in Microsoft Graph data](#).

New Federated Apps available in Azure AD Application gallery - August 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In August 2020 we have added following 25 new applications in our App gallery with Federation support:

[Backup365](#), [Soapbox](#), [Alma SIS](#), [Enlyft Dynamics 365 Connector](#), [Serraview Space Utilization Software Solutions](#), [Uniq](#), [Visibly](#), [Zylo](#), [Edmentum - Courseware Assessments](#) [Exact Path](#), [CyberLAB](#), [Altamira HRM](#), [WireWheel](#), [Zix Compliance and Capture](#), [Greenlight Enterprise Business Controls Platform](#), [Genetec Clearance](#), [iSAMS](#), [VeraSMART](#), [Amiko](#), [Twingate](#), [Funnel Leasing](#), [Scalefusion](#), [Bpanda](#), [Vivun Calendar Connect](#), [FortiGate SSL VPN](#), [Wandera End User](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, read the details here

<https://aka.ms/AzureADAppRequest>

Resource Forests now available for Azure AD DS

Type: New feature **Service category:** Azure AD Domain Services

Product capability: Azure AD Domain Services

The capability of resource forests in Azure AD Domain Services is now generally available. You can now enable authorization without password hash synchronization to use Azure AD Domain Services, including smart-card authorization. To learn more, see [Replica sets concepts and features for Azure Active Directory Domain Services \(preview\)](#).

Regional replica support for Azure AD DS managed domains now available

Type: New feature

Service category: Azure AD Domain Services

Product capability: Azure AD Domain Services

You can expand a managed domain to have more than one replica set per Azure AD tenant. Replica sets can be added to any peered virtual network in any Azure region that supports Azure AD Domain Services. Additional replica sets in different Azure regions provide geographical disaster recovery for legacy applications if an Azure region goes offline. To learn more, see [Replica sets concepts and features for Azure Active Directory Domain Services \(preview\)](#).

General Availability of Azure AD My Sign-Ins

Type: New feature

Service category: Authentications (Logins)

Product capability: End User Experiences

Azure AD My Sign-Ins is a new feature that allows enterprise users to review their sign-in history to check for any unusual activity. Additionally, this feature allows end users to report "This wasn't me" or "This was me" on suspicious activities. To learn more about using this feature, see [View and search your recent sign-in activity from the My Sign-Ins page](#).

SAP SuccessFactors HR driven user provisioning to Azure AD is now generally available

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

You can now integrate SAP SuccessFactors as the authoritative identity source with Azure AD and automate the end-to-end identity lifecycle using HR events like new hires and terminations to drive provisioning and de-provisioning of accounts in Azure AD.

To learn more about how to configure SAP SuccessFactors inbound provisioning to Azure AD, refer to the tutorial [Configure SAP SuccessFactors to Active Directory user provisioning](#).

Custom Open ID Connect MS Graph API support for Azure AD B2C

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

Previously, Custom Open ID Connect providers could only be added or managed through the Azure portal. Now

the Azure AD B2C customers can add and manage them through Microsoft Graph APIs beta version as well. To learn how to configure this resource with APIs, see [identityProvider resource type](#).

Assign Azure AD built-in roles to cloud groups

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

You can now assign Azure AD built-in roles to cloud groups with this new feature. For example, you can assign the SharePoint Administrator role to Contoso_SharePoint_Admins group. You can also use PIM to make the group an eligible member of the role, instead of granting standing access. To learn how to configure this feature, see [Use cloud groups to manage role assignments in Azure Active Directory \(preview\)](#).

Insights Business Leader built-in role now available

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

Users in the Insights Business Leader role can access a set of dashboards and insights via the [Microsoft 365 Insights application](#). This includes full access to all dashboards and presented insights and data exploration functionality. However, users in this role don't have access to product configuration settings, which is the responsibility of the Insights Administrator role. To learn more about this role, see [Administrator role permissions in Azure Active Directory](#)

Insights Administrator built-in role now available

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

Users in the Insights Administrator role can access the full set of administrative capabilities in the [Microsoft 365 Insights application](#). A user in this role can read directory information, monitor service health, file support tickets, and access the Insights administrator settings aspects. To learn more about this role, see [Administrator role permissions in Azure Active Directory](#)

Application Admin and Cloud Application Admin can manage extension properties of applications

Type: Changed feature

Service category: Azure AD roles

Product capability: Access Control

Previously, only the Global Administrator could manage the [extension property](#). We're now enabling this capability for the Application Administrator and Cloud Application Administrator as well.

MIM 2016 SP2 hotfix 4.6.263.0 and connectors 1.1.1301.0

Type: Changed feature

Service category: Microsoft Identity Manager

Product capability: Identity Lifecycle Management

A [hotfix rollup package \(build 4.6.263.0\)](#) is available for Microsoft Identity Manager (MIM) 2016 Service Pack 2 (SP2). This rollup package contains updates for the MIM CM, MIM Synchronization Manager, and PAM components. In addition, the MIM generic connectors build 1.1.1301.0 includes updates for the Graph connector.

July 2020

As an IT Admin, I want to target client apps using Conditional Access

Type: Plan for change

Service category: Conditional Access

Product capability: Identity Security & Protection

With the GA release of the client apps condition in Conditional Access, new policies will now apply by default to all client applications. This includes legacy authentication clients. Existing policies will remain unchanged, but the *Configure Yes/No* toggle will be removed from existing policies to easily see which client apps are applied to by the policy.

When creating a new policy, make sure to exclude users and service accounts that are still using legacy authentication; if you don't, they will be blocked. [Learn more](#).

Upcoming SCIM compliance fixes

Type: Plan for change

Service category: App Provisioning

Product capability: Identity Lifecycle Management

The Azure AD provisioning service leverages the SCIM standard for integrating with applications. Our implementation of the SCIM standard is evolving, and we expect to make changes to our behavior around how we perform PATCH operations as well as set the property "active" on a resource. [Learn more](#).

Group owner setting on Azure Admin portal will be changed

Type: Plan for change

Service category: Group Management

Product capability: Collaboration

Owner settings on Groups general setting page can be configured to restrict owner assignment privileges to a limited group of users in the Azure Admin portal and Access Panel. We will soon have the ability to assign group owner privilege not only on these two UX portals but also enforce the policy on the backend to provide consistent behavior across endpoints, such as PowerShell and Microsoft Graph.

We will start to disable the current setting for the customers who are not using it and will offer an option to scope users for group owner privilege in the next few months. For guidance on updating group settings, see Edit your group information using [Azure Active Directory](#).

Azure Active Directory Registration Service is ending support for TLS 1.0 and 1.1

Type: Plan for change

Service category: Device Registration and Management

Product capability: Platform

Transport layer security (TLS) 1.2 and update servers and clients will soon communicate with Azure Active Directory Device Registration Service. Support for TLS 1.0 and 1.1 for communication with Azure AD Device Registration service will retire:

- On August 31, 2020, in all sovereign clouds (GCC High, DoD, etc.)
- On October 30, 2020, in all commercial clouds

[Learn more](#) about TLS 1.2 for the Azure AD Registration Service.

Windows Hello for Business Sign Ins visible in Azure AD Sign In Logs

Type: Fixed

Service category: Reporting

Product capability: Monitoring & Reporting

Windows Hello for Business allows end users to sign into Windows machines with a gesture (such as a PIN or biometric). Azure AD admins may want to differentiate Windows Hello for Business sign-ins from other Windows sign-ins as part of an organization's journey to passwordless authentication.

Admins can now see whether a Windows authentication used Windows Hello for Business by checking the Authentication Details tab for a Windows sign-in event in the Azure AD Sign-Ins blade in the Azure portal. Windows Hello for Business authentications will include "WindowsHelloForBusiness" in the Authentication Method field. For more information on interpreting Sign-In Logs, please see the [Sign-In Logs documentation](#).

Fixes to group deletion behavior and performance improvements

Type: Fixed

Service category: App Provisioning

Product capability: Identity Lifecycle Management

Previously, when a group changed from "in-scope" to "out-of-scope" and an admin clicked restart before the change was completed, the group object was not being deleted. Now the group object will be deleted from the target application when it goes out of scope (disabled, deleted, unassigned, or did not pass scoping filter). [Learn more](#).

Public Preview: Admins can now add custom content in the email to reviewers when creating an access review

Type: New feature

Service category: Access Reviews

Product capability: Identity Governance

When a new access review is created, the reviewer receives an email requesting them to complete the access review. Many of our customers asked for the ability to add custom content to the email, such as contact information, or other additional supporting content to guide the reviewer.

Now available in public preview, administrators can specify custom content in the email sent to reviewers by adding content in the "advanced" section of Azure AD Access Reviews. For guidance on creating access reviews, see [Create an access review of groups and applications in Azure AD access reviews](#).

Authorization Code Flow for Single-page apps available

Type: New feature

Service category: Authentications (Logins)

Product capability: Developer Experience

Because of modern browser 3rd party cookie restrictions such as Safari ITP, SPAs will have to use the authorization code flow rather than the implicit flow to maintain SSO, and MSAL.js v 2.x will now support the authorization code flow.

There are corresponding updates to the Azure portal so you can update your SPA to be type "spa" and use the auth code flow. See [Sign in users and get an access token in a JavaScript SPA using the auth code flow](#) for further guidance.

Azure AD Application Proxy now supports the Remote Desktop Services Web Client

Type: New feature

Service category: App Proxy

Product capability: Access Control

Azure AD Application Proxy now supports the Remote Desktop Services (RDS) Web Client. The RDS web client

allows users to access Remote Desktop infrastructure through any HTML5-capable browser such as Microsoft Edge, Internet Explorer 11, Google Chrome, etc. Users can interact with remote apps or desktops like they would with a local device from anywhere. By using Azure AD Application Proxy you can increase the security of your RDS deployment by enforcing pre-authentication and Conditional Access policies for all types of rich client apps. For guidance, see [Publish Remote Desktop with Azure AD Application Proxy](#).

Next generation Azure AD B2C user flows in public preview

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

Simplified user flow experience offers feature parity with preview features and is the home for all new features. Users will be able to enable new features within the same user flow, reducing the need to create multiple versions with every new feature release. Lastly, the new, user-friendly UX simplifies the selection and creation of user flows. Try it now by [creating a user flow](#).

For more information about users flows, see [User flow versions in Azure Active Directory B2C](#).

New Federated Apps available in Azure AD Application gallery - July 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In July 2020 we have added following 55 new applications in our App gallery with Federation support:

Clap Your Hands, Appreiz, Inextor Vault, Beekast, Templafy OpenID Connect, PeterConnects receptionist, AlohaCloud, Control Tower, Cocoom, COINS Construction Cloud, Medxnote MT, Reflekt, Rever, MyCompanyArchive, GReminders, Titanfile, Wootric, SolarWinds Orion, OpenText Directory Services, Datasite, BlogIn, IntSights, kpifire, Textline, Cloud Academy - SSO, Community Spark, Chatwork, CloudSign, C3M Cloud Control, SmartHR, NumlyEngage™, Michigan Data Hub Single Sign-On, Egress, SendSafely, Eletive, Right-Hand Cybersecurity ADI, Fyde Enterprise Authentication, Verme, Lenses.io, Momenta, Uprise, Q, CloudCords, TellMe Bot, Inspire, Mavericks Identity Orchestrator SAML Connector, Smartschool (School Management System), Zepto - Intelligent timekeeping, Studi.ly, Trackplan, Skedda, WhosOnLocation, Coggle, Kemp LoadMaster, BrowserStack Single Sign-on

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>

For listing your application in the Azure AD app gallery, please read the details here

<https://aka.ms/AzureADAppRequest>

View role assignments across all scopes and ability to download them to a csv file

Type: Changed feature

Service category: Azure AD roles

Product capability: Access Control

You can now view role assignments across all scopes for a role in the "Roles and administrators" tab in the Azure AD portal. You can also download those role assignments for each role into a CSV file. For guidance on viewing and adding role assignments, see [View and assign administrator roles in Azure Active Directory](#).

Azure Active Directory Multi-Factor Authentication Software Development (Azure MFA SDK) Deprecation

Type: Deprecated

Service category: MFA

Product capability: Identity Security & Protection

The Azure Active Directory Multi-Factor Authentication Software Development (Azure MFA SDK) reached the end of life on November 14th, 2018, as first announced in November 2017. Microsoft will be shutting down the SDK service effective on September 30th, 2020. Any calls made to the SDK will fail.

If your organization is using the Azure MFA SDK, you need to migrate by September 30th, 2020:

- Azure MFA SDK for MIM: If you use the SDK with MIM, you should migrate to Azure AD Multi-Factor Authentication (MFA) Server and activate Privileged Access Management (PAM) following these [instructions](#).
 - Azure MFA SDK for customized apps: Consider integrating your app into Azure AD and use Conditional Access to enforce MFA. To get started, review this [page](#).
-

June 2020

User risk condition in Conditional Access policy

Type: Plan for change

Service category: Conditional Access

Product capability: Identity Security & Protection

User risk support in Azure AD Conditional Access policy allows you to create multiple user risk-based policies. Different minimum user risk levels can be required for different users and apps. Based on user risk, you can create policies to block access, require multifactor authentication, secure password change, or redirect to Microsoft Cloud App Security to enforce session policy, such as additional auditing.

The user risk condition requires Azure AD Premium P2 because it uses Azure Identity Protection, which is a P2 offering. For more information about conditional access, refer to [Azure AD Conditional Access documentation](#).

SAML SSO now supports apps that require SPNameQualifier to be set when requested

Type: Fixed

Service category: Enterprise Apps

Product capability: SSO

Some SAML applications require SPNameQualifier to be returned in the assertion subject when requested. Now Azure AD responds correctly when a SPNameQualifier is requested in the request NameID policy. This also works for SP initiated sign-in, and IdP initiated sign-in will follow. To learn more about SAML protocol in Azure Active Directory, see [Single Sign-On SAML protocol](#).

Azure AD B2B Collaboration supports inviting MSA and Google users in Azure Government tenants

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Azure Government tenants using the B2B collaboration features can now invite users that have a Microsoft or Google account. To find out if your tenant can use these capabilities, follow the instructions at [How can I tell if B2B collaboration is available in my Azure US Government tenant?](#).

User object in MS Graph v1 now includes externalUserState and externalUserStateChangedDateTime properties

Type: New feature

Service category: B2B

Product capability: B2B/B2C

The externalUserState and externalUserStateChangedDateTime properties can be used to find invited B2B guests who have not accepted their invitations yet as well as build automation such as deleting users who haven't

accepted their invitations after some number of days. These properties are now available in MS Graph v1. For guidance on using these properties, refer to [User resource type](#).

Manage authentication sessions in Azure AD Conditional Access is now generally available

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Authentication session management capabilities allow you to configure how often your users need to provide sign-in credentials and whether they need to provide credentials after closing and reopening browsers to offer more security and flexibility in your environment.

Additionally, authentication session management used to only apply to the First Factor Authentication on Azure AD joined, Hybrid Azure AD joined, and Azure AD registered devices. Now authentication session management will apply to multifactor authentication (MFA) as well. For more information, see [Configure authentication session management with Conditional Access](#).

New Federated Apps available in Azure AD Application gallery - June 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In June 2020 we have added the following 29 new applications in our App gallery with Federation support:

[Shopify Plus](#), [Ekarda](#), [MailGates](#), [BullseyeTDP](#), [Raketa](#), [Segment](#), [Ai Auditor](#), [Pobuca Connect](#), [Proto.io](#), [Gatekeeper](#), [Hub Planner](#), [Ansira-Partner Go-to-Market Toolbox](#), [IBM Digital Business Automation on Cloud](#), [Kisi Physical Security](#), [ViewpointOne](#), [IntelligenceBank](#), [pymetrics](#), [Zero](#), [InStation](#), [edX for Business SAML 2.0 Integration](#), [MOOC Office 365](#), [SmartKargo](#), [PKI signing platform](#), [SiteIntel](#), [Field iD](#), [Curricula SAML](#), [Perforce Helix Core - Helix Authentication Service](#), [MyCompliance Cloud](#), [Smallstep SSH](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>. For listing your application in the Azure AD app gallery, please read the details here: <https://aka.ms/AzureADAppRequest>.

API connectors for External Identities self-service sign-up are now in public preview

Type: New feature

Service category: B2B

Product capability: B2B/B2C

External Identities API connectors enable you to leverage web APIs to integrate self-service sign-up with external cloud systems. This means you can now invoke web APIs as specific steps in a sign-up flow to trigger cloud-based custom workflows. For example, you can use API connectors to:

- Integrate with a custom approval workflows.
- Perform identity proofing
- Validate user input data
- Overwrite user attributes
- Run custom business logic

For more information about all of the experiences possible with API connectors, see [Use API connectors to customize and extend self-service sign-up](#), or [Customize External Identities self-service sign-up with web API integrations](#).

Provision on-demand and get users into your apps in seconds

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

The Azure AD provisioning service currently operates on a cyclic basis. The service runs every 40 mins. The [on-demand provisioning capability](#) allows you to pick a user and provision them in seconds. This capability allows you to quickly troubleshoot provisioning issues, without having to do a restart to force the provisioning cycle to start again.

New permission for using Azure AD entitlement management in Graph

Type: New feature

Service category: Other

Product capability: Entitlement Management

A new delegated permission `EntitlementManagement.Read.All` is now available for use with the Entitlement Management API in Microsoft Graph beta. To find out more about the available APIs, see [Working with the Azure AD entitlement management API](#).

Identity Protection APIs available in v1.0

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

The `riskyUsers` and `riskDetections` Microsoft Graph APIs are now generally available. Now that they are available at the v1.0 endpoint, we invite you to use them in production. For more information, please check out the [Microsoft Graph docs](#).

Sensitivity labels to apply policies to Microsoft 365 groups is now generally available

Type: New feature

Service category: Group Management

Product capability: Collaboration

You can now create sensitivity labels and use the label settings to apply policies to Microsoft 365 groups, including privacy (Public or Private) and external user access policy. You can create a label with the privacy policy to be Private, and external user access policy to not allow to add guest users. When a user applies this label to a group, the group will be private, and no guest users are allowed to be added to the group.

Sensitivity labels are important to protect your business-critical data and enable you to manage groups at scale, in a compliant and secure fashion. For guidance on using sensitivity labels, refer to [Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory \(preview\)](#).

Updates to support for Microsoft Identity Manager for Azure AD Premium customers

Type: Changed feature

Service category: Microsoft Identity Manager

Product capability: Identity Lifecycle Management

Azure Support is now available for Azure AD integration components of Microsoft Identity Manager 2016, through the end of Extended Support for Microsoft Identity Manager 2016. Read more at [Support update for Azure AD Premium customers using Microsoft Identity Manager](#).

The use of group membership conditions in SSO claims configuration is increased

Type: Changed feature

Service category: Enterprise Apps

Product capability: SSO

Previously, the number of groups you could use when you conditionally change claims based on group membership within any single application configuration was limited to 10. The use of group membership conditions in SSO claims configuration has now increased to a maximum of 50 groups. For more information on how to configure claims, refer to [Enterprise Applications SSO claims configuration](#).

Enabling basic formatting on the Sign In Page Text component in Company Branding.

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

The Company Branding functionality on the Azure AD/Microsoft 365 login experience has been updated to allow the customer to add hyperlinks and simple formatting, including bold font, underline, and italics. For guidance on using this functionality, see [Add branding to your organization's Azure Active Directory sign-in page](#).

Provisioning performance improvements

Type: Changed feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

The provisioning service has been updated to reduce the time for an [incremental cycle](#) to complete. This means that users and groups will be provisioned into their applications faster than they were previously. All new provisioning jobs created after 6/10/2020 will automatically benefit from the performance improvements. Any applications configured for provisioning before 6/10/2020 will need to restart once after 6/10/2020 to take advantage of the performance improvements.

Announcing the deprecation of ADAL and MS Graph Parity

Type: Deprecated

Service category: N/A

Product capability: Device Lifecycle Management

Now that Microsoft Authentication Libraries (MSAL) is available, we will no longer add new features to the Azure Active Directory Authentication Libraries (ADAL) and will end security patches on June 30th, 2022. For more information on how to migrate to MSAL, refer to [Migrate applications to Microsoft Authentication Library \(MSAL\)](#).

Additionally, we have finished the work to make all Azure AD Graph functionality available through MS Graph. So, Azure AD Graph APIs will receive only bugfix and security fixes through June 30th, 2022. For more information, see [Update your applications to use Microsoft Authentication Library and Microsoft Graph API](#)

May 2020

Retirement of properties in signIns, riskyUsers, and riskDetections APIs

Type: Plan for change

Service category: Identity Protection

Product capability: Identity Security & Protection

Currently, enumerated types are used to represent the riskType property in both the riskDetections API and riskyUserHistoryItem (in preview). Enumerated types are also used for the riskEventTypes property in the signIns API. Going forward we will represent these properties as strings.

Customers should transition to the riskEventType property in the beta riskDetections and riskyUserHistoryItem API, and to riskEventTypes_v2 property in the beta signIns API by September 9th, 2020. At that date, we will be

retiring the current riskType and riskEventTypes properties. For more information, refer to [Changes to risk event properties and Identity Protection APIs on Microsoft Graph](#).

Deprecation of riskEventTypes property in signIns v1.0 API on Microsoft Graph

Type: Plan for change

Service category: Reporting

Product capability: Identity Security & Protection

Enumerated types will switch to string types when representing risk event properties in Microsoft Graph September 2020. In addition to impacting the preview APIs, this change will also impact the in-production signIns API.

We have introduced a new riskEventTypes_v2 (string) property to the signIns v1.0 API. We will retire the current riskEventTypes (enum) property on June 11, 2022 in accordance with our Microsoft Graph deprecation policy. Customers should transition to the riskEventTypes_v2 property in the v1.0 signIns API by June 11, 2022. For more information, refer to [Deprecation of riskEventTypes property in signIns v1.0 API on Microsoft Graph](#).

Upcoming changes to multifactor authentication (MFA) email notifications

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

We are making the following changes to the email notifications for cloud multifactor authentication (MFA):

E-mail notifications will be sent from the following address: azure-noreply@microsoft.com and msonlineservicesteam@microsoftonline.com. We're updating the content of fraud alert emails to better indicate the required steps to unblock users.

New self-service sign up for users in federated domains who can't access Microsoft Teams because they aren't synced to Azure Active Directory.

Type: Plan for change

Service category: Authentications (Logins)

Product capability: User Authentication

Currently, users who are in domains federated in Azure AD, but who are not synced into the tenant, can't access Teams. Starting at the end of June, this new capability will enable them to do so by extending the existing email verified sign up feature. This will allow users who can sign in to a federated IdP, but who don't yet have a user object in Azure AD, to have a user object created automatically and be authenticated for Teams. Their user object will be marked as "self-service sign up." This is an extension of the existing capability to do email verified self-sign up that users in managed domains can do and can be controlled using the same flag. This change will complete rolling out during the following two months. Watch for documentation updates [here](#).

Upcoming fix: The OIDC discovery document for the Azure Government cloud is being updated to reference the correct Graph endpoints.

Type: Plan for change

Service category: Sovereign Clouds

Product capability: User Authentication

Starting in June, the OIDC discovery document [Microsoft identity platform and OpenID Connect protocol](#) on the [Azure Government cloud](#) endpoint (login.microsoftonline.us), will begin to return the correct [National cloud graph endpoint](#) (<https://graph.microsoft.us> or <https://dod-graph.microsoft.us>), based on the tenant provided. It currently provides the incorrect Graph endpoint (graph.microsoft.com) "msgraph_host" field.

This bug fix will be rolled out gradually over approximately 2 months.

Azure Government users will no longer be able to sign in on login.microsoftonline.com

Type: Plan for Change

Service category: Sovereign Clouds

Product capability: User Authentication

On 1 June 2018, the official Azure Active Directory (Azure AD) Authority for Azure Government changed from <https://login-us.microsoftonline.com> to <https://login.microsoftonline.us>. If you own an application within an Azure Government tenant, you must update your application to sign users in on the .us endpoint.

Starting May 5th, Azure AD will begin enforcing the endpoint change, blocking Azure Government users from signing into apps hosted in Azure Government tenants using the public endpoint (microsoftonline.com).

Impacted apps will begin seeing an error AADSTS900439 - USGClientNotSupportedOnPublicEndpoint.

There will be a gradual rollout of this change with enforcement expected to be complete across all apps June 2020. For more details, please see the [Azure Government blog post](#).

SAML Single Logout request now sends NameID in the correct format

Type: Fixed

Service category: Authentications (Logins)

Product capability: User Authentication

When a user clicks on sign-out (e.g., in the MyApps portal), Azure AD sends a SAML Single Logout message to each app that is active in the user session and has a Logout URL configured. These messages contain a NameID in a persistent format.

If the original SAML sign-in token used a different format for NameID (e.g. email/UPN), then the SAML app cannot correlate the NameID in the logout message to an existing session (as the NameIDs used in both messages are different), which caused the logout message to be discarded by the SAML app and the user to stay logged in. This fix makes the sign-out message consistent with the NameID configured for the application.

Hybrid Identity Administrator role is now available with Cloud Provisioning

Type: New feature

Service category: Azure AD Cloud Provisioning

Product capability: Identity Lifecycle Management

IT Admins can start using the new "Hybrid Admin" role as the least privileged role for setting up Azure AD Connect Cloud Provisioning. With this new role, you no longer have to use the Global Admin role to setup and configure Cloud Provisioning. [Learn more](#).

New Federated Apps available in Azure AD Application gallery - May 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In May 2020, we have added the following 36 new applications in our App gallery with Federation support:

[Moula](#), [SurveyPal](#), [Kbot365](#), [TackleBox](#), [Powell Teams](#), [Talentsoft Assistant](#), [ASC Recording Insights](#), [GO1](#), [B-Engaged](#), [Competella Contact Center Workgroup](#), [Asite](#), [ImageSoft Identity](#), [My IBISWorld](#), [insuite](#), [Change Process Management](#), [Cyara CX Assurance Platform](#), [Smart Global Governance](#), [Prezi](#), [Mapbox](#), [Datava](#), [Enterprise Service Platform](#), [Whimsical](#), [Trelica](#), [EasySSO for Confluence](#), [EasySSO for BitBucket](#), [EasySSO for Bamboo](#), [Torii](#), [Axiad Cloud](#), [Humanage](#), [ColorTokens ZTNA](#), [CCH Tagetik](#), [ShareVault](#), [Vyond](#), [TextExpander](#), [Anyone Home CRM](#), [askSpoke](#), [ice Contact Center](#)

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>.

For listing your application in the Azure AD app gallery, please read the details here
<https://aka.ms/AzureADAppRequest>.

Report-only mode for Conditional Access is now generally available

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

[Report-only mode for Azure AD Conditional Access](#) lets you evaluate the result of a policy without enforcing access controls. You can test report-only policies across your organization and understand their impact before enabling them, making deployment safer and easier. Over the past few months, we've seen strong adoption of report-only mode—over 26M users are already in scope of a report-only policy. With the announcement today, new Azure AD Conditional Access policies will be created in report-only mode by default. This means you can monitor the impact of your policies from the moment they're created. And for those of you who use the MS Graph APIs, you can [manage report-only policies programmatically](#) as well.

Self-service sign up for guest users

Type: New feature

Service category: B2B

Product capability: B2B/B2C

With External Identities in Azure AD, you can allow people outside your organization to access your apps and resources while letting them sign in using whatever identity they prefer. When sharing an application with external users, you might not always know in advance who will need access to the application. With [self-service sign-up](#), you can enable guest users to sign up and gain a guest account for your line of business (LOB) apps. The sign-up flow can be created and customized to support Azure AD and social identities. You can also collect additional information about the user during sign-up.

Conditional Access Insights and Reporting workbook is generally available

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

The [insights and reporting workbook](#) gives admins a summary view of Azure AD Conditional Access in their tenant. With the capability to select an individual policy, admins can better understand what each policy does and monitor any changes in real time. The workbook streams data stored in Azure Monitor, which you can set up in a few minutes [following these instructions](#). To make the dashboard more discoverable, we've moved it to the new insights and reporting tab within the Azure AD Conditional Access menu.

Policy details blade for Conditional Access is in public preview

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

The new [policy details blade](#) displays the assignments, conditions, and controls satisfied during conditional access policy evaluation. You can access the blade by selecting a row in the Conditional Access or Report-only tabs of the Sign-in details.

New query capabilities for Directory Objects in Microsoft Graph are in Public Preview

Type: New feature

Service category: MS Graph Product capability: Developer Experience

New capabilities are being introduced for Microsoft Graph Directory Objects APIs, enabling Count, Search, Filter, and Sort operations. This will give developers the ability to quickly query our Directory Objects without workarounds such as in-memory filtering and sorting. Find out more in this [blog post](#).

We are currently in Public Preview, looking for feedback. Please send your comments with this [brief survey](#).

Configure SAML-based single sign-on using Microsoft Graph API (Beta)

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

Support for creating and configuring an application from the Azure AD Gallery using MS Graph APIs in Beta is now available. If you need to set up SAML-based single sign-on for multiple instances of an application, save time by using the Microsoft Graph APIs to [automate the configuration of SAML-based single sign-on](#).

New provisioning connectors in the Azure AD Application Gallery - May 2020

Type: New feature

Service category: App Provisioning

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [8x8](#)
- [Juno Journey](#)
- [MediusFlow](#)
- [New Relic by Organization](#)
- [Oracle Cloud Infrastructure Console](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

SAML Token Encryption is Generally Available

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

[SAML token encryption](#) allows applications to be configured to receive encrypted SAML assertions. The feature is now generally available in all clouds.

Group name claims in application tokens is Generally Available

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

The group claims issued in a token can now be limited to just those groups assigned to the application. This is especially important when users are members of large numbers of groups and there was a risk of exceeding token size limits. With this new capability in place, the ability to [add group names to tokens](#) is generally available.

Workday Writeback now supports setting work phone number attributes

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

We have enhanced the Workday Writeback provisioning app to now support writeback of work phone number and mobile number attributes. In addition to email and username, you can now configure the Workday Writeback provisioning app to flow phone number values from Azure AD to Workday. For more details on how to configure phone number writeback, refer to the [Workday Writeback](#) app tutorial.

Publisher Verification (preview)

Type: New feature

Service category: Other

Product capability: Developer Experience

Publisher verification (preview) helps admins and end users understand the authenticity of application developers integrating with the Microsoft identity platform. For details, refer to [Publisher verification \(preview\)](#).

Authorization Code Flow for Single-page apps

Type: Changed feature **Service category:** Authentication **Product capability:** Developer Experience

Because of modern browser [3rd party cookie restrictions such as Safari ITP](#), SPAs will have to use the authorization code flow rather than the implicit flow to maintain SSO; MSAL.js v 2.x will now support the authorization code flow. There are corresponding updates to the Azure portal so you can update your SPA to be type "spa" and use the auth code flow. For guidance, refer to [Quickstart: Sign in users and get an access token in a JavaScript SPA using the auth code flow](#).

Improved Filtering for Devices is in Public Preview

Type: Changed Feature

Service category: Device Management **Product capability:** Device Lifecycle Management

Previously, the only filters you could use were "Enabled" and "Activity date." Now, you can [filter your list of devices on more properties](#), including OS type, join type, compliance, and more. These additions should simplify locating a particular device.

The new App registrations experience for Azure AD B2C is now generally available

Type: Changed Feature

Service category: B2C - Consumer Identity Management

Product capability: Identity Lifecycle Management

The new App registrations experience for Azure AD B2C is now generally available.

Previously, you had to manage your B2C consumer-facing applications separately from the rest of your apps using the legacy 'Applications' experience. That meant different app creation experiences across different places in Azure.

The new experience shows all B2C app registrations and Azure AD app registrations in one place and provides a consistent way to manage them. Whether you need to manage a customer-facing app or an app that has access to Microsoft Graph to programmatically manage Azure AD B2C resources, you only need to learn one way to do things.

You can reach the new experience by navigating the Azure AD B2C service and selecting the App registrations blade. The experience is also accessible from the Azure Active Directory service.

The Azure AD B2C App registrations experience is based on the general [App Registration experience](#) for Azure AD tenants but is tailored for Azure AD B2C. The legacy "Applications" experience will be deprecated in the future.

For more information, visit [The New app registration experience for Azure AD B2C](#).

April 2020

Combined security info registration experience is now generally available

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Security & Protection

The combined registration experience for Multi-Factor Authentication (MFA) and Self-Service Password Reset (SSPR) is now generally available. This new registration experience enables users to register for multifactor authentication (MFA) and SSPR in a single, step-by-step process. When you deploy the new experience for your organization, users can register in less time and with fewer hassles. Check out the blog post [here](#).

Continuous Access Evaluation

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Security & Protection

Continuous Access Evaluation is a new security feature that enables near real-time enforcement of policies on relying parties consuming Azure AD Access Tokens when events happen in Azure AD (such as user account deletion). We are rolling this feature out first for Teams and Outlook clients. For more details, please read our [blog](#) and [documentation](#).

SMS Sign-in: Firstline Workers can sign in to Azure AD-backed applications with their phone number and no password

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Office is launching a series of mobile-first business apps that cater to non-traditional organizations, and to employees in large organizations that don't use email as their primary communication method. These apps target frontline employees, deskless workers, field agents, or retail employees that may not get an email address from their employer, have access to a computer, or to IT. This project will let these employees sign in to business applications by entering a phone number and roundtripping a code. For more details, please see our [admin documentation](#) and [end user documentation](#).

Invite internal users to use B2B collaboration

Type: New feature

Service category: B2B

Product capability:

We're expanding B2B invitation capability to allow existing internal accounts to be invited to use B2B collaboration credentials going forward. This is done by passing the user object to the Invite API in addition to typical parameters like the invited email address. The user's object ID, UPN, group membership, app assignment, etc. remain intact, but going forward they'll use B2B to authenticate with their home tenant credentials rather than the internal credentials they used before the invitation. For details, see the [documentation](#).

Report-only mode for Conditional Access is now generally available

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

[Report-only mode for Azure AD Conditional Access](#) lets you evaluate the result of a policy without enforcing access controls. You can test report-only policies across your organization and understand their impact before enabling them, making deployment safer and easier. Over the past few months, we've seen strong adoption of report-only mode, with over 26M users already in scope of a report-only policy. With this announcement, new Azure AD Conditional Access policies will be created in report-only mode by default. This means you can monitor the impact of your policies from the moment they're created. And for those of you who use the MS Graph APIs, you can also [manage report-only policies programmatically](#).

Conditional Access insights and reporting workbook is generally available

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

The Conditional Access [insights and reporting workbook](#) gives admins a summary view of Azure AD Conditional Access in their tenant. With the capability to select an individual policy, admins can better understand what each policy does and monitor any changes in real time. The workbook streams data stored in Azure Monitor, which you can set up in a few minutes [following these instructions](#). To make the dashboard more discoverable, we've moved it to the new insights and reporting tab within the Azure AD Conditional Access menu.

Policy details blade for Conditional Access is in public preview

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

The new [policy details blade](#) displays which assignments, conditions, and controls were satisfied during conditional access policy evaluation. You can access the blade by selecting a row in the **Conditional Access** or **Report-only** tabs of the Sign-in details.

New Federated Apps available in Azure AD App gallery - April 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In April 2020, we've added these 31 new apps with Federation support to the app gallery:

[SincroPool Apps](#), [SmartDB](#), [Float](#), [LMS365](#), [IWT Procurement Suite](#), [Lunni](#), [EasySSO for Jira](#), [Virtual Training Academy](#), [Meraki Dashboard](#), [Microsoft 365 Mover](#), [Speaker Engage](#), [Honestly](#), [Ally](#), [DutyFlow](#), [AlertMedia](#), [gr8 People](#), [Pendo](#), [HighGround](#), [Harmony](#), [Timetabling Solutions](#), [SynchroNet CLICK](#), [empower](#), [Fortes Change Cloud](#), [Litmus](#), [GroupTalk](#), [Frontify](#), [MongoDB Cloud](#), [TicketLMS Learn](#), [COCO](#), [Nitro Productivity Suite](#), [Trend Micro Web Security\(TMWS\)](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Microsoft Graph delta query support for oAuth2PermissionGrant available for Public Preview

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Delta query for oAuth2PermissionGrant is available for public preview! You can now track changes without having to continuously poll Microsoft Graph. [Learn more.](#)

Microsoft Graph delta query support for organizational contact generally available

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Delta query for organizational contacts is generally available! You can now track changes in production apps without having to continuously poll Microsoft Graph. Replace any existing code that continuously polls orgContact data by delta query to significantly improve performance. [Learn more.](#)

Microsoft Graph delta query support for application generally available

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Delta query for applications is generally available! You can now track changes in production apps without having to continuously poll Microsoft Graph. Replace any existing code that continuously polls application data by delta query to significantly improve performance. [Learn more.](#)

Microsoft Graph delta query support for administrative units available for Public Preview

Type: New feature

Service category: MS Graph

Product capability: Developer Experience Delta query for administrative units is available for public preview! You can now track changes without having to continuously poll Microsoft Graph. [Learn more.](#)

Manage authentication phone numbers and more in new Microsoft Graph beta APIs

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

These APIs are a key tool for managing your users' authentication methods. Now you can programmatically pre-register and manage the authenticators used for multifactor authentication (MFA) and self-service password reset (SSPR). This has been one of the most-requested features in the Azure AD Multi-Factor Authentication (MFA), SSPR, and Microsoft Graph spaces. The new APIs we've released in this wave give you the ability to:

- Read, add, update, and remove a user's authentication phones
- Reset a user's password
- Turn on and off SMS-sign-in

For more information, see [Azure AD authentication methods API overview](#).

Administrative Units Public Preview

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

Administrative units allow you to grant admin permissions that are restricted to a department, region, or other segment of your organization that you define. You can use administrative units to delegate permissions to regional administrators or to set policy at a granular level. For example, a User account admin could update profile information, reset passwords, and assign licenses for users only in their administrative unit.

Using administrative units, a central administrator could:

- Create an administrative unit for decentralized management of resources
- Assign a role with administrative permissions over only Azure AD users in an administrative unit
- Populate the administrative units with users and groups as needed

For more information, see [Administrative units management in Azure Active Directory \(preview\)](#).

Printer Administrator and Printer Technician built-in roles

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

Printer Administrator: Users with this role can register printers and manage all aspects of all printer configurations in the Microsoft Universal Print solution, including the Universal Print Connector settings. They can consent to all delegated print permission requests. Printer Administrators also have access to print reports.

Printer Technician: Users with this role can register printers and manage printer status in the Microsoft Universal Print solution. They can also read all connector information. Key tasks a Printer Technician cannot do are set user permissions on printers and sharing printers. [Learn more](#).

Hybrid Identity Admin built-in role

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

Users in this role can enable, configure and manage services and settings related to enabling hybrid identity in Azure AD. This role grants the ability to configure Azure AD to one of the three supported authentication methods—Password hash synchronization (PHS), Pass-through authentication (PTA) or Federation (AD FS or 3rd party federation provider)—and to deploy related on-premises infrastructure to enable them. On-premises infrastructure includes Provisioning and PTA agents. This role grants the ability to enable Seamless Single Sign-On (S-SSO) to enable seamless authentication on non-Windows 10 devices or non-Windows Server 2016 computers. In addition, this role grants the ability to see sign-in logs and to access health and analytics for monitoring and troubleshooting purposes. [Learn more](#).

Network Administrator built-in role

Type: New feature

Service category: Azure AD roles

Product capability: Access Control

Users with this role can review network perimeter architecture recommendations from Microsoft that are based on network telemetry from their user locations. Network performance for Microsoft 365 relies on careful enterprise customer network perimeter architecture, which is generally user location-specific. This role allows for editing of discovered user locations and configuration of network parameters for those locations to facilitate improved telemetry measurements and design recommendations. [Learn more.](#)

Bulk activity and downloads in the Azure AD admin portal experience

Type: New feature

Service category: User Management

Product capability: Directory

Now you can perform bulk activities on users and groups in Azure AD by uploading a CSV file in the Azure AD admin portal experience. You can create users, delete users, and invite guest users. And you can add and remove members from a group.

You can also download lists of Azure AD resources from the Azure AD admin portal experience. You can download the list of users in the directory, the list of groups in the directory, and the members of a particular group.

For more information, check out the following:

- [Create users or invite guest users](#)
 - [Delete users or restore deleted users](#)
 - [Download list of users or Download list of groups](#)
 - [Add \(import\) members or remove members or Download list of members](#) for a group
-

My Staff delegated user management

Type: New feature

Service category: User Management

Product capability:

My Staff enables Firstline Managers, such as a store manager, to ensure that their staff members are able to access their Azure AD accounts. Instead of relying on a central helpdesk, organizations can delegate common tasks, such as resetting passwords or changing phone numbers, to a Firstline Manager. With My Staff, a user who can't access their account can re-gain access in just a couple of clicks, with no helpdesk or IT staff required. For more information, see the [Manage your users with My Staff \(preview\)](#) and [Delegate user management with My Staff \(preview\)](#).

An upgraded end user experience in access reviews

Type: Changed feature

Service category: Access Reviews

Product capability: Identity Governance

We have updated the reviewer experience for Azure AD access reviews in the My Apps portal. At the end of April, your reviewers who are logged in to the Azure AD access reviews reviewer experience will see a banner that will allow them to try the updated experience in My Access. Please note that the updated Access reviews experience offers the same functionality as the current experience, but with an improved user interface on top of new capabilities to enable your users to be productive. [You can learn more about the updated experience here.](#)

This public preview will last until the end of July 2020. At the end of July, reviewers who have not opted into the preview experience will be automatically directed to My Access to perform access reviews. If you wish to have your reviewers permanently switched over to the preview experience in My Access now, [please make a request here](#).

Workday inbound user provisioning and writeback apps now support the latest versions of Workday Web Services API

Type: Changed feature

Service category: App Provisioning

Product capability:

Based on customer feedback, we have now updated the Workday inbound user provisioning and writeback apps in the enterprise app gallery to support the latest versions of the Workday Web Services (WWS) API. With this change, customers can specify the WWS API version that they would like to use in the connection string. This gives customers the ability to retrieve more HR attributes available in the releases of Workday. The Workday Writeback app now uses the recommended Change_Work_Contact_Info Workday web service to overcome the limitations of Maintain_Contact_Info.

If no version is specified in the connection string, by default, the Workday inbound provisioning apps will continue to use WWS v21.1 To switch to the latest Workday APIs for inbound user provisioning, customers need to update the connection string as documented [in the tutorial](#) and also update the XPATHs used for Workday attributes as documented in the [Workday attribute reference guide](#).

To use the new API for writeback, there are no changes required in the Workday Writeback provisioning app. On the Workday side, ensure that the Workday Integration System User (ISU) account has permissions to invoke the Change_Work_Contact business process as documented in the tutorial section, [Configure business process security policy permissions](#).

We have updated our [tutorial guide](#) to reflect the new API version support.

Users with default access role are now in scope for provisioning

Type: Changed feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

Historically, users with the default access role have been out of scope for provisioning. We've heard feedback that customers want users with this role to be in scope for provisioning. As of April 16, 2020, all new provisioning configurations allow users with the default access role to be provisioned. Gradually we will change the behavior for existing provisioning configurations to support provisioning users with this role. [Learn more](#).

Updated provisioning UI

Type: Changed feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

We've refreshed our provisioning experience to create a more focused management view. When you navigate to the provisioning blade for an enterprise application that has already been configured, you'll be able to easily monitor the progress of provisioning and manage actions such as starting, stopping, and restarting provisioning. [Learn more](#).

Dynamic Group rule validation is now available for Public Preview

Type: Changed feature

Service category: Group Management

Product capability: Collaboration

Azure Active Directory (Azure AD) now provides the means to validate dynamic group rules. On the **Validate rules** tab, you can validate your dynamic rule against sample group members to confirm the rule is working as expected. When creating or updating dynamic group rules, administrators want to know whether a user or a device will be a member of the group. This helps evaluate whether a user or device meets the rule criteria and aids in troubleshooting when membership is not expected.

For more information, see [Validate a dynamic group membership rule \(preview\)](#).

Identity Secure Score - Security Defaults and multifactor authentication (MFA) improvement action updates

Type: Changed feature

Service category: N/A

Product capability: Identity Security & Protection

Supporting security defaults for Azure AD improvement actions: Microsoft Secure Score will be updating improvement actions to support [security defaults in Azure AD](#), which make it easier to help protect your organization with pre-configured security settings for common attacks. This will affect the following improvement actions:

- Ensure all users can complete multifactor authentication for secure access
- Require multi-factor authentication (MFA) for administrative roles
- Enable policy to block legacy authentication

Multifactor authentication (MFA) improvement action updates: To reflect the need for businesses to ensure the upmost security while applying policies that work with their business, Microsoft Secure Score has removed three improvement actions centered around multifactor authentication and added two.

Removed improvement actions:

- Register all users for multifactor authentication
- Require multifactor authentication (MFA) for all users
- Require multifactor authentication (MFA) for Azure AD privileged roles

Added improvement actions:

- Ensure all users can complete multifactor authentication for secure access
- Require multifactor authentication (MFA) for administrative roles

These new improvement actions require registering your users or admins for multifactor authentication (MFA) across your directory and establishing the right set of policies that fit your organizational needs. The main goal is to have flexibility while ensuring all your users and admins can authenticate with multiple factors or risk-based identity verification prompts. That can take the form of having multiple policies that apply scoped decisions, or setting security defaults (as of March 16th) that let Microsoft decide when to challenge users for multifactor authentication (MFA). [Read more about what's new in Microsoft Secure Score](#).

March 2020

Unmanaged Azure Active Directory accounts in B2B update for March 2021

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

Beginning on March 31, 2021, Microsoft will no longer support the redemption of invitations by creating unmanaged Azure Active Directory (Azure AD) accounts and tenants for B2B collaboration scenarios. In preparation for this, we encourage you to opt in to [email one-time passcode authentication](#).

Users with the default access role will be in scope for provisioning

Type: Plan for change

Service category: App Provisioning

Product capability: Identity Lifecycle Management

Historically, users with the default access role have been out of scope for provisioning. We've heard feedback that customers want users with this role to be in scope for provisioning. We're working on deploying a change so that all new provisioning configurations will allow users with the default access role to be provisioned.

Gradually, we'll change the behavior for existing provisioning configurations to support provisioning users with this role. No customer action is required. We'll post an update to our [documentation](#) once this change is in place.

Azure AD B2B collaboration will be available in Microsoft Azure operated by 21Vianet (Azure China 21Vianet) tenants

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

The Azure AD B2B collaboration capabilities will be made available in Microsoft Azure operated by 21Vianet (Azure China 21Vianet) tenants, enabling users in an Azure China 21Vianet tenant to collaborate seamlessly with users in other Azure China 21Vianet tenants. [Learn more about Azure AD B2B collaboration](#).

Azure AD B2B Collaboration invitation email redesign

Type: Plan for change

Service category: B2B

Product capability: B2B/B2C

The [emails](#) that are sent by the Azure AD B2B collaboration invitation service to invite users to the directory will be redesigned to make the invitation information and the user's next steps clearer.

HomeRealmDiscovery policy changes will appear in the audit logs

Type: Fixed

Service category: Audit

Product capability: Monitoring & Reporting

We fixed a bug where changes to the [HomeRealmDiscovery policy](#) were not included in the audit logs. You will now be able to see when and how the policy was changed, and by whom.

New Federated Apps available in Azure AD App gallery - March 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In March 2020, we've added these 51 new apps with Federation support to the app gallery:

[Cisco AnyConnect](#), [Zoho One China](#), [PlusPlus](#), [Profit.co SAML App](#), [iPoint Service Provider](#), [contextx.ai SPHERE](#),

Wisdom By Invictus, Flare Digital Signage, Logz.io - Cloud Observability for Engineers, SpectrumU, BizzContact, Elqano SSO, MarketSignShare, CrossKnowledge Learning Suite, Netvision Compas, FCM HUB, RIB A/S, Byggeweb Mobile, GoLinks, Datadog, Zscaler B2B User Portal, LIFT, Planview Enterprise One, WatchTeams, Aster, Skills Workflow, Node Insight, IP Platform, InVision, Pipedrive, Showcase Workshop, Greenlight Integration Platform, Greenlight Compliant Access Management, Grok Learning, Miradore Online, Khoros Care, AskYourTeam, TruNarrative, Smartwaiver, Bizagi Studio for Digital Process Automation, insuiteX, sybo, Britive, WhosOffice, E-days, Kollective SDN, Witivio, Playvox, Korn Ferry 360, Campus Café, Catchpoint, Code42

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Azure AD B2B Collaboration available in Azure Government tenants

Type: New feature

Service category: B2B

Product capability: B2B/B2C

The Azure AD B2B collaboration features are now available between some Azure Government tenants. To find out if your tenant is able to use these capabilities, follow the instructions at [How can I tell if B2B collaboration is available in my Azure US Government tenant?](#).

Azure Monitor integration for Azure Logs is now available in Azure Government

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Azure Monitor integration with Azure AD logs is now available in Azure Government. You can route Azure AD Logs (Audit and Sign-in Logs) to a storage account, event hub and Log Analytics. Please check out the [detailed documentation](#) as well as [deployment plans for reporting and monitoring](#) for Azure AD scenarios.

Identity Protection Refresh in Azure Government

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

We're excited to share that we have now rolled out the refreshed [Azure AD Identity Protection](#) experience in the [Microsoft Azure Government portal](#). For more information, see our [announcement blog post](#).

Disaster recovery: Download and store your provisioning configuration

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

The Azure AD provisioning service provides a rich set of configuration capabilities. Customers need to be able to save their configuration so that they can refer to it later or roll back to a known good version. We've added the ability to download your provisioning configuration as a JSON file and upload it when you need it. [Learn more](#).

SSPR (self-service password reset) now requires two gates for admins in Microsoft Azure operated by 21Vianet (Azure China 21Vianet)

Type: Changed feature

Service category: Self-Service Password Reset

Product capability: Identity Security & Protection

Previously in Microsoft Azure operated by 21Vianet (Azure China 21Vianet), admins using self-service password reset (SSPR) to reset their own passwords needed only one "gate" (challenge) to prove their identity. In public and other national clouds, admins generally must use two gates to prove their identity when using SSPR. But because we didn't support SMS or phone calls in Azure China 21Vianet, we allowed one-gate password reset by admins.

We're creating SSPR feature parity between Azure China 21Vianet and the public cloud. Going forward, admins must use two gates when using SSPR. SMS, phone calls, and Authenticator app notifications and codes will be supported. [Learn more](#).

Password length is limited to 256 characters

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

To ensure the reliability of the Azure AD service, user passwords are now limited in length to 256 characters. Users with passwords longer than this will be asked to change their password on subsequent login, either by contacting their admin or by using the self-service password reset feature.

This change was enabled on March 13th, 2020, at 10AM PST (18:00 UTC), and the error is AADSTS 50052, InvalidPasswordExceedsMaxLength. See the [breaking change notice](#) for more details.

Azure AD sign-in logs are now available for all free tenants through the Azure portal

Type: Changed feature

Service category: Reporting

Product capability: Monitoring & Reporting

Starting now, customers who have free tenants can access the [Azure AD sign-in logs from the Azure portal](#) for up to 7 days. Previously, sign-in logs were available only for customers with Azure Active Directory Premium licenses. With this change, all tenants can access these logs through the portal.

NOTE

Customers still need a premium license (Azure Active Directory Premium P1 or P2) to access the sign-in logs through Microsoft Graph API and Azure Monitor.

Deprecation of Directory-wide groups option from Groups General Settings on Azure portal

Type: Deprecated

Service category: Group Management

Product capability: Collaboration

To provide a more flexible way for customers to create directory-wide groups that best meet their needs, we've replaced the **Directory-wide Groups** option from the **Groups > General** settings in the Azure portal with a link to [dynamic group documentation](#). We've improved our documentation to include more instructions so administrators can create all-user groups that include or exclude guest users.

February 2020

Upcoming changes to custom controls

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

We're planning to replace the current custom controls preview with an approach that allows partner-provided authentication capabilities to work seamlessly with the Azure Active Directory administrator and end user experiences. Today, partner multifactor authentication (MFA) solutions face the following limitations: they work only after a password has been entered; they don't serve as multifactor authentication (MFA) for step-up authentication in other key scenarios; and they don't integrate with end user or administrative credential management functions. The new implementation will allow partner-provided authentication factors to work alongside built-in factors for key scenarios, including registration, usage, multifactor authentication (MFA) claims, step up authentication, reporting, and logging.

Custom controls will continue to be supported in preview alongside the new design until it reaches general availability. At that point, we'll give customers time to migrate to the new design. Because of the limitations of the current approach, we won't onboard new providers until the new design is available. We are working closely with customers and providers and will communicate the timeline as we get closer. [Learn more](#).

Identity Secure Score - multifactor authentication (MFA) improvement action updates

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

To reflect the need for businesses to ensure the upmost security while applying policies that work with their business, Microsoft Secure Score is removing three improvement actions centered around multifactor authentication (MFA), and adding two.

The following improvement actions will be removed:

- Register all users for multifactor authentication (MFA)
- Require multifactor authentication (MFA) for all users
- Require multifactor authentication (MFA) for Azure AD privileged roles

The following improvement actions will be added:

- Ensure all users can complete multifactor authentication (MFA) for secure access
- Require multifactor authentication (MFA) for administrative roles

These new improvement actions will require registering your users or admins for multifactor authentication (MFA) across your directory and establishing the right set of policies that fit your organizational needs. The main goal is to have flexibility while ensuring all your users and admins can authenticate with multiple factors or risk-based identity verification prompts. This can take the form of setting security defaults that let Microsoft decide when to challenge users for multifactor authentication (MFA), or having multiple policies that apply scoped decisions. As part of these improvement action updates, Baseline protection policies will no longer be included in scoring calculations. [Read more about what's coming in Microsoft Secure Score](#).

Azure AD Domain Services SKU selection

Type: New feature

Service category: Azure AD Domain Services

Product capability: Azure AD Domain Services

We've heard feedback that Azure AD Domain Services customers want more flexibility in selecting performance levels for their instances. Starting on February 1, 2020, we switched from a dynamic model (where Azure AD determines the performance and pricing tier based on object count) to a self-selection model. Now customers can choose a performance tier that matches their environment. This change also allows us to enable new scenarios like Resource Forests, and Premium features like daily backups. The object count is now unlimited for all SKUs, but we'll continue to offer object count suggestions for each tier.

No immediate customer action is required. For existing customers, the dynamic tier that was in use on

February 1, 2020, determines the new default tier. There is no pricing or performance impact as the result of this change. Going forward, Azure AD DS customers will need to evaluate performance requirements as their directory size and workload characteristics change. Switching between service tiers will continue to be a no-downtime operation, and we will no longer automatically move customers to new tiers based on the growth of their directory. Furthermore, there will be no price increases, and new pricing will align with our current billing model. For more information, see the [Azure AD DS SKUs documentation](#) and the [Azure AD Domain Services pricing page](#).

New Federated Apps available in Azure AD App gallery - February 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In February 2020, we've added these 31 new apps with Federation support to the app gallery:

[IamIP Patent Platform](#), [Experience Cloud](#), [NS1 SSO For Azure](#), [Barracuda Email Security Service](#), [ABa Reporting](#), [In Case of Crisis - Online Portal](#), [BIC Cloud Design](#), [Beekeeper Azure AD Data Connector](#), [Korn Ferry Assessments](#), [Verkada Command](#), [Splashtop](#), [Syxsense](#), [EAB Navigate](#), [New Relic \(Limited Release\)](#), [Thulium](#), [Ticket Manager](#), [Template Chooser for Teams](#), [Beesy](#), [Health Support System](#), [MURAL](#), [Hive](#), [LavaDo](#), [Wakelet](#), [Firmex VDR](#), [ThingLink for Teachers and Schools](#), [Coda](#), [NearpodApp](#), [WEDO](#), [InvitePeople](#), [Reprints Desk - Article Galaxy](#), [TeamViewer](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New provisioning connectors in the Azure AD Application Gallery - February 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Mixpanel](#)
- [TeamViewer](#)
- [Azure Databricks](#)
- [PureCloud by Genesys](#)
- [Zapier](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Azure AD support for FIDO2 security keys in hybrid environments

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

We're announcing the public preview of Azure AD support for FIDO2 security keys in Hybrid environments. Users can now use FIDO2 security keys to sign in to their Hybrid Azure AD joined Windows 10 devices and get seamless sign-on to their on-premises and cloud resources. Support for Hybrid environments has been the top most-requested feature from our passwordless customers since we initially launched the public preview for FIDO2 support in Azure AD joined devices. Passwordless authentication using advanced technologies like biometrics and public/private key cryptography provide convenience and ease-of-use while being secure. With

this public preview, you can now use modern authentication like FIDO2 security keys to access traditional Active Directory resources. For more information, go to [SSO to on-premises resources](#).

To get started, visit [enable FIDO2 security keys for your tenant](#) for step-by-step instructions.

The new My Account experience is now generally available

Type: Changed feature

Service category: My Profile/Account

Product capability: End User Experiences

My Account, the one stop shop for all end-user account management needs, is now generally available! End users can access this new site via URL, or in the header of the new My Apps experience. Learn more about all the self-service capabilities the new experience offers at [My Account Portal Overview](#).

My Account site URL updating to myaccount.microsoft.com

Type: Changed feature

Service category: My Profile/Account

Product capability: End User Experiences

The new My Account end user experience will be updating its URL to <https://myaccount.microsoft.com> in the next month. Find more information about the experience and all the account self-service capabilities it offers to end users at [My Account portal help](#).

January 2020

The new My Apps portal is now generally available

Type: Plan for change

Service category: My Apps

Product capability: End User Experiences

Upgrade your organization to the new My Apps portal that is now generally available! Find more information on the new portal and collections at [Create collections on the My Apps portal](#).

Workspaces in Azure AD have been renamed to collections

Type: Changed feature

Service category: My Apps

Product capability: End User Experiences

Workspaces, the filters admins can configure to organize their users' apps, will now be referred to as collections. Find more info on how to configure them at [Create collections on the My Apps portal](#).

Azure AD B2C Phone sign-up and sign-in using custom policy (Public Preview)

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

With phone number sign-up and sign-in, developers and enterprises can allow their customers to sign up and sign in using a one-time password sent to the user's phone number via SMS. This feature also lets the customer change their phone number if they lose access to their phone. With the power of custom policies and phone sign-up and sign-in, allows developers and enterprises to communicate their brand through page customization. Find out how to [set up phone sign-up and sign-in with custom policies in Azure AD B2C](#).

New provisioning connectors in the Azure AD Application Gallery - January 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Promapp](#)
- [Zscaler Private Access](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD App gallery - January 2020

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In January 2020, we've added these 33 new apps with Federation support to the app gallery:

[JOSA](#), [Fastly Edge Cloud](#), [Terraform Enterprise](#), [Spintr SSO](#), [Abibot Netlogistik](#), [SkyKick](#), [Upshotly](#), [LeaveBot](#), [DataCamp](#), [TripActions](#), [SmartWork](#), [Dotcom-Monitor](#), [SSOGEN - Azure AD SSO Gateway for Oracle E-Business Suite - EBS](#), [PeopleSoft](#), and [JDE](#), [Hosted MyCirqa SSO](#), [Yuhu Property Management Platform](#), [LumApps](#), [Upwork Enterprise](#), [Talentsoft](#), [SmartDB for Microsoft Teams](#), [PressPage](#), [ContractSafe Saml2 SSO](#), [Maxient Conduct Manager Software](#), [Helpshift](#), [PortalTalk 365](#), [CoreView](#), [Squelch Cloud Office365 Connector](#), [PingFlow Authentication](#), [PrinterLogic SaaS](#), [Taskize Connect](#), [Sandwai](#), [EZRentOut](#), [AssetSonar](#), [Akari Virtual Assistant](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Two new Identity Protection detections

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

We've added two new sign-in linked detection types to Identity Protection: Suspicious inbox manipulation rules and Impossible travel. These offline detections are discovered by Microsoft Cloud App Security (MCAS) and influence the user and sign-in risk in Identity Protection. For more information on these detections, see our [sign-in risk types](#).

Breaking Change: URI Fragments will not be carried through the login redirect

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

Starting on February 8, 2020, when a request is sent to login.microsoftonline.com to sign in a user, the service will append an empty fragment to the request. This prevents a class of redirect attacks by ensuring that the browser wipes out any existing fragment in the request. No application should have a dependency on this behavior. For more information, see [Breaking changes](#) in the Microsoft identity platform documentation.

December 2019

[Integrate SAP SuccessFactors provisioning into Azure AD and on-premises AD \(Public Preview\)](#)

Type: New feature

Service category: App Provisioning

Product capability: Identity Lifecycle Management

You can now integrate SAP SuccessFactors as an authoritative identity source in Azure AD. This integration helps you automate the end-to-end identity lifecycle, including using HR-based events, like new hires or terminations, to control provisioning of Azure AD accounts.

For more information about how to set up SAP SuccessFactors inbound provisioning to Azure AD, see the [Configure SAP SuccessFactors automatic provisioning](#) tutorial.

Support for customized emails in Azure AD B2C (Public Preview)

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

You can now use Azure AD B2C to create customized emails when your users sign up to use your apps. By using DisplayControls (currently in preview) and a third-party email provider (such as, [SendGrid](#), [SparkPost](#), or a custom REST API), you can use your own email template, **From** address, and subject text, as well as support localization and custom one-time password (OTP) settings.

For more information, see [Custom email verification in Azure Active Directory B2C](#).

Replacement of baseline policies with security defaults

Type: Changed feature

Service category: Other

Product capability: Identity Security and Protection

As part of a secure-by-default model for authentication, we're removing the existing baseline protection policies from all tenants. This removal is targeted for completion at the end of February. The replacement for these baseline protection policies is security defaults. If you've been using baseline protection policies, you must plan to move to the new security defaults policy or to Conditional Access. If you haven't used these policies, there is no action for you to take.

For more information about the new security defaults, see [What are security defaults?](#) For more information about Conditional Access policies, see [Common Conditional Access policies](#).

November 2019

Support for the SameSite attribute and Chrome 80

Type: Plan for change

Service category: Authentications (Logins)

Product capability: User Authentication

As part of a secure-by-default model for cookies, the Chrome 80 browser is changing how it treats cookies without the `SameSite` attribute. Any cookie that doesn't specify the `SameSite` attribute will be treated as though it was set to `SameSite=Lax`, which will result in Chrome blocking certain cross-domain cookie sharing scenarios that your app may depend on. To maintain the older Chrome behavior, you can use the `SameSite=None` attribute and add an additional `Secure` attribute, so cross-site cookies can only be accessed over HTTPS connections. Chrome is scheduled to complete this change by February 4, 2020.

We recommend all our developers test their apps using this guidance:

- Set the default value for the **Use Secure Cookie** setting to **Yes**.

- Set the default value for the **SameSite** attribute to **None**.
- Add an additional **SameSite** attribute of **Secure**.

For more information, see [Upcoming SameSite Cookie Changes in ASP.NET and ASP.NET Core](#) and [Potential disruption to customer websites and Microsoft products and services in Chrome version 79 and later](#).

New hotfix for Microsoft Identity Manager (MIM) 2016 Service Pack 2 (SP2)

Type: Fixed

Service category: Microsoft Identity Manager

Product capability: Identity Lifecycle Management

A hotfix rollup package (build 4.6.34.0) is available for Microsoft Identity Manager (MIM) 2016 Service Pack 2 (SP2). This rollup package resolves issues and adds improvements that are described in the "Issues fixed and improvements added in this update" section.

For more information and to download the hotfix package, see [Microsoft Identity Manager 2016 Service Pack 2 \(build 4.6.34.0\) Update Rollup is available](#).

New AD FS app activity report to help migrate apps to Azure AD (Public Preview)

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

Use the new Active Directory Federation Services (AD FS) app activity report, in the Azure portal, to identify which of your apps are capable of being migrated to Azure AD. The report assesses all AD FS apps for compatibility with Azure AD, checks for any issues, and gives guidance about preparing individual apps for migration.

For more information, see [Use the AD FS application activity report to migrate applications to Azure AD](#).

New workflow for users to request administrator consent (Public Preview)

Type: New feature

Service category: Enterprise Apps

Product capability: Access Control

The new admin consent workflow gives admins a way to grant access to apps that require admin approval. If a user tries to access an app, but is unable to provide consent, they can now send a request for admin approval. The request is sent by email, and placed in a queue that's accessible from the Azure portal, to all the admins who have been designated as reviewers. After a reviewer takes action on a pending request, the requesting users are notified of the action.

For more information, see [Configure the admin consent workflow \(preview\)](#).

New Azure AD App Registrations Token configuration experience for managing optional claims (Public Preview)

Type: New feature

Service category: Other

Product capability: Developer Experience

The new **Azure AD App Registrations Token configuration** blade on the Azure portal now shows app developers a dynamic list of optional claims for their apps. This new experience helps to streamline Azure AD app migrations and to minimize optional claims misconfigurations.

For more information, see [Provide optional claims to your Azure AD app](#).

New two-stage approval workflow in Azure AD entitlement management (Public Preview)

Type: New feature

Service category: Other

Product capability: Entitlement Management

We've introduced a new two-stage approval workflow that allows you to require two approvers to approve a user's request to an access package. For example, you can set it so the requesting user's manager must first approve, and then you can also require a resource owner to approve. If one of the approvers doesn't approve, access isn't granted.

For more information, see [Change request and approval settings for an access package in Azure AD entitlement management](#).

Updates to the My Apps page along with new workspaces (Public Preview)

Type: New feature

Service category: My Apps

Product capability: 3rd Party Integration

You can now customize the way your organization's users view and access the refreshed My Apps experience. This new experience also includes the new workspaces feature, which makes it easier for your users to find and organize apps.

For more information about the new My Apps experience and creating workspaces, see [Create workspaces on the My Apps portal](#).

Google social ID support for Azure AD B2B collaboration (General Availability)

Type: New feature

Service category: B2B

Product capability: User Authentication

New support for using Google social IDs (Gmail accounts) in Azure AD helps to make collaboration simpler for your users and partners. There's no longer a need for your partners to create and manage a new Microsoft-specific account. Microsoft Teams now fully supports Google users on all clients and across the common and tenant-related authentication endpoints.

For more information, see [Add Google as an identity provider for B2B guest users](#).

Microsoft Edge Mobile Support for Conditional Access and Single Sign-on (General Availability)

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Azure AD for Microsoft Edge on iOS and Android now supports Azure AD Single Sign-On and Conditional Access:

- **Microsoft Edge single sign-on (SSO):** Single sign-on is now available across native clients (such as Microsoft Outlook and Microsoft Edge) for all Azure AD -connected apps.
- **Microsoft Edge conditional access:** Through application-based conditional access policies, your users must use Microsoft Intune-protected browsers, such as Microsoft Edge.

For more information about conditional access and SSO with Microsoft Edge, see the [Microsoft Edge Mobile Support for Conditional Access and Single Sign-on Now Generally Available](#) blog post. For more information about how to set up your client apps using [app-based conditional access](#) or [device-based conditional access](#), see

Manage web access using a Microsoft Intune policy-protected browser.

Azure AD entitlement management (General Availability)

Type: New feature

Service category: Other

Product capability: Entitlement Management

Azure AD entitlement management is a new identity governance feature, which helps organizations manage identity and access lifecycle at scale. This new feature helps by automating access request workflows, access assignments, reviews, and expiration across groups, apps, and SharePoint Online sites.

With Azure AD entitlement management, you can more efficiently manage access both for employees and also for users outside your organization who need access to those resources.

For more information, see [What is Azure AD entitlement management?](#)

Automate user account provisioning for these newly supported SaaS apps

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

[SAP Cloud Platform Identity Authentication Service](#), [RingCentral](#), [SpaceIQ](#), [Miro](#), [Cloudgate](#), [Infor CloudSuite](#), [OfficeSpace Software](#), [Priority Matrix](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New Federated Apps available in Azure AD App gallery - November 2019

Type: New feature

Service category: Enterprise Apps

Product capability: 3rd Party Integration

In November 2019, we've added these 21 new apps with Federation support to the app gallery:

[Airtable](#), [Hootsuite](#), [Blue Access for Members \(BAM\)](#), [Bitly](#), [Riva](#), [ResLife Portal](#), [NegometrixPortal Single Sign On \(SSO\)](#), [TeamsChamp](#), [Motus](#), [MyAryaka](#), [BlueMail](#), [Beedle](#), [Visma](#), [OneDesk](#), [Foko Retail](#), [Qmarkets Idea & Innovation Management](#), [Netskope User Authentication](#), [uniFLOW Online](#), [Claromentis](#), [Jisc Student Voter Registration](#), [e4enable](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New and improved Azure AD application gallery

Type: Changed feature

Service category: Enterprise Apps

Product capability: SSO

We've updated the Azure AD application gallery to make it easier for you to find pre-integrated apps that support provisioning, OpenID Connect, and SAML on your Azure Active Directory tenant.

For more information, see [Add an application to your Azure Active Directory tenant](#).

Increased app role definition length limit from 120 to 240 characters

Type: Changed feature

Service category: Enterprise Apps

Product capability: SSO

We've heard from customers that the length limit for the app role definition value in some apps and services is too short at 120 characters. In response, we've increased the maximum length of the role value definition to 240 characters.

For more information about using application-specific role definitions, see [Add app roles in your application and receive them in the token](#).

October 2019

Deprecation of the identityRiskEvent API for Azure AD Identity Protection risk detections

Type: Plan for change Service category: Identity Protection Product capability: Identity Security & Protection

In response to developer feedback, Azure AD Premium P2 subscribers can now perform complex queries on Azure AD Identity Protection's risk detection data by using the new riskDetection API for Microsoft Graph. The existing [identityRiskEvent](#) API beta version will stop returning data around **January 10, 2020**. If your organization is using the identityRiskEvent API, you should transition to the new riskDetection API.

For more information about the new riskDetection API, see the [Risk detection API reference documentation](#).

Application Proxy support for the SameSite Attribute and Chrome 80

Type: Plan for change Service category: App Proxy Product capability: Access Control

A couple of weeks prior to the Chrome 80 browser release, we plan to update how Application Proxy cookies treat the **SameSite** attribute. With the release of Chrome 80, any cookie that doesn't specify the **SameSite** attribute will be treated as though it was set to `SameSite=Lax`.

To help avoid potentially negative impacts due to this change, we're updating Application Proxy access and session cookies by:

- Setting the default value for the **Use Secure Cookie** setting to **Yes**.
- Setting the default value for the **SameSite** attribute to **None**.

NOTE

Application Proxy access cookies have always been transmitted exclusively over secure channels. These changes only apply to session cookies.

For more information about the Application Proxy cookie settings, see [Cookie settings for accessing on-premises applications in Azure Active Directory](#).

App registrations (legacy) and app management in the Application Registration Portal ([apps.dev.microsoft.com](#)) is no longer available

Type: Plan for change Service category: N/A Product capability: Developer Experience

Users with Azure AD accounts can no longer register or manage applications using the Application Registration Portal ([apps.dev.microsoft.com](#)), or register and manage applications in the App registrations (legacy) experience in the Azure portal.

To learn more about the new App registrations experience, see the [App registrations in the Azure portal training guide](#).

Users are no longer required to re-register during migration from per-user multifactor authentication (MFA) to Conditional Access-based multifactor authentication (MFA)

Type: Fixed Service category: MFA Product capability: Identity Security & Protection

We've fixed a known issue whereby when users were required to re-register if they were disabled for per-user MultiFactor Authentication (MFA) and then enabled for multifactor authentication (MFA) through a Conditional Access policy.

To require users to re-register, you can select the **Required re-register multifactor authentication (MFA)** option from the user's authentication methods in the Azure AD portal.

New capabilities to transform and send claims in your SAML token

Type: New feature Service category: Enterprise Apps Product capability: SSO

We've added additional capabilities to help you to customize and send claims in your SAML token. These new capabilities include:

- Additional claims transformation functions, helping you to modify the value you send in the claim.
- Ability to apply multiple transformations to a single claim.
- Ability to specify the claim source, based on the user type and the group to which the user belongs.

For detailed information about these new capabilities, including how to use them, see [Customize claims issued in the SAML token for enterprise applications](#).

New My Sign-ins page for end users in Azure AD

Type: New feature Service category: Authentications (Logins) Product capability: Monitoring & Reporting

We've added a new **My Sign-ins** page (<https://mysignins.microsoft.com>) to let your organization's users view their recent sign-in history to check for any unusual activity. This new page allows your users to see:

- If anyone is attempting to guess their password.
- If an attacker successfully signed in to their account and from what location.
- What apps the attacker tried to access.

For more information, see the [Users can now check their sign-in history for unusual activity](#) blog.

Migration of Azure AD Domain Services (Azure AD DS) from classic to Azure Resource Manager virtual networks

Type: New feature Service category: Azure AD Domain Services Product capability: Azure AD Domain Services

To our customers who have been stuck on classic virtual networks -- we have great news for you! You can now perform a one-time migration from a classic virtual network to an existing Resource Manager virtual network. After moving to the Resource Manager virtual network, you'll be able to take advantage of the additional and upgraded features such as, fine-grained password policies, email notifications, and audit logs.

For more information, see [Preview - Migrate Azure AD Domain Services from the Classic virtual network model to Resource Manager](#).

Updates to the Azure AD B2C page contract layout

Type: New feature **Service category:** B2C - Consumer Identity Management **Product capability:** B2B/B2C

We've introduced some new changes to version 1.2.0 of the page contract for Azure AD B2C. In this updated version, you can now control the load order for your elements, which can also help to stop the flicker that happens when the style sheet (CSS) is loaded.

For a full list of the changes made to the page contract, see the [Version change log](#).

Update to the My Apps page along with new workspaces (Public preview)

Type: New feature **Service category:** My Apps **Product capability:** Access Control

You can now customize the way your organization's users view and access the brand-new My Apps experience, including using the new workspaces feature to make it easier for them to find apps. The new workspaces functionality acts as a filter for the apps your organization's users already have access to.

For more information on rolling out the new My Apps experience and creating workspaces, see [Create workspaces on the My Apps \(preview\) portal](#).

Support for the monthly active user-based billing model (General availability)

Type: New feature **Service category:** B2C - Consumer Identity Management **Product capability:** B2B/B2C

Azure AD B2C now supports monthly active users (MAU) billing. MAU billing is based on the number of unique users with authentication activity during a calendar month. Existing customers can switch to this new billing method at any time.

Starting on November 1, 2019, all new customers will automatically be billed using this method. This billing method benefits customers through cost benefits and the ability to plan ahead.

For more information, see [Upgrade to monthly active users billing model](#).

New Federated Apps available in Azure AD App gallery - October 2019

Type: New feature **Service category:** Enterprise Apps **Product capability:** 3rd Party Integration

In October 2019, we've added these 35 new apps with Federation support to the app gallery:

[In Case of Crisis – Mobile](#), [Juno Journey](#), [ExponentHR](#), [Tact](#), [OpusCapita Cash Management](#), [Salestimator](#), [Learnster](#), [Dynatrace](#), [HunchBuzz](#), [Freshworks](#), [eCornell](#), [ShipHazmat](#), [Netskope Cloud Security](#), [Contentful](#), [Bindtuning](#), [HireVue Coordinate – Europe](#), [HireVue Coordinate - US Only](#), [HireVue Coordinate - US](#), [WittyParrot Knowledge Box](#), [Cloudmore](#), [Visit.org](#), [Cambium Xirrus EasyPass Portal](#), [Paylocity](#), [Mail Luck!](#), [Teamie](#), [Velocity for Teams](#), [SIGNL4](#), [EAB Navigate IMPL](#), [ScreenMeet](#), [Omega Point](#), [Speaking Email for Intune \(iPhone\)](#), [Speaking Email for Office 365 Direct \(iPhone/Android\)](#), [ExactCare SSO](#), [iHealthHome Care Navigation System](#), [Qubie](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Consolidated Security menu item in the Azure AD portal

Type: Changed feature **Service category:** Identity Protection **Product capability:** Identity Security & Protection

You can now access all of the available Azure AD security features from the new **Security** menu item, and from the **Search** bar, in the Azure portal. Additionally, the new **Security** landing page, called **Security - Getting started**, will provide links to our public documentation, security guidance, and deployment guides.

The new **Security** menu includes:

- Conditional Access
- Identity Protection
- Security Center
- Identity Secure Score
- Authentication methods
- Multifactor authentication (MFA)
- Risk reports - Risky users, Risky sign-ins, Risk detections
- And more...

For more information, see [Security - Getting started](#).

Office 365 groups expiration policy enhanced with autorenewal

Type: Changed feature **Service category:** Group Management **Product capability:** Identity Lifecycle Management

The Office 365 groups expiration policy has been enhanced to automatically renew groups that are actively in use by its members. Groups will be autorenewed based on user activity across all the Office 365 apps, including Outlook, SharePoint, and Teams.

This enhancement helps to reduce your group expiration notifications and helps to make sure that active groups continue to be available. If you already have an active expiration policy for your Office 365 groups, you don't need to do anything to turn on this new functionality.

For more information, see [Configure the expiration policy for Office 365 groups](#).

Updated Azure AD Domain Services (Azure AD DS) creation experience

Type: Changed feature **Service category:** Azure AD Domain Services **Product capability:** Azure AD Domain Services

We've updated Azure AD Domain Services (Azure AD DS) to include a new and improved creation experience, helping you to create a managed domain in just three clicks! In addition, you can now upload and deploy Azure AD DS from a template.

For more information, see [Tutorial: Create and configure an Azure Active Directory Domain Services instance](#).

September 2019

Plan for change: Deprecation of the Power BI content packs

Type: Plan for change **Service category:** Reporting **Product capability:** Monitoring & Reporting

Starting on October 1, 2019, Power BI will begin to deprecate all content packs, including the Azure AD Power BI content pack. As an alternative to this content pack, you can use Azure AD Workbooks to gain insights into your Azure AD-related services. Additional workbooks are coming, including workbooks about Conditional Access policies in report-only mode, app consent-based insights, and more.

For more information about the workbooks, see [How to use Azure Monitor workbooks for Azure Active Directory reports](#). For more information about the deprecation of the content packs, see the [Announcing Power BI template apps general availability](#) blog post.

My Profile is renaming and integrating with the Microsoft Office account page

Type: Plan for change **Service category:** My Profile/Account **Product capability:** Collaboration

Starting in October, the My Profile experience will become My Account. As part of that change, everywhere that

currently says, **My Profile** will change to **My Account**. On top of the naming change and some design improvements, the updated experience will offer additional integration with the Microsoft Office account page. Specifically, you'll be able to access Office installations and subscriptions from the **Overview Account** page, along with Office-related contact preferences from the **Privacy** page.

For more information about the My Profile (preview) experience, see [My Profile \(preview\) portal overview](#).

Bulk manage groups and members using CSV files in the Azure AD portal (Public Preview)

Type: New feature Service category: Group Management Product capability: Collaboration

We're pleased to announce public preview availability of the bulk group management experiences in the Azure AD portal. You can now use a CSV file and the Azure AD portal to manage groups and member lists, including:

- Adding or removing members from a group.
- Downloading the list of groups from the directory.
- Downloading the list of group members for a specific group.

For more information, see [Bulk add members](#), [Bulk remove members](#), [Bulk download members list](#), and [Bulk download groups list](#).

Dynamic consent is now supported through a new admin consent endpoint

Type: New feature Service category: Authentications (Logins) Product capability: User Authentication

We've created a new admin consent endpoint to support dynamic consent, which is helpful for apps that want to use the dynamic consent model on the Microsoft Identity platform.

For more information about how to use this new endpoint, see [Using the admin consent endpoint](#).

New Federated Apps available in Azure AD App gallery - September 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In September 2019, we've added these 29 new apps with Federation support to the app gallery:

ScheduleLook, MS Azure SSO Access for Ethidex Compliance Office™ - Single sign-on, iServer Portal, SKYSITE, Concur Travel and Expense, WorkBoard, <https://apps.yeeflow.com/>, ARC Facilities, Luware Stratus Team, Wide Ideas, Prisma Cloud, JDLT Client Hub, RENRAKU, SealPath Secure Browser, Prisma Cloud, <https://app.penneo.com/>, <https://app.testhtm.com/settings/email-integration>, Cintoo Cloud, Whitesource, Hosted Heritage Online SSO, IDC, CakeHR, BIS, Coo Kai Team Build, Sonarqube, Adobe Identity Management, Discovery Benefits SSO, Amelio, <https://itask.yipinapp.com/>

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New Azure AD Global Reader role

Type: New feature Service category: Azure AD roles Product capability: Access Control

Starting on September 24, 2019, we're going to start rolling out a new Azure Active Directory (AD) role called Global Reader. This rollout will start with production and Global cloud customers (GCC), finishing up worldwide in October.

The Global Reader role is the read-only counterpart to Global Administrator. Users in this role can read settings and administrative information across Microsoft 365 services, but can't take management actions. We've created the Global Reader role to help reduce the number of Global Administrators in your organization.

Because Global Administrator accounts are powerful and vulnerable to attack, we recommend that you have fewer than five Global Administrators. We recommend using the Global Reader role for planning, audits, or investigations. We also recommend using the Global Reader role in combination with other limited administrator roles, like Exchange Administrator, to help get work done without requiring the Global Administrator role.

The Global Reader role works with the new Microsoft 365 Admin Center, Exchange Admin Center, Teams Admin Center, Security Center, Compliance Center, Azure AD Admin Center, and the Device Management Admin Center.

NOTE

At the start of public preview, the Global Reader role won't work with: SharePoint, Privileged Access Management, Customer Lockbox, sensitivity labels, Teams Lifecycle, Teams Reporting & Call Analytics, Teams IP Phone Device Management, and Teams App Catalog.

For more information, see [Administrator role permissions in Azure Active Directory](#).

Access an on-premises Report Server from your Power BI Mobile app using Azure Active Directory Application Proxy

Type: New feature **Service category:** App Proxy **Product capability:** Access Control

New integration between the Power BI mobile app and Azure AD Application Proxy allows you to securely sign in to the Power BI mobile app and view any of your organization's reports hosted on the on-premises Power BI Report Server.

For information about the Power BI Mobile app, including where to download the app, see the [Power BI site](#). For more information about how to set up the Power BI mobile app with Azure AD Application Proxy, see [Enable remote access to Power BI Mobile with Azure AD Application Proxy](#).

New version of the AzureADPreview PowerShell module is available

Type: Changed feature **Service category:** Other **Product capability:** Directory

New cmdlets were added to the AzureADPreview module, to help define and assign custom roles in Azure AD, including:

- `Add-AzureADMSFeatureRolloutPolicyDirectoryObject`
- `Get-AzureADMSFeatureRolloutPolicy`
- `New-AzureADMSFeatureRolloutPolicy`
- `Remove-AzureADMSFeatureRolloutPolicy`
- `Remove-AzureADMSFeatureRolloutPolicyDirectoryObject`
- `Set-AzureADMSFeatureRolloutPolicy`

New version of Azure AD Connect

Type: Changed feature **Service category:** Other **Product capability:** Directory

We've released an updated version of Azure AD Connect for auto-upgrade customers. This new version includes several new features, improvements, and bug fixes.

Azure Active Directory Multi-Factor Authentication (MFA) Server, version 8.0.2 is now available

Type: Fixed **Service category:** MFA **Product capability:** Identity Security & Protection

If you're an existing customer, who activated Azure AD Multi-Factor Authentication (MFA) Server prior to July 1, 2019, you can now download the latest version of Azure AD Multi-Factor Authentication (MFA) Server (version

8.0.2). In this new version, we:

- Fixed an issue so when Azure AD sync changes a user from Disabled to Enabled, an email is sent to the user.
- Fixed an issue so customers can successfully upgrade, while continuing to use the Tags functionality.
- Added the Kosovo (+383) country code.
- Added one-time bypass audit logging to the MultiFactorAuthSvc.log.
- Improved performance for the Web Service SDK.
- Fixed other minor bugs.

Starting July 1, 2019, Microsoft stopped offering multifactor authentication (MFA) Server for new deployments. New customers who require multifactor authentication should use cloud-based Azure AD Multi-Factor Authentication. For more information, see [Planning a cloud-based Azure AD Multi-Factor Authentication deployment](#).

August 2019

Enhanced search, filtering, and sorting for groups is available in the Azure AD portal (Public Preview)

Type: New feature Service category: Group Management Product capability: Collaboration

We're pleased to announce public preview availability of the enhanced groups-related experiences in the Azure AD portal. These enhancements help you better manage groups and member lists, by providing:

- Advanced search capabilities, such as substring search on groups lists.
- Advanced filtering and sorting options on member and owner lists.
- New search capabilities for member and owner lists.
- More accurate group counts for large groups.

For more information, see [Manage groups in the Azure portal](#).

New custom roles are available for app registration management (Public Preview)

Type: New feature Service category: Azure AD roles Product capability: Access Control

Custom roles (available with an Azure AD P1 or P2 subscription) can now help provide you with fine-grained access, by letting you create role definitions with specific permissions and then to assign those roles to specific resources. Currently, you create custom roles by using permissions for managing app registrations and then assigning the role to a specific app. For more information about custom roles, see [Custom administrator roles in Azure Active Directory \(preview\)](#).

If you need additional permissions or resources supported, which you don't currently see, you can send feedback to our [Azure feedback site](#) and we'll add your request to our update road map.

New provisioning logs can help you monitor and troubleshoot your app provisioning deployment (Public Preview)

Type: New feature Service category: App Provisioning Product capability: Identity Lifecycle Management

New provisioning logs are available to help you monitor and troubleshoot the user and group provisioning deployment. These new log files include information about:

- What groups were successfully created in [ServiceNow](#)
- What roles were imported from [AWS Single-Account Access](#)

- What employees weren't imported from [Workday](#)

For more information, see [Provisioning reports in the Azure Active Directory portal \(preview\)](#).

New security reports for all Azure AD administrators (General Availability)

Type: New feature Service category: Identity Protection Product capability: Identity Security & Protection

By default, all Azure AD administrators will soon be able to access modern security reports within Azure AD.

Until the end of September, you will be able to use the banner at the top of the modern security reports to return to the old reports.

The modern security reports will provide additional capabilities from the older versions, including:

- Advanced filtering and sorting
- Bulk actions, such as dismissing user risk
- Confirmation of compromised or safe entities
- Risk state, covering: At risk, Dismissed, Remediated, and Confirmed compromised
- New risk-related detections (available to Azure AD Premium subscribers)

For more information, see [Risky users](#), [Risky sign-ins](#), and [Risk detections](#).

User-assigned managed identity is available for Virtual Machines and Virtual Machine Scale Sets (General Availability)

Type: New feature Service category: Managed identities for Azure resources Product capability: Developer Experience

User-assigned managed identities are now generally available for Virtual Machines and Virtual Machine Scale Sets. As part of this, Azure can create an identity in the Azure AD tenant that's trusted by the subscription in use, and can be assigned to one or more Azure service instances. For more information about user-assigned managed identities, see [What is managed identities for Azure resources?](#).

Users can reset their passwords using a mobile app or hardware token (General Availability)

Type: Changed feature Service category: Self Service Password Reset Product capability: User Authentication

Users who have registered a mobile app with your organization can now reset their own password by approving a notification from the Microsoft Authenticator app or by entering a code from their mobile app or hardware token.

For more information, see [How it works: Azure AD self-service password reset](#). For more information about the user experience, see [Reset your own work or school password overview](#).

ADAL.NET ignores the MSAL.NET shared cache for on-behalf-of scenarios

Type: Fixed Service category: Authentications (Logins) Product capability: User Authentication

Starting with Azure AD authentication library (ADAL.NET) version 5.0.0-preview, app developers must [serialize one cache per account for web apps and web APIs](#). Otherwise, some scenarios using the [on-behalf-of flow](#) for Java, along with some specific use cases of `UserAssertion`, may result in an elevation of privilege. To avoid this vulnerability, ADAL.NET now ignores the Microsoft Authentication Library for dotnet (MSAL.NET) shared cache for on-behalf-of scenarios.

For more information about this issue, see [Azure Active Directory Authentication Library Elevation of Privilege Vulnerability](#).

New Federated Apps available in Azure AD App gallery - August 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In August 2019, we've added these 26 new apps with Federation support to the app gallery:

Civic Platform, Amazon Business, ProNovos Ops Manager, Cognidox, Viareport's Inativ Portal (Europe), Azure Databricks, Robin, Academy Attendance, Priority Matrix, Cousto MySpace, Uploadcare, Carbonite Endpoint Backup, CPQSync by Cincom, Chargebee, deliver.media™ Portal, Frontline Education, F5, stashcat AD connect, Blink, Vocoli, ProNovos Analytics, Sigstr, Darwinbox, Watch by Colors, Harness, EAB Navigate Strategic Care

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New versions of the AzureAD PowerShell and AzureADPreview PowerShell modules are available

Type: Changed feature Service category: Other Product capability: Directory

New updates to the AzureAD and AzureAD Preview PowerShell modules are available:

- A new `-Filter` parameter was added to the `Get-AzureADDirectoryRole` parameter in the AzureAD module. This parameter helps you filter on the directory roles returned by the cmdlet.
- New cmdlets were added to the AzureADPreview module, to help define and assign custom roles in Azure AD, including:
 - `Get-AzureADMSRoleAssignment`
 - `Get-AzureADMSRoleDefinition`
 - `New-AzureADMSRoleAssignment`
 - `New-AzureADMSRoleDefinition`
 - `Remove-AzureADMSRoleAssignment`
 - `Remove-AzureADMSRoleDefinition`
 - `Set-AzureADMSRoleDefinition`

Improvements to the UI of the dynamic group rule builder in the Azure portal

Type: Changed feature Service category: Group Management Product capability: Collaboration

We've made some UI improvements to the dynamic group rule builder, available in the Azure portal, to help you more easily set up a new rule, or change existing rules. This design improvement allows you to create rules with up to five expressions, instead of just one. We've also updated the device property list to remove deprecated device properties.

For more information, see [Manage dynamic membership rules](#).

New Microsoft Graph app permission available for use with access reviews

Type: Changed feature Service category: Access Reviews Product capability: Identity Governance

We've introduced a new Microsoft Graph app permission, `AccessReview.ReadWrite.Membership`, which allows apps to automatically create and retrieve access reviews for group memberships and app assignments. This permission can be used by your scheduled jobs or as part of your automation, without requiring a logged-in user context.

For more information, see the [Example how to create Azure AD access reviews using Microsoft Graph app permissions with PowerShell blog](#).

Azure AD activity logs are now available for government cloud instances in Azure Monitor

Type: Changed feature Service category: Reporting Product capability: Monitoring & Reporting

We're excited to announce that Azure AD activity logs are now available for government cloud instances in Azure Monitor. You can now send Azure AD logs to your storage account or to an event hub to integrate with your SIEM tools, like [Sumologic](#), [Splunk](#), and [ArcSight](#).

For more information about setting up Azure Monitor, see [Azure AD activity logs in Azure Monitor](#).

Update your users to the new, enhanced security info experience

Type: Changed feature Service category: Authentications (Logins) Product capability: User Authentication

On September 25, 2019, we'll be turning off the old, non-enhanced security info experience for registering and managing user security info and only turning on the new, [enhanced version](#). This means that your users will no longer be able to use the old experience.

For more information about the enhanced security info experience, see our [admin documentation](#) and our [user documentation](#).

To turn on this new experience, you must:

1. Sign in to the Azure portal as a Global Administrator or User Administrator.
2. Go to **Azure Active Directory > User settings > Manage settings for access panel preview features**.
3. In the **Users can use preview features for registering and managing security info - enhanced** area, select **Selected**, and then either choose a group of users or choose **All** to turn on this feature for all users in the tenant.
4. In the **Users can use preview features for registering and managing security info** area, select **None**.
5. Save your settings.

After you save your settings, you'll no longer have access to the old security info experience.

IMPORTANT

If you don't complete these steps before September 25, 2019, your Azure Active Directory tenant will be automatically enabled for the enhanced experience. If you have questions, please contact us at registrationpreview@microsoft.com.

Authentication requests using POST logins will be more strictly validated

Type: Changed feature Service category: Authentications (Logins) Product capability: Standards

Starting on September 2, 2019, authentication requests using the POST method will be more strictly validated against the HTTP standards. Specifically, spaces and double-quotes ("") will no longer be removed from request form values. These changes aren't expected to break any existing clients, and will help to make sure that requests sent to Azure AD are reliably handled every time.

For more information, see the [Azure AD breaking changes notices](#).

July 2019

Plan for change: Application Proxy service update to support only TLS 1.2

Type: Plan for change Service category: App Proxy Product capability: Access Control

To help provide you with our strongest encryption, we're going to begin limiting Application Proxy service access to only TLS 1.2 protocols. This limitation will initially be rolled out to customers who are already using TLS 1.2 protocols, so you won't see the impact. Complete deprecation of the TLS 1.0 and TLS 1.1 protocols will be complete on August 31, 2019. Customers still using TLS 1.0 and TLS 1.1 will receive advanced notice to prepare for this change.

To maintain the connection to the Application Proxy service throughout this change, we recommend that you make sure your client-server and browser-server combinations are updated to use TLS 1.2. We also recommend that you make sure to include any client systems used by your employees to access apps published through the Application Proxy service.

For more information, see [Add an on-premises application for remote access through Application Proxy in Azure Active Directory](#).

Plan for change: Design updates are coming for the Application Gallery

Type: Plan for change Service category: Enterprise Apps Product capability: SSO

New user interface changes are coming to the design of the **Add from the gallery** area of the **Add an application** blade. These changes will help you more easily find your apps that support automatic provisioning, OpenID Connect, Security Assertion Markup Language (SAML), and Password single sign-on (SSO).

Plan for change: Removal of the multifactor authentication (MFA) server IP address from the Office 365 IP address

Type: Plan for change Service category: MFA Product capability: Identity Security & Protection

We're removing the multifactor authentication (MFA) server IP address from the [Office 365 IP Address and URL Web service](#). If you currently rely on these pages to update your firewall settings, you must make sure you're also including the list of IP addresses documented in the [Azure Active Directory Multi-Factor Authentication Server firewall requirements](#) section of the [Getting started with the Azure Active Directory Multi-Factor Authentication Server](#) article.

App-only tokens now require the client app to exist in the resource tenant

Type: Fixed Service category: Authentications (Logins) Product capability: User Authentication

On July 26, 2019, we changed how we provide app-only tokens through the [client credentials grant](#). Previously, apps could get tokens to call other apps, regardless of whether the client app was in the tenant. We've updated this behavior so single-tenant resources, sometimes called Web APIs, can only be called by client apps that exist in the resource tenant.

If your app isn't located in the resource tenant, you'll get an error message that says,

The service principal named <app_name> was not found in the tenant named <tenant_name>. This can happen if the application has not been installed by the administrator of the tenant.

To fix this problem, you must create the client app service principal in the tenant, using either the [admin consent endpoint](#) or [through PowerShell](#), which ensures your tenant has given the app permission to operate within the tenant.

For more information, see [What's new for authentication?](#).

NOTE

Existing consent between the client and the API continues to not be required. Apps should still be doing their own authorization checks.

New passwordless sign-in to Azure AD using FIDO2 security keys

Type: New feature **Service category:** Authentications (Logins) **Product capability:** User Authentication

Azure AD customers can now set policies to manage FIDO2 security keys for their organization's users and groups. End users can also self-register their security keys, use the keys to sign in to their Microsoft accounts on web sites while on FIDO-capable devices, as well as sign-in to their Azure AD-joined Windows 10 devices.

For more information, see [Enable passwordless sign in for Azure AD \(preview\)](#) for administrator-related information, and [Set up security info to use a security key \(Preview\)](#) for end-user-related information.

New Federated Apps available in Azure AD App gallery - July 2019

Type: New feature **Service category:** Enterprise Apps **Product capability:** 3rd Party Integration

In July 2019, we've added these 18 new apps with Federation support to the app gallery:

[Ungerboeck Software](#), [Bright Pattern Omnichannel Contact Center](#), [Clever Nelly](#), [AcquireIO](#), [Looop](#), [productboard](#), [MS Azure SSO Access for Ethidex Compliance Office™](#), [Hype](#), [Abstract](#), [Ascentis](#), [Flipsnack](#), [Wandera](#), [TwineSocial](#), [Kallidus](#), [HyperAnna](#), [PharmID WasteWitness](#), [i2B Connect](#), [JFrog Artifactory](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Automate user account provisioning for these newly supported SaaS apps

Type: New feature **Service category:** Enterprise Apps **Product capability:** Monitoring & Reporting

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Dialpad](#)
- [Federated Directory](#)
- [Figma](#)
- [Leapsome](#)
- [Peakon](#)
- [Smartsheet](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#)

New Azure AD Domain Services service tag for Network Security Group

Type: New feature **Service category:** Azure AD Domain Services **Product capability:** Azure AD Domain Services

If you're tired of managing long lists of IP addresses and ranges, you can use the new `AzureActiveDirectoryDomainServices` network service tag in your Azure network security group to help secure inbound traffic to your Azure AD Domain Services virtual network subnet.

For more information about this new service tag, see [Network Security Groups for Azure AD Domain Services](#).

New Security Audits for Azure AD Domain Services (Public Preview)

Type: New feature **Service category:** Azure AD Domain Services **Product capability:** Azure AD Domain Services

We're pleased to announce the release of Azure AD Domain Service Security Auditing to public preview. Security

auditing helps provide you with critical insight into your authentication services by streaming security audit events to targeted resources, including Azure Storage, Azure Log Analytics workspaces, and Azure Event Hubs, using the Azure AD Domain Service portal.

For more information, see [Enable Security Audits for Azure AD Domain Services \(Preview\)](#).

New Authentication methods usage & insights (Public Preview)

Type: New feature **Service category:** Self Service Password Reset **Product capability:** Monitoring & Reporting

The new Authentication methods usage & insights reports can help you to understand how features like Azure AD Multi-Factor Authentication and self-service password reset are being registered and used in your organization, including the number of registered users for each feature, how often self-service password reset is used to reset passwords, and by which method the reset happens.

For more information, see [Authentication methods usage & insights \(preview\)](#).

New security reports are available for all Azure AD administrators (Public Preview)

Type: New feature **Service category:** Identity Protection **Product capability:** Identity Security & Protection

All Azure AD administrators can now select the banner at the top of existing security reports, such as the **Users flagged for risk** report, to start using the new security experience as shown in the **Risky users** and the **Risky sign-ins** reports. Over time, all of the security reports will move from the older versions to the new versions, with the new reports providing you the following additional capabilities:

- Advanced filtering and sorting
- Bulk actions, such as dismissing user risk
- Confirmation of compromised or safe entities
- Risk state, covering: At risk, Dismissed, Remediated, and Confirmed compromised

For more information, see [Risky users report](#) and [Risky sign-ins report](#).

New Security Audits for Azure AD Domain Services (Public Preview)

Type: New feature **Service category:** Azure AD Domain Services **Product capability:** Azure AD Domain Services

We're pleased to announce the release of Azure AD Domain Service Security Auditing to public preview. Security auditing helps provide you with critical insight into your authentication services by streaming security audit events to targeted resources, including Azure Storage, Azure Log Analytics workspaces, and Azure Event Hubs, using the Azure AD Domain Service portal.

For more information, see [Enable Security Audits for Azure AD Domain Services \(Preview\)](#).

New B2B direct federation using SAML/WS-Fed (Public Preview)

Type: New feature **Service category:** B2B **Product capability:** B2B/B2C

Direct federation helps to make it easier for you to work with partners whose IT-managed identity solution is not Azure AD, by working with identity systems that support the SAML or WS-Fed standards. After you set up a direct federation relationship with a partner, any new guest user you invite from that domain can collaborate with you using their existing organizational account, making the user experience for your guests more seamless.

For more information, see [Direct federation with AD FS and third-party providers for guest users \(preview\)](#).

Automate user account provisioning for these newly supported SaaS apps

Type: New feature Service category: Enterprise Apps Product capability: Monitoring & Reporting

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Dialpad](#)
- [Federated Directory](#)
- [Figma](#)
- [Leapsome](#)
- [Peakon](#)
- [Smartsheet](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

New check for duplicate group names in the Azure AD portal

Type: New feature Service category: Group Management Product capability: Collaboration

Now, when you create or update a group name from the Azure AD portal, we'll perform a check to see if you are duplicating an existing group name in your resource. If we determine that the name is already in use by another group, you'll be asked to modify your name.

For more information, see [Manage groups in the Azure AD portal](#).

Azure AD now supports static query parameters in reply (redirect) URIs

Type: New feature Service category: Authentications (Logins) Product capability: User Authentication

Azure AD apps can now register and use reply (redirect) URIs with static query parameters (for example, `https://contoso.com/oauth2?idp=microsoft`) for OAuth 2.0 requests. The static query parameter is subject to string matching for reply URLs, just like any other part of the reply URI. If there's no registered string that matches the URL-decoded redirect-uri, the request is rejected. If the reply URI is found, the entire string is used to redirect the user, including the static query parameter.

Dynamic reply URLs are still forbidden because they represent a security risk and can't be used to retain state information across an authentication request. For this purpose, use the `state` parameter.

Currently, the app registration screens of the Azure portal still block query parameters. However, you can manually edit the app manifest to add and test query parameters in your app. For more information, see [What's new for authentication?](#).

Activity logs (MS Graph APIs) for Azure AD are now available through PowerShell Cmdlets

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

We're excited to announce that Azure AD activity logs (Audit and Sign-ins reports) are now available through the Azure AD PowerShell module. Previously, you could create your own scripts using MS Graph API endpoints, and now we've extended that capability to PowerShell cmdlets.

For more information about how to use these cmdlets, see [Azure AD PowerShell cmdlets for reporting](#).

Updated filter controls for Audit and Sign-in logs in Azure AD

Type: Changed feature Service category: Reporting Product capability: Monitoring & Reporting

We've updated the Audit and Sign-in log reports so you can now apply various filters without having to add them as columns on the report screens. Additionally, you can now decide how many filters you want to show on the screen. These updates all work together to make your reports easier to read and more scoped to your needs.

For more information about these updates, see [Filter audit logs](#) and [Filter sign-in activities](#).

June 2019

New riskDetections API for Microsoft Graph (Public preview)

Type: New feature Service category: Identity Protection Product capability: Identity Security & Protection

We're pleased to announce the new riskDetections API for Microsoft Graph is now in public preview. You can use this new API to view a list of your organization's Identity Protection-related user and sign-in risk detections. You can also use this API to more efficiently query your risk detections, including details about the detection type, status, level, and more.

For more information, see the [Risk detection API reference documentation](#).

New Federated Apps available in Azure AD app gallery - June 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In June 2019, we've added these 22 new apps with Federation support to the app gallery:

[Azure AD SAML Toolkit](#), [Otsuka Shokai \(大塚商会\)](#), [ANAQUA](#), [Azure VPN Client](#), [Expenseln](#), [Helper Helper](#), [Costpoint](#), [GlobalOne](#), [Mercedes-Benz In-Car Office](#), [Skore](#), [Oracle Cloud Infrastructure Console](#), [CyberArk SAML Authentication](#), [Scrible Edu](#), [PandaDoc](#), [Perceptyx](#), [Proptimise OS](#), [Vtiger CRM \(SAML\)](#), Oracle Access Manager for Oracle Retail Merchandising, Oracle Access Manager for Oracle E-Business Suite, Oracle IDCS for E-Business Suite, Oracle IDCS for PeopleSoft, Oracle IDCS for JD Edwards

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Automate user account provisioning for these newly supported SaaS apps

Type: New feature Service category: Enterprise Apps Product capability: Monitoring & Reporting

You can now automate creating, updating, and deleting user accounts for these newly integrated apps:

- [Zoom](#)
- [Envoy](#)
- [Proxyclick](#)
- [4me](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#)

View the real-time progress of the Azure AD provisioning service

Type: Changed feature Service category: App Provisioning Product capability: Identity Lifecycle Management

We've updated the Azure AD provisioning experience to include a new progress bar that shows you how far you are in the user provisioning process. This updated experience also provides information about the number of users provisioned during the current cycle, as well as how many users have been provisioned to date.

For more information, see [Check the status of user provisioning](#).

Company branding now appears on sign out and error screens

Type: Changed feature Service category: Authentications (Logins) Product capability: User Authentication

We've updated Azure AD so that your company branding now appears on the sign out and error screens, as well as the sign-in page. You don't have to do anything to turn on this feature, Azure AD simply uses the assets you've already set up in the **Company branding** area of the Azure portal.

For more information about setting up your company branding, see [Add branding to your organization's Azure Active Directory pages](#).

Azure Active Directory Multi-Factor Authentication (MFA) Server is no longer available for new deployments

Type: Deprecated Service category: MFA Product capability: Identity Security & Protection

As of July 1, 2019, Microsoft will no longer offer multifactor authentication (MFA) Server for new deployments. New customers who want to require multifactor authentication in their organization must now use cloud-based Azure AD Multi-Factor Authentication. Customers who activated multifactor authentication (MFA) Server prior to July 1 won't see a change. You'll still be able to download the latest version, get future updates, and generate activation credentials.

For more information, see [Getting started with the Azure Active Directory Multi-Factor Authentication Server](#). For more information about cloud-based Azure AD Multi-Factor Authentication, see [Planning a cloud-based Azure AD Multi-Factor Authentication deployment](#).

May 2019

Service change: Future support for only TLS 1.2 protocols on the Application Proxy service

Type: Plan for change Service category: App Proxy Product capability: Access Control

To help provide best-in-class encryption for our customers, we're limiting access to only TLS 1.2 protocols on the Application Proxy service. This change is gradually being rolled out to customers who are already only using TLS 1.2 protocols, so you shouldn't see any changes.

Deprecation of TLS 1.0 and TLS 1.1 happens on August 31, 2019, but we'll provide additional advanced notice, so you'll have time to prepare for this change. To prepare for this change make sure your client-server and browser-server combinations, including any clients your users use to access apps published through Application Proxy, are updated to use the TLS 1.2 protocol to maintain the connection to the Application Proxy service. For more information, see [Add an on-premises application for remote access through Application Proxy in Azure Active Directory](#).

Use the usage and insights report to view your app-related sign-in data

Type: New feature Service category: Enterprise Apps Product capability: Monitoring & Reporting

You can now use the usage and insights report, located in the **Enterprise applications** area of the Azure portal, to get an application-centric view of your sign-in data, including info about:

- Top used apps for your organization
- Apps with the most failed sign-ins
- Top sign-in errors for each app

For more information about this feature, see [Usage and insights report in the Azure Active Directory portal](#)

Automate your user provisioning to cloud apps using Azure AD

Type: New feature Service category: Enterprise Apps Product capability: Monitoring & Reporting

Follow these new tutorials to use the Azure AD Provisioning Service to automate the creation, deletion, and updating of user accounts for the following cloud-based apps:

- [Comeet](#)
- [DynamicSignal](#)
- [KeeperSecurity](#)

You can also follow this new [Dropbox tutorial](#), which provides info about how to provision group objects.

For more information about how to better secure your organization through automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Identity secure score is now available in Azure AD (General availability)

Type: New feature Service category: N/A Product capability: Identity Security & Protection

You can now monitor and improve your identity security posture by using the identity secure score feature in Azure AD. The identity secure score feature uses a single dashboard to help you:

- Objectively measure your identity security posture, based on a score between 1 and 223.
- Plan for your identity security improvements
- Review the success of your security improvements

For more information about the identity security score feature, see [What is the identity secure score in Azure Active Directory?](#).

New App registrations experience is now available (General availability)

Type: New feature Service category: Authentications (Logins) Product capability: Developer Experience

The new [App registrations](#) experience is now in general availability. This new experience includes all the key features you're familiar with from the Azure portal and the Application Registration portal and improves upon them through:

- **Better app management.** Instead of seeing your apps across different portals, you can now see all your apps in one location.
- **Simplified app registration.** From the improved navigation experience to the revamped permission selection experience, it's now easier to register and manage your apps.
- **More detailed information.** You can find more details about your app, including quickstart guides and more.

For more information, see [Microsoft identity platform](#) and the [App registrations experience is now generally available!](#) blog announcement.

New capabilities available in the Risky Users API for Identity Protection

Type: New feature Service category: Identity Protection Product capability: Identity Security & Protection

We're pleased to announce that you can now use the Risky Users API to retrieve users' risk history, dismiss risky users, and to confirm users as compromised. This change helps you to more efficiently update the risk status of your users and understand their risk history.

For more information, see the [Risky Users API reference documentation](#).

New Federated Apps available in Azure AD app gallery - May 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In May 2019, we've added these 21 new apps with Federation support to the app gallery:

[Freedcamp](#), [Real Links](#), [Kianda](#), [Simple Sign](#), [Braze](#), [Displayr](#), [Templafy](#), [Marketo Sales Engage](#), [ACLP](#), [OutSystems](#), [Meta4 Global HR](#), [Quantum Workplace](#), [Cobalt](#), [webMethods API Cloud](#), [RedFlag](#), [Whatfix](#), [Control](#), [JOBHUB](#), [NEOGOV](#), [Foodee](#), [MyVR](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Improved groups creation and management experiences in the Azure AD portal

Type: New feature Service category: Group Management Product capability: Collaboration

We've made improvements to the groups-related experiences in the Azure AD portal. These improvements allow administrators to better manage groups lists, members lists, and to provide additional creation options.

Improvements include:

- Basic filtering by membership type and group type.
- Addition of new columns, such as Source and Email address.
- Ability to multi-select groups, members, and owner lists for easy deletion.
- Ability to choose an email address and add owners during group creation.

For more information, see [Create a basic group and add members using Azure Active Directory](#).

Configure a naming policy for Office 365 groups in Azure AD portal (General availability)

Type: Changed feature Service category: Group Management Product capability: Collaboration

Administrators can now configure a naming policy for Office 365 groups, using the Azure AD portal. This change helps to enforce consistent naming conventions for Office 365 groups created or edited by users in your organization.

You can configure naming policy for Office 365 groups in two different ways:

- Define prefixes or suffixes, which are automatically added to a group name.
- Upload a customized set of blocked words for your organization, which are not allowed in group names (for example, "CEO, Payroll, HR").

For more information, see [Enforce a Naming Policy for Office 365 groups](#).

Microsoft Graph API endpoints are now available for Azure AD activity logs (General availability)

Type: Changed feature Service category: Reporting Product capability: Monitoring & Reporting

We're happy to announce general availability of Microsoft Graph API endpoints support for Azure AD activity logs. With this release, you can now use Version 1.0 of both the Azure AD audit logs, as well as the sign-in logs APIs.

For more information, see [Azure AD audit log API overview](#).

Administrators can now use Conditional Access for the combined registration process (Public preview)

Type: New feature Service category: Conditional Access Product capability: Identity Security & Protection

Administrators can now create Conditional Access policies for use by the combined registration page. This includes applying policies to allow registration if:

- Users are on a trusted network.
- Users are a low sign-in risk.
- Users are on a managed device.
- Users agree to the organization's terms of use (TOU).

For more information about Conditional Access and password reset, you can see the [Conditional Access for the Azure AD combined MFA and password reset registration experience blog post](#). For more information about Conditional Access policies for the combined registration process, see [Conditional Access policies for combined registration](#). For more information about the Azure AD terms of use feature, see [Azure Active Directory terms of use feature](#).

April 2019

New Azure AD threat intelligence detection is now available as part of Azure AD Identity Protection

Type: New feature Service category: Azure AD Identity Protection Product capability: Identity Security & Protection

Azure AD threat intelligence detection is now available as part of the updated Azure AD Identity Protection feature. This new functionality helps to indicate unusual user activity for a specific user or activity that's consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

For more information about the refreshed version of Azure AD Identity Protection, see the [Four major Azure AD Identity Protection enhancements are now in public preview](#) blog and the [What is Azure Active Directory Identity Protection \(refreshed\)?](#) article. For more information about Azure AD threat intelligence detection, see the [Azure Active Directory Identity Protection risk detections](#) article.

Azure AD entitlement management is now available (Public preview)

Type: New feature Service category: Identity Governance Product capability: Identity Governance

Azure AD entitlement management, now in public preview, helps customers to delegate management of access packages, which defines how employees and business partners can request access, who must approve, and how long they have access. Access packages can manage membership in Azure AD and Office 365 groups, role assignments in enterprise applications, and role assignments for SharePoint Online sites. Read more about entitlement management at the [overview of Azure AD entitlement management](#). To learn more about the breadth of Azure AD Identity Governance features, including Privileged Identity Management, access reviews and terms of use, see [What is Azure AD Identity Governance?](#).

Configure a naming policy for Office 365 groups in Azure AD portal (Public preview)

Type: New feature Service category: Group Management Product capability: Collaboration

Administrators can now configure a naming policy for Office 365 groups, using the Azure AD portal. This change helps to enforce consistent naming conventions for Office 365 groups created or edited by users in your organization.

You can configure naming policy for Office 365 groups in two different ways:

- Define prefixes or suffixes, which are automatically added to a group name.

- Upload a customized set of blocked words for your organization, which are not allowed in group names (for example, "CEO, Payroll, HR").

For more information, see [Enforce a Naming Policy for Office 365 groups](#).

Azure AD Activity logs are now available in Azure Monitor (General availability)

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

To help address your feedback about visualizations with the Azure AD Activity logs, we're introducing a new Insights feature in Log Analytics. This feature helps you gain insights about your Azure AD resources by using our interactive templates, called Workbooks. These pre-built Workbooks can provide details for apps or users, and include:

- **Sign-ins.** Provides details for apps and users, including sign-in location, the in-use operating system or browser client and version, and the number of successful or failed sign-ins.
- **Legacy authentication and Conditional Access.** Provides details for apps and users using legacy authentication, including multifactor authentication usage triggered by Conditional Access policies, apps using Conditional Access policies, and so on.
- **Sign-in failure analysis.** Helps you to determine if your sign-in errors are occurring due to a user action, policy issues, or your infrastructure.
- **Custom reports.** You can create new, or edit existing Workbooks to help customize the Insights feature for your organization.

For more information, see [How to use Azure Monitor workbooks for Azure Active Directory reports](#).

New Federated Apps available in Azure AD app gallery - April 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In April 2019, we've added these 21 new apps with Federation support to the app gallery:

[SAP Fiori](#), [HRworks Single Sign-On](#), [Percolate](#), [MobiControl](#), [Citrix NetScaler](#), [Shibumi](#), [Benchling](#), [MileIQ](#), [PageDNA](#), [EduBrite LMS](#), [RStudio Connect](#), [AMMS](#), [Mitel Connect](#), [Alibaba Cloud \(Role-based SSO\)](#), [Certent](#), [Equity Management](#), [Sectigo Certificate Manager](#), [GreenOrbit](#), [Workgrid](#), [monday.com](#), [SurveyMonkey](#), [Enterprise](#), [Indigo](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New access reviews frequency option and multiple role selection

Type: New feature Service category: Access Reviews Product capability: Identity Governance

New updates in Azure AD access reviews allow you to:

- Change the frequency of your access reviews to **semi-annually**, in addition to the previously existing options of weekly, monthly, quarterly, and annually.
- Select multiple Azure AD and Azure resource roles when creating a single access review. In this situation, all roles are set up with the same settings and all reviewers are notified at the same time.

For more information about how to create an access review, see [Create an access review of groups or applications in Azure AD access reviews](#).

Azure AD Connect email alert system(s) are transitioning, sending new email sender information for some

customers

Type: Changed feature Service category: AD Sync Product capability: Platform

Azure AD Connect is in the process of transitioning our email alert system(s), potentially showing some customers a new email sender. To address this, you must add azure-noreply@microsoft.com to your organization's allowlist or you won't be able to continue receiving important alerts from your Office 365, Azure, or your Sync services.

UPN suffix changes are now successful between Federated domains in Azure AD Connect

Type: Fixed Service category: AD Sync Product capability: Platform

You can now successfully change a user's UPN suffix from one Federated domain to another Federated domain in Azure AD Connect. This fix means you should no longer experience the FederatedDomainChangeError error message during the synchronization cycle or receive a notification email stating, "Unable to update this object in Azure Active Directory, because the attribute [FederatedUser.UserPrincipalName], is not valid. Update the value in your local directory services".

Increased security using the app protection-based Conditional Access policy in Azure AD (Public preview)

Type: New feature Service category: Conditional Access Product capability: Identity Security & Protection

App protection-based Conditional Access is now available by using the **Require app protection** policy. This new policy helps to increase your organization's security by helping to prevent:

- Users gaining access to apps without a Microsoft Intune license.
- Users being unable to get a Microsoft Intune app protection policy.
- Users gaining access to apps without a configured Microsoft Intune app protection policy.

For more information, see [How to Require app protection policy for cloud app access with Conditional Access](#).

New support for Azure AD single sign-on and Conditional Access in Microsoft Edge (Public preview)

Type: New feature Service category: Conditional Access Product capability: Identity Security & Protection

We've enhanced our Azure AD support for Microsoft Edge, including providing new support for Azure AD single sign-on and Conditional Access. If you've previously used Microsoft Intune Managed Browser, you can now use Microsoft Edge instead.

For more information about setting up and managing your devices and apps using Conditional Access, see [Require managed devices for cloud app access with Conditional Access](#) and [Require approved client apps for cloud app access with Conditional Access](#). For more information about how to manage access using Microsoft Edge with Microsoft Intune policies, see [Manage Internet access using a Microsoft Intune policy-protected browser](#).

March 2019

Identity Experience Framework and custom policy support in Azure Active Directory B2C is now available (GA)

Type: New feature Service category: B2C - Consumer Identity Management Product capability: B2B/B2C

You can now create custom policies in Azure AD B2C, including the following tasks, which are supported at-scale and under our Azure SLA:

- Create and upload custom authentication user journeys by using custom policies.

- Describe user journeys step-by-step as exchanges between claims providers.
- Define conditional branching in user journeys.
- Transform and map claims for use in real-time decisions and communications.
- Use REST API-enabled services in your custom authentication user journeys. For example, with email providers, CRMs, and proprietary authorization systems.
- Federate with identity providers who are compliant with the OpenIDConnect protocol. For example, with multi-tenant Azure AD, social account providers, or two-factor verification providers.

For more information about creating custom policies, see [Developer notes for custom policies in Azure Active Directory B2C](#) and read [Alex Simon's blog post, including case studies](#).

New Federated Apps available in Azure AD app gallery - March 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In March 2019, we've added these 14 new apps with Federation support to the app gallery:

[ISEC7 Mobile Exchange Delegate](#), [MediusFlow](#), [ePlatform](#), [Fulcrum](#), [ExcellityGlobal](#), [Explanation-Based Auditing System](#), [Lean](#), [Powerschool Performance Matters](#), [Cinode](#), [Iris Intranet](#), [Empactis](#), [SmartDraw](#), [Confirmit Horizons](#), [TAS](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New Zscaler and Atlassian provisioning connectors in the Azure AD gallery - March 2019

Type: New feature Service category: App Provisioning Product capability: 3rd Party Integration

Automate creating, updating, and deleting user accounts for the following apps:

[Zscaler](#), [Zscaler Beta](#), [Zscaler One](#), [Zscaler Two](#), [Zscaler Three](#), [Zscaler ZSCloud](#), [Atlassian Cloud](#)

For more information about how to better secure your organization through automated user account provisioning, see [Automate user provisioning to SaaS applications with Azure AD](#).

Restore and manage your deleted Office 365 groups in the Azure AD portal

Type: New feature Service category: Group Management Product capability: Collaboration

You can now view and manage your deleted Office 365 groups from the Azure AD portal. This change helps you to see which groups are available to restore, along with letting you permanently delete any groups that aren't needed by your organization.

For more information, see [Restore expired or deleted groups](#).

Single sign-on is now available for Azure AD SAML-secured on-premises apps through Application Proxy (public preview)

Type: New feature Service category: App Proxy Product capability: Access Control

You can now provide a single sign-on (SSO) experience for on-premises, SAML-authenticated apps, along with remote access to these apps through Application Proxy. For more information about how to set up SAML SSO with your on-premises apps, see [SAML single sign-on for on-premises applications with Application Proxy \(Preview\)](#).

Client apps in request loops will be interrupted to improve reliability and user experience

Type: New feature Service category: Authentications (Logins) Product capability: User Authentication

Client apps can incorrectly issue hundreds of the same login requests over a short period of time. These requests, whether they're successful or not, all contribute to a poor user experience and heightened workloads for the IDP, increasing latency for all users and reducing the availability of the IDP.

This update sends an `invalid_grant` error:

`AADSTS50196: The server terminated an operation because it encountered a loop while processing a request` to client apps that issue duplicate requests multiple times over a short period of time, beyond the scope of normal operation. Client apps that encounter this issue should show an interactive prompt, requiring the user to sign in again. For more information about this change and about how to fix your app if it encounters this error, see [What's new for authentication?](#).

New Audit Logs user experience now available

Type: Changed feature Service category: Reporting Product capability: Monitoring & Reporting

We've created a new Azure AD Audit logs page to help improve both readability and how you search for your information. To see the new Audit logs page, select **Audit logs** in the **Activity** section of Azure AD.

The screenshot shows the 'Audit logs' page in the Azure Active Directory portal. The left sidebar includes sections for Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Notifications settings, Security (with sub-options like Security overview (Preview), Identity Secure Score (Preview), Conditional Access, and MFA), and Monitoring (with sub-options like Sign-ins and Audit logs). The 'Audit logs' option under Monitoring is highlighted. The main area displays a table of audit log entries with columns: DATE, SERVICE, CATEGORY, ACTIVITY, and STATUS. The table lists various events from March 2019, such as Core Directory Policy updates, RoleManagement, and UserManagement activities, all marked as Success.

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS
3/25/2019, 2:52:29 PM	Core Directory	Policy	Update policy	Success
3/25/2019, 12:56:09 PM	Core Directory	RoleManagement	Add member to role	Failure
3/25/2019, 12:56:03 PM	Access Reviews	UserManagement	Create access review	Success
3/24/2019, 2:52:28 PM	Core Directory	Policy	Update policy	Success
3/24/2019, 10:49:15 AM	Access Reviews	UserManagement	Access review ended	Success
3/23/2019, 2:52:32 PM	Core Directory	Policy	Update policy	Success
3/22/2019, 2:52:32 PM	Core Directory	Policy	Update policy	Success
3/22/2019, 2:52:31 PM	Core Directory	Policy	Update policy	Success
3/21/2019, 2:52:31 PM	Core Directory	Policy	Update policy	Success
3/21/2019, 12:56:38 PM	Access Reviews	UserManagement	Apply access review	Success
3/21/2019, 12:56:35 PM	Access Reviews	UserManagement	Apply access review	Success

For more information about the new Audit logs page, see [Audit activity reports in the Azure Active Directory portal](#).

New warnings and guidance to help prevent accidental administrator lockout from misconfigured Conditional Access policies

Type: Changed feature Service category: Conditional Access Product capability: Identity Security & Protection

To help prevent administrators from accidentally locking themselves out of their own tenants through misconfigured Conditional Access policies, we've created new warnings and updated guidance in the Azure portal. For more information about the new guidance, see [What are service dependencies in Azure Active Directory Conditional Access](#).

Improved end-user terms of use experiences on mobile devices

Type: Changed feature **Service category:** Terms of use **Product capability:** Governance

We've updated our existing terms of use experiences to help improve how you review and consent to terms of use on a mobile device. You can now zoom in and out, go back, download the information, and select hyperlinks. For more information about the updated terms of use, see [Azure Active Directory terms of use feature](#).

New Azure AD Activity logs download experience available

Type: Changed feature **Service category:** Reporting **Product capability:** Monitoring & Reporting

You can now download large amounts of activity logs directly from the Azure portal. This update lets you:

- Download up to 250,000 rows.
- Get notified after the download completes.
- Customize your file name.
- Determine your output format, either JSON or CSV.

For more information about this feature, see [Quickstart: Download an audit report using the Azure portal](#)

Breaking change: Updates to condition evaluation by Exchange ActiveSync (EAS)

Type: Plan for change **Service category:** Conditional Access **Product capability:** Access Control

We're in the process of updating how Exchange ActiveSync (EAS) evaluates the following conditions:

- User location, based on country, region, or IP address
- Sign-in risk
- Device platform

If you've previously used these conditions in your Conditional Access policies, be aware that the condition behavior might change. For example, if you previously used the user location condition in a policy, you might find the policy now being skipped based on the location of your user.

February 2019

Configurable Azure AD SAML token encryption (Public preview)

Type: New feature **Service category:** Enterprise Apps **Product capability:** SSO

You can now configure any supported SAML app to receive encrypted SAML tokens. When configured and used with an app, Azure AD encrypts the emitted SAML assertions using a public key obtained from a certificate stored in Azure AD.

For more information about configuring your SAML token encryption, see [Configure Azure AD SAML token encryption](#).

Create an access review for groups or apps using Azure AD Access Reviews

Type: New feature **Service category:** Access Reviews **Product capability:** Governance

You can now include multiple groups or apps in a single Azure AD access review for group membership or app assignment. Access reviews with multiple groups or apps are set up using the same settings and all included reviewers are notified at the same time.

For more information about how create an access review using Azure AD Access Reviews, see [Create an access review of groups or applications in Azure AD Access Reviews](#)

New Federated Apps available in Azure AD app gallery - February 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In February 2019, we've added these 27 new apps with Federation support to the app gallery:

[Euromonitor Passport](#), [MindTickle](#), [FAT FINGER](#), [AirStack](#), [Oracle Fusion ERP](#), [IDrive](#), [Skyward Qmlativ](#), [Brightidea](#), [AlertOps](#), [Soloinsight-CloudGate SSO](#), [Permission Click](#), [Brandfolder](#), [StoregateSmartFile](#), [Pexip](#), [Stormboard](#), [Seismic](#), [Share A Dream](#), [Bugsnag](#), [webMethods Integration Cloud](#), [Knowledge Anywhere LMS](#), [OU Campus](#), [Periscope Data](#), [Netop Portal](#), [smartvid.io](#), [PureCloud by Genesys](#), [ClickUp Productivity Platform](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Enhanced combined multi-factor authentication (MFA)/SSPR registration

Type: Changed feature Service category: Self Service Password Reset Product capability: User Authentication

In response to customer feedback, we've enhanced the combined multifactor authentication (MFA)/SSPR registration preview experience, helping your users to more quickly register their security info for both multifactor authentication (MFA) and SSPR.

To turn on the enhanced experience for your users' today, follow these steps:

1. As a global administrator or user administrator, sign in to the Azure portal and go to [Azure Active Directory](#) > [User settings](#) > [Manage settings for access panel preview features](#).
2. In the **Users who can use the preview features for registering and managing security info – refresh** option, choose to turn on the features for a **Selected group of users** or for **All users**.

Over the next few weeks, we'll be removing the ability to turn on the old combined multifactor authentication (MFA)/SSPR registration preview experience for tenants that don't already have it turned on.

To see if the control will be removed for your tenant, follow these steps:

1. As a global administrator or user administrator, sign in to the Azure portal and go to [Azure Active Directory](#) > [User settings](#) > [Manage settings for access panel preview features](#).
2. If the **Users who can use the preview features for registering and managing security info** option is set to **None**, the option will be removed from your tenant.

Regardless of whether you previously turned on the old combined multifactor authentication (MFA)/SSPR registration preview experience for users or not, the old experience will be turned off at a future date. Because of that, we strongly suggest that you move to the new, enhanced experience as soon as possible.

For more information about the enhanced registration experience, see the [Cool enhancements to the Azure AD combined MFA and password reset registration experience](#).

Updated policy management experience for user flows

Type: Changed feature Service category: B2C - Consumer Identity Management Product capability: B2B/B2C

We've updated the policy creation and management process for user flows (previously known as, built-in policies) easier. This new experience is now the default for all of your Azure AD tenants.

You can provide additional feedback and suggestions by using the smile or frown icons in the **Send us feedback** area at the top of the portal screen.

For more information about the new policy management experience, see the [Azure AD B2C now has JavaScript customization and many more new features](#) blog.

Choose specific page element versions provided by Azure AD B2C

Type: New feature **Service category:** B2C - Consumer Identity Management **Product capability:** B2B/B2C

You can now choose a specific version of the page elements provided by Azure AD B2C. By selecting a specific version, you can test your updates before they appear on a page and you can get predictable behavior.

Additionally, you can now opt in to enforce specific page versions to allow JavaScript customizations. To turn on this feature, go to the **Properties** page in your user flows.

For more information about choosing specific versions of page elements, see the [Azure AD B2C now has JavaScript customization and many more new features](#) blog.

Configurable end-user password requirements for B2C (GA)

Type: New feature **Service category:** B2C - Consumer Identity Management **Product capability:** B2B/B2C

You can now set up your organization's password complexity for your end users, instead of having to use your native Azure AD password policy. From the **Properties** blade of your user flows (previously known as your built-in policies), you can choose a password complexity of **Simple** or **Strong**, or you can create a **Custom** set of requirements.

For more information about password complexity requirement configuration, see [Configure complexity requirements for passwords in Azure Active Directory B2C](#).

New default templates for custom branded authentication experiences

Type: New feature **Service category:** B2C - Consumer Identity Management **Product capability:** B2B/B2C

You can use our new default templates, located on the **Page layouts** blade of your user flows (previously known as built-in policies), to create a custom branded authentication experience for your users.

For more information about using the templates, see [Azure AD B2C now has JavaScript customization and many more new features](#).

January 2019

Active Directory B2B collaboration using one-time passcode authentication (Public preview)

Type: New feature **Service category:** B2B **Product capability:** B2B/B2C

We've introduced one-time passcode authentication (OTP) for B2B guest users who can't be authenticated through other means like Azure AD, a Microsoft account (MSA), or Google federation. This new authentication method means that guest users don't have to create a new Microsoft account. Instead, while redeeming an invitation or accessing a shared resource, a guest user can request a temporary code to be sent to an email address. Using this temporary code, the guest user can continue to sign in.

For more information, see [Email one-time passcode authentication \(preview\)](#) and the blog, [Azure AD makes sharing and collaboration seamless for any user with any account](#).

New Azure AD Application Proxy cookie settings

Type: New feature **Service category:** App Proxy **Product capability:** Access Control

We've introduced three new cookie settings, available for your apps that are published through Application Proxy:

- **Use HTTP-Only cookie.** Sets the **HTTPOnly** flag on your Application Proxy access and session cookies.

Turning on this setting provides additional security benefits, such as helping to prevent copying or modifying of cookies through client-side scripting. We recommend you turn on this flag (choose Yes) for the added benefits.

- **Use secure cookie.** Sets the **Secure** flag on your Application Proxy access and session cookies. Turning on this setting provides additional security benefits, by making sure cookies are only transmitted over TLS secure channels, such as HTTPS. We recommend you turn on this flag (choose Yes) for the added benefits.
- **Use persistent cookie.** Prevents access cookies from expiring when the web browser is closed. These cookies last for the lifetime of the access token. However, the cookies are reset if the expiration time is reached or if the user manually deletes the cookie. We recommend you keep the default setting **No**, only turning on the setting for older apps that don't share cookies between processes.

For more information about the new cookies, see [Cookie settings for accessing on-premises applications in Azure Active Directory](#).

New Federated Apps available in Azure AD app gallery - January 2019

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In January 2019, we've added these 35 new apps with Federation support to the app gallery:

Firstbird, Folloze, Talent Palette, Infor CloudSuite, Cisco Umbrella, Zscaler Internet Access Administrator, Expiration Reminder, InstaVR Viewer, CorpTax, Verb, OpenLattice, TheOrgWiki, Pavaso Digital Close, GoodPractice Toolkit, Cloud Service PICCO, AuditBoard, iProva, Workable, CallPlease, GTNexus SSO System, CBRE ServiceInsight, Deskradar, Coralogixv, Signagelive, ARES for Enterprise, K2 for Office 365, Xledger, iDiD Manager, HighGear, Visitly, Korn Ferry ALP, Acadia, Adoddle cSaas Platform

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New Azure AD Identity Protection enhancements (Public preview)

Type: Changed feature Service category: Identity Protection Product capability: Identity Security & Protection

We're excited to announce that we've added the following enhancements to the Azure AD Identity Protection public preview offering, including:

- An updated and more integrated user interface
- Additional APIs
- Improved risk assessment through machine learning
- Product-wide alignment across risky users and risky sign-ins

For more information about the enhancements, see [What is Azure Active Directory Identity Protection \(refreshed\)?](#) to learn more and to share your thoughts through the in-product prompts.

New App Lock feature for the Microsoft Authenticator app on iOS and Android devices

Type: New feature Service category: Microsoft Authenticator App Product capability: Identity Security & Protection

To keep your one-time passcodes, app information, and app settings more secure, you can turn on the App Lock feature in the Microsoft Authenticator app. Turning on App Lock means you'll be asked to authenticate using

your PIN or biometric every time you open the Microsoft Authenticator app.

For more information, see the [Microsoft Authenticator app FAQ](#).

Enhanced Azure AD Privileged Identity Management (PIM) export capabilities

Type: New feature **Service category:** Privileged Identity Management **Product capability:** Privileged Identity Management

Privileged Identity Management (PIM) administrators can now export all active and eligible role assignments for a specific resource, which includes role assignments for all child resources. Previously, it was difficult for administrators to get a complete list of role assignments for a subscription and they had to export role assignments for each specific resource.

For more information, see [View activity and audit history for Azure resource roles in PIM](#).

November/December 2018

Users removed from synchronization scope no longer switch to cloud-only accounts

Type: Fixed **Service category:** User Management **Product capability:** Directory

IMPORTANT

We've heard and understand your frustration because of this fix. Therefore, we've reverted this change until such time that we can make the fix easier for you to implement in your organization.

We've fixed a bug in which the DirSyncEnabled flag of a user would be erroneously switched to **False** when the Active Directory Domain Services (AD DS) object was excluded from synchronization scope and then moved to the Recycle Bin in Azure AD on the following sync cycle. As a result of this fix, if the user is excluded from sync scope and afterwards restored from Azure AD Recycle Bin, the user account remains as synchronized from on-premises AD, as expected, and cannot be managed in the cloud since its source of authority (SoA) remains as on-premises AD.

Prior to this fix, there was an issue when the DirSyncEnabled flag was switched to False. It gave the wrong impression that these accounts were converted to cloud-only objects and that the accounts could be managed in the cloud. However, the accounts still retained their SoA as on-premises and all synchronized properties (shadow attributes) coming from on-premises AD. This condition caused multiple issues in Azure AD and other cloud workloads (like Exchange Online) that expected to treat these accounts as synchronized from AD but were now behaving like cloud-only accounts.

At this time, the only way to truly convert a synchronized-from-AD account to cloud-only account is by disabling DirSync at the tenant level, which triggers a backend operation to transfer the SoA. This type of SoA change requires (but is not limited to) cleaning all the on-premises related attributes (such as LastDirSyncTime and shadow attributes) and sending a signal to other cloud workloads to have its respective object converted to a cloud-only account too.

This fix consequently prevents direct updates on the ImmutableID attribute of a user synchronized from AD, which in some scenarios in the past were required. By design, the ImmutableID of an object in Azure AD, as the name implies, is meant to be immutable. New features implemented in Azure AD Connect Health and Azure AD Connect Synchronization client are available to address such scenarios:

- **Large-scale ImmutableID update for many users in a staged approach**

For example, you need to do a lengthy AD DS inter-forest migration. Solution: Use Azure AD Connect to **Configure Source Anchor** and, as the user migrates, copy the existing ImmutableID values from Azure

AD into the local AD DS user's ms-DS-Consistency-Guid attribute of the new forest. For more information, see [Using ms-DS-ConsistencyGuid as sourceAnchor](#).

- **Large-scale ImmutableID updates for many users in one shot**

For example, while implementing Azure AD Connect you make a mistake, and now you need to change the SourceAnchor attribute. Solution: Disable DirSync at the tenant level and clear all the invalid ImmutableID values. For more information, see [Turn off directory synchronization for Office 365](#).

- **Rematch on-premises user with an existing user in Azure AD** For example, a user that has been re-created in AD DS generates a duplicate in Azure AD account instead of rematching it with an existing Azure AD account (orphaned object). Solution: Use Azure AD Connect Health in the Azure portal to remap the Source Anchor/ImmutableID. For more information, see [Orphaned object scenario](#).

Breaking Change: Updates to the audit and sign-in logs schema through Azure Monitor

Type: Changed feature Service category: Reporting Product capability: Monitoring & Reporting

We're currently publishing both the Audit and Sign-in log streams through Azure Monitor, so you can seamlessly integrate the log files with your SIEM tools or with Log Analytics. Based on your feedback, and in preparation for this feature's general availability announcement, we're making the following changes to our schema. These schema changes and its related documentation updates will happen by the first week of January.

New fields in the Audit schema

We're adding a new **Operation Type** field, to provide the type of operation performed on the resource. For example, **Add**, **Update**, or **Delete**.

Changed fields in the Audit schema

The following fields are changing in the Audit schema:

FIELD NAME	WHAT CHANGED	OLD VALUES	NEW VALUES
Category	This was the Service Name field. It's now the Audit Categories field. Service Name has been renamed to the loggedByService field.	<ul style="list-style-type: none">• Account Provisioning• Core Directory• Self-service Password Reset	<ul style="list-style-type: none">• User Management• Group Management• App Management
targetResources	Includes TargetResourceType at the top level.		<ul style="list-style-type: none">• Policy• App• User• Group
loggedByService	Provides the name of the service that generated the audit log.	Null	<ul style="list-style-type: none">• Account Provisioning• Core Directory• Self-service password reset
Result	Provides the result of the audit logs. Previously, this was enumerated, but we now show the actual value.	<ul style="list-style-type: none">• 0• 1	<ul style="list-style-type: none">• Success• Failure

Changed fields in the Sign-in schema

The following fields are changing in the Sign-in schema:

Field Name	What changed	Old Values	New Values
appliedConditionalAccessPolicies	This was the conditionalaccessPolicies field. It's now the appliedConditionalAccessPolicies field.	No change	No change
conditionalAccessStatus	Provides the result of the Conditional Access Policy Status at sign-in. Previously, this was enumerated, but we now show the actual value.	<ul style="list-style-type: none"> • 0 • 1 • 2 • 3 	<ul style="list-style-type: none"> • Success • Failure • Not Applied • Disabled
appliedConditionalAccessPolicies: result	Provides the result of the individual Conditional Access Policy Status at sign-in. Previously, this was enumerated, but we now show the actual value.	<ul style="list-style-type: none"> • 0 • 1 • 2 • 3 	<ul style="list-style-type: none"> • Success • Failure • Not Applied • Disabled

For more information about the schema, see [Interpret the Azure AD audit logs schema in Azure Monitor \(preview\)](#)

Identity Protection improvements to the supervised machine learning model and the risk score engine

Type: Changed feature Service category: Identity Protection Product capability: Risk Scores

Improvements to the Identity Protection-related user and sign-in risk assessment engine can help to improve user risk accuracy and coverage. Administrators may notice that user risk level is no longer directly linked to the risk level of specific detections, and that there's an increase in the number and level of risky sign-in events.

Risk detections are now evaluated by the supervised machine learning model, which calculates user risk by using additional features of the user's sign-ins and a pattern of detections. Based on this model, the administrator might find users with high risk scores, even if detections associated with that user are of low or medium risk.

Administrators can reset their own password using the Microsoft Authenticator app (Public preview)

Type: Changed feature Service category: Self Service Password Reset Product capability: User Authentication

Azure AD administrators can now reset their own password using the Microsoft Authenticator app notifications or a code from any mobile authenticator app or hardware token. To reset their own password, administrators will now be able to use two of the following methods:

- Microsoft Authenticator app notification
- Other mobile authenticator app / Hardware token code
- Email
- Phone call
- Text message

For more information about using the Microsoft Authenticator app to reset passwords, see [Azure AD self-service password reset - Mobile app and SSPR \(Preview\)](#)

New Azure AD Cloud Device Administrator role (Public preview)

Type: New feature **Service category:** Device Registration and Management **Product capability:** Access control

Administrators can assign users to the new Cloud Device Administrator role to perform cloud device administrator tasks. Users assigned the Cloud Device Administrators role can enable, disable, and delete devices in Azure AD, along with being able to read Windows 10 BitLocker keys (if present) in the Azure portal.

For more information about roles and permissions, see [Assigning administrator roles in Azure Active Directory](#)

Manage your devices using the new activity timestamp in Azure AD (Public preview)

Type: New feature **Service category:** Device Registration and Management **Product capability:** Device Lifecycle Management

We realize that over time you must refresh and retire your organizations' devices in Azure AD, to avoid having stale devices in your environment. To help with this process, Azure AD now updates your devices with a new activity timestamp, helping you to manage your device lifecycle.

For more information about how to get and use this timestamp, see [How To: Manage the stale devices in Azure AD](#)

Administrators can require users to accept a terms of use on each device

Type: New feature **Service category:** Terms of use **Product capability:** Governance

Administrators can now turn on the **Require users to consent on every device** option to require your users to accept your terms of use on every device they're using on your tenant.

For more information, see the [Per-device terms of use section of the Azure Active Directory terms of use feature](#).

Administrators can configure a terms of use to expire based on a recurring schedule

Type: New feature **Service category:** Terms of use **Product capability:** Governance

Administrators can now turn on the **Expire consents** option to make a terms of use expire for all of your users based on your specified recurring schedule. The schedule can be annually, bi-annually, quarterly, or monthly. After the terms of use expire, users must reaccept.

For more information, see the [Add terms of use section of the Azure Active Directory terms of use feature](#).

Administrators can configure a terms of use to expire based on each user's schedule

Type: New feature **Service category:** Terms of use **Product capability:** Governance

Administrators can now specify a duration that user must reaccept a terms of use. For example, administrators can specify that users must reaccept a terms of use every 90 days.

For more information, see the [Add terms of use section of the Azure Active Directory terms of use feature](#).

New Azure AD Privileged Identity Management (PIM) emails for Azure Active Directory roles

Type: New feature **Service category:** Privileged Identity Management **Product capability:** Privileged Identity Management

Customers using Azure AD Privileged Identity Management (PIM) can now receive a weekly digest email, including the following information for the last seven days:

- Overview of the top eligible and permanent role assignments
- Number of users activating roles

- Number of users assigned to roles in PIM
- Number of users assigned to roles outside of PIM
- Number of users "made permanent" in PIM

For more information about PIM and the available email notifications, see [Email notifications in PIM](#).

Group-based licensing is now generally available

Type: Changed feature Service category: Other Product capability: Directory

Group-based licensing is out of public preview and is now generally available. As part of this general release, we've made this feature more scalable and have added the ability to reprocess group-based licensing assignments for a single user and the ability to use group-based licensing with Office 365 E3/A3 licenses.

For more information about group-based licensing, see [What is group-based licensing in Azure Active Directory?](#)

New Federated Apps available in Azure AD app gallery - November 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In November 2018, we've added these 26 new apps with Federation support to the app gallery:

CoreStack, HubSpot, GetThere, Gra-Pe, eHour, Consent2Go, Appinux, DriveDollar, Useall, Infinite Campus, Alaya, HeyBuddy, Wrike SAML, Drift, Zenegy for Business Central 365, Everbridge Member Portal, IDEO, Ivanti Service Manager (ISM), Peakon, Allbound SSO, Plex Apps - Classic Test, Plex Apps – Classic, Plex Apps - UX Test, Plex Apps – UX, Plex Apps – IAM, CRAFTS - Childcare Records, Attendance, & Financial Tracking System

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

October 2018

Azure AD Logs now work with Azure Log Analytics (Public preview)

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

We're excited to announce that you can now forward your Azure AD logs to Azure Log Analytics! This top-requested feature helps give you even better access to analytics for your business, operations, and security, as well as a way to help monitor your infrastructure. For more information, see the [Azure Active Directory Activity logs in Azure Log Analytics now available](#) blog.

New Federated Apps available in Azure AD app gallery - October 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In October 2018, we've added these 14 new apps with Federation support to the app gallery:

My Award Points, Vibe HCM, ambyint, MyWorkDrive, BorrowBox, Dialpad, ON24 Virtual Environment, RingCentral, Zscaler Three, Phraseanet, Appraisd, Workspot Control, Shuccho Navi, Glassfrog

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Azure AD Domain Services Email Notifications

Type: New feature **Service category:** Azure AD Domain Services **Product capability:** Azure AD Domain Services

Azure AD Domain Services provides alerts on the Azure portal about misconfigurations or problems with your managed domain. These alerts include step-by-step guides so you can try to fix the problems without having to contact support.

Starting in October, you'll be able to customize the notification settings for your managed domain so when new alerts occur, an email is sent to a designated group of people, eliminating the need to constantly check the portal for updates.

For more information, see [Notification settings in Azure AD Domain Services](#).

Azure AD portal supports using the ForceDelete domain API to delete custom domains

Type: Changed feature **Service category:** Directory Management **Product capability:** Directory

We're pleased to announce that you can now use the ForceDelete domain API to delete your custom domain names by asynchronously renaming references, like users, groups, and apps from your custom domain name (contoso.com) back to the initial default domain name (contoso.onmicrosoft.com).

This change helps you to more quickly delete your custom domain names if your organization no longer uses the name, or if you need to use the domain name with another Azure AD.

For more information, see [Delete a custom domain name](#).

September 2018

Updated administrator role permissions for dynamic groups

Type: Fixed **Service category:** Group Management **Product capability:** Collaboration

We've fixed an issue so specific administrator roles can now create and update dynamic membership rules, without needing to be the owner of the group.

The roles are:

- Global administrator
- Intune administrator
- User administrator

For more information, see [Create a dynamic group and check status](#)

Simplified Single Sign-On (SSO) configuration settings for some third-party apps

Type: New feature **Service category:** Enterprise Apps **Product capability:** SSO

We realize that setting up Single Sign-On (SSO) for Software as a Service (SaaS) apps can be challenging due to the unique nature of each apps configuration. We've built a simplified configuration experience to auto-populate the SSO configuration settings for the following third-party SaaS apps:

- Zendesk
- ArcGis Online
- Jamf Pro

To start using this one-click experience, go to the [Azure portal > SSO configuration](#) page for the app. For more information, see [SaaS application integration with Azure Active Directory](#)

Azure Active Directory - Where is your data located? page

Type: New feature Service category: Other Product capability: GoLocal

Select your company's region from the [Azure Active Directory - Where is your data located](#) page to view which Azure datacenter houses your Azure AD data at rest for all Azure AD services. You can filter the information by specific Azure AD services for your company's region.

To access this feature and for more information, see [Azure Active Directory - Where is your data located](#).

New deployment plan available for the My Apps Access panel

Type: New feature Service category: My Apps Product capability: SSO

Check out the new deployment plan that's available for the My Apps Access panel (<https://aka.ms/deploymentplans>). The My Apps Access panel provides users with a single place to find and access their apps. This portal also provides users with self-service opportunities, such as requesting access to apps and groups, or managing access to these resources on behalf of others.

For more information, see [What is the My Apps portal?](#)

New Troubleshooting and Support tab on the Sign-ins Logs page of the Azure portal

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

The new **Troubleshooting and Support** tab on the **Sign-ins** page of the Azure portal, is intended to help admins and support engineers troubleshoot issues related to Azure AD sign-ins. This new tab provides the error code, error message, and remediation recommendations (if any) to help solve the problem. If you're unable to resolve the problem, we also give you a new way to create a support ticket using the **Copy to clipboard** experience, which populates the **Request ID** and **Date (UTC)** fields for the log file in your support ticket.

The screenshot shows the 'Wingtip Toys - Sign-ins' page in the Azure portal. The left sidebar includes sections for Company branding, User settings, Properties, Notifications settings, Security (with Identity Secure Score), Conditional access, MFA Server, Users flagged for risk, Risky sign-ins, Authentication methods, Activity (Sign-ins selected), and Audit logs. The main area has a search bar and filter options for User, Application, Sign-in status, and Correlation Id. Below these are tabs for Sign-in info, Device info, MFA, Conditional Access, and Troubleshooting and support (which is highlighted with a red box). Under the Troubleshooting and support tab, there are sections for Sign-in status (Failure), Sign-in error code (65005), and Failure reason (describing a missing resource access list). To the right, there's a 'Create a new support request' section with steps 1-4, and fields for Request Id (d8ca2572-ec81-4a3b-b3fa-14d4568f0600) and Timestamp (2018-09-19T04:19:04.734Z).

Enhanced support for custom extension properties used to create dynamic membership rules

Type: Changed feature Service category: Group Management Product capability: Collaboration

With this update, you can now click the **Get custom extension properties** link from the dynamic user group rule builder, enter your unique app ID, and receive the full list of custom extension properties to use when creating a dynamic membership rule for users. This list can also be refreshed to get any new custom extension properties for that app.

For more information about using custom extension properties for dynamic membership rules, see [Extension properties and custom extension properties](#)

New approved client apps for Azure AD app-based Conditional Access

Type: Plan for change Service category: Conditional Access Product capability: Identity security and protection

The following apps are on the list of approved client apps:

- Microsoft To-Do
- Microsoft Stream

For more information, see:

- [Azure AD app-based Conditional Access](#)
-

New support for Self-Service Password Reset from the Windows 7/8/8.1 Lock screen

Type: New feature Service category: SSPR Product capability: User Authentication

After you set up this new feature, your users will see a link to reset their password from the **Lock** screen of a device running Windows 7, Windows 8, or Windows 8.1. By clicking that link, the user is guided through the same password reset flow as through the web browser.

For more information, see [How to enable password reset from Windows 7, 8, and 8.1](#)

Change notice: Authorization codes will no longer be available for reuse

Type: Plan for change Service category: Authentications (Logins) Product capability: User Authentication

Starting on November 15, 2018, Azure AD will stop accepting previously used authentication codes for apps. This security change helps to bring Azure AD in line with the OAuth specification and will be enforced on both the v1 and v2 endpoints.

If your app reuses authorization codes to get tokens for multiple resources, we recommend that you use the code to get a refresh token, and then use that refresh token to acquire additional tokens for other resources. Authorization codes can only be used once, but refresh tokens can be used multiple times across multiple resources. An app that attempts to reuse an authentication code during the OAuth code flow will get an `invalid_grant` error.

For this and other protocols-related changes, see [the full list of what's new for authentication](#).

New Federated Apps available in Azure AD app gallery - September 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In September 2018, we've added these 16 new apps with Federation support to the app gallery:

[Uberflip](#), [Comeet Recruiting Software](#), [Workteam](#), [ArcGIS Enterprise](#), [Nucleo](#), [JDA Cloud](#), [Snowflake](#), [NavigoCloud](#), [Figma](#), [join.me](#), [ZephyrSSO](#), [Silverback](#), [Riverbed Xirrus EasyPass](#), [Rackspace SSO](#), [Enlyft SSO for Azure](#), [SurveyMonkey](#), [Convene](#), [dmarcian](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Support for additional claims transformations methods

Type: New feature Service category: Enterprise Apps Product capability: SSO

We've introduced new claim transformation methods, `ToLower()` and `ToUpper()`, which can be applied to SAML tokens from the SAML-based [Single Sign-On Configuration](#) page.

For more information, see [How to customize claims issued in the SAML token for enterprise applications in Azure AD](#)

Updated SAML-based app configuration UI (preview)

Type: Changed feature Service category: Enterprise Apps Product capability: SSO

As part of our updated SAML-based app configuration UI, you'll get:

- An updated walkthrough experience for configuring your SAML-based apps.
- More visibility about what's missing or incorrect in your configuration.
- The ability to add multiple email addresses for expiration certificate notification.
- New claim transformation methods, ToLower() and ToUpper(), and more.
- A way to upload your own token signing certificate for your enterprise apps.
- A way to set the NameID Format for SAML apps, and a way to set the NameID value as Directory Extensions.

To turn on this updated view, click the [Try out our new experience](#) link from the top of the Single Sign-On page. For more information, see [Tutorial: Configure SAML-based single sign-on for an application with Azure Active Directory](#).

August 2018

Changes to Azure Active Directory IP address ranges

Type: Plan for change Service category: Other Product capability: Platform

We're introducing larger IP ranges to Azure AD, which means if you've configured Azure AD IP address ranges for your firewalls, routers, or Network Security Groups, you'll need to update them. We're making this update so you won't have to change your firewall, router, or Network Security Groups IP range configurations again when Azure AD adds new endpoints.

Network traffic is moving to these new ranges over the next two months. To continue with uninterrupted service, you must add these updated values to your IP Addresses before September 10, 2018:

- 20.190.128.0/18
- 40.126.0.0/18

We strongly recommend not removing the old IP Address ranges until all of your network traffic has moved to the new ranges. For updates about the move and to learn when you can remove the old ranges, see [Office 365 URLs and IP address ranges](#).

Change notice: Authorization codes will no longer be available for reuse

Type: Plan for change Service category: Authentications (Logins) Product capability: User Authentication

Starting on November 15, 2018, Azure AD will stop accepting previously used authentication codes for apps. This security change helps to bring Azure AD in line with the OAuth specification and will be enforced on both the v1 and v2 endpoints.

If your app reuses authorization codes to get tokens for multiple resources, we recommend that you use the code to get a refresh token, and then use that refresh token to acquire additional tokens for other resources. Authorization codes can only be used once, but refresh tokens can be used multiple times across multiple resources. An app that attempts to reuse an authentication code during the OAuth code flow will get an

invalid_grant error.

For this and other protocols-related changes, see [the full list of what's new for authentication](#).

Converged security info management for self-service password (SSPR) and multifactor authentication (MFA)

Type: New feature Service category: SSPR Product capability: User Authentication

This new feature helps people manage their security info (such as, phone number, mobile app, and so on) for SSPR and multifactor authentication (MFA) in a single location and experience; as compared to previously, where it was done in two different locations.

This converged experience also works for people using either SSPR or multifactor authentication (MFA). Additionally, if your organization doesn't enforce multifactor authentication (MFA) or SSPR registration, people can still register any multifactor authentication (MFA) or SSPR security info methods allowed by your organization from the My Apps portal.

This is an opt-in public preview. Administrators can turn on the new experience (if desired) for a selected group or for all users in a tenant. For more information about the converged experience, see the [Converged experience blog](#)

New HTTP-Only cookies setting in Azure AD Application proxy apps

Type: New feature Service category: App Proxy Product capability: Access Control

There's a new setting called, **HTTP-Only Cookies** in your Application Proxy apps. This setting helps provide extra security by including the **HTTPOnly** flag in the HTTP response header for both Application Proxy access and session cookies, stopping access to the cookie from a client-side script and further preventing actions like copying or modifying the cookie. Although this flag hasn't been used previously, your cookies have always been encrypted and transmitted using a TLS connection to help protect against improper modifications.

This setting isn't compatible with apps using ActiveX controls, such as Remote Desktop. If you're in this situation, we recommend that you turn off this setting.

For more information about the HTTP-Only Cookies setting, see [Publish applications using Azure AD Application Proxy](#).

Privileged Identity Management (PIM) for Azure resources supports Management Group resource types

Type: New feature Service category: Privileged Identity Management Product capability: Privileged Identity Management

Just-In-Time activation and assignment settings can now be applied to Management Group resource types, just like you already do for Subscriptions, Resource Groups, and Resources (such as VMs, App Services, and more). In addition, anyone with a role that provides administrator access for a Management Group can discover and manage that resource in PIM.

For more information about PIM and Azure resources, see [Discover and manage Azure resources by using Privileged Identity Management](#)

Application access (preview) provides faster access to the Azure AD portal

Type: New feature Service category: Privileged Identity Management Product capability: Privileged Identity Management

Today, when activating a role using PIM, it can take over 10 minutes for the permissions to take effect. If you choose to use Application access, which is currently in public preview, administrators can access the Azure AD portal as soon as the activation request completes.

Currently, Application access only supports the Azure AD portal experience and Azure resources. For more information about PIM and Application access, see [What is Azure AD Privileged Identity Management?](#)

New Federated Apps available in Azure AD app gallery - August 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In August 2018, we've added these 16 new apps with Federation support to the app gallery:

[Hornbill](#), [Bridgeline Unbound](#), [Sauce Labs - Mobile and Web Testing](#), [Meta Networks Connector](#), [Way We Do](#), [Spotinst](#), [ProMaster \(by Inlogik\)](#), [SchoolBooking](#), [4me](#), [Dossier](#), [N2F - Expense reports](#), [Comm100 Live Chat](#), [SafeConnect](#), [ZenQMS](#), [eLuminate](#), [Dovetale](#).

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Native Tableau support is now available in Azure AD Application Proxy

Type: Changed feature Service category: App Proxy Product capability: Access Control

With our update from the OpenID Connect to the OAuth 2.0 Code Grant protocol for our pre-authentication protocol, you no longer have to do any additional configuration to use Tableau with Application Proxy. This protocol change also helps Application Proxy better support more modern apps by using only HTTP redirects, which are commonly supported in JavaScript and HTML tags.

New support to add Google as an identity provider for B2B guest users in Azure Active Directory (preview)

Type: New feature Service category: B2B Product capability: B2B/B2C

By setting up federation with Google in your organization, you can let invited Gmail users sign in to your shared apps and resources using their existing Google account, without having to create a personal Microsoft Account (MSAs) or an Azure AD account.

This is an opt-in public preview. For more information about Google federation, see [Add Google as an identity provider for B2B guest users](#).

July 2018

Improvements to Azure Active Directory email notifications

Type: Changed feature Service category: Other Product capability: Identity lifecycle management

Azure Active Directory (Azure AD) emails now feature an updated design, as well as changes to the sender email address and sender display name, when sent from the following services:

- Azure AD Access Reviews
- Azure AD Connect Health
- Azure AD Identity Protection
- Azure AD Privileged Identity Management
- Enterprise App Expiring Certificate Notifications
- Enterprise App Provisioning Service Notifications

The email notifications will be sent from the following email address and display name:

- Email address: azure-noreply@microsoft.com
- Display name: Microsoft Azure

For an example of some of the new e-mail designs and more information, see [Email notifications in Azure AD PIM](#).

Azure AD Activity Logs are now available through Azure Monitor

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

The Azure AD Activity Logs are now available in public preview for the Azure Monitor (Azure's platform-wide monitoring service). Azure Monitor offers you long-term retention and seamless integration, in addition to these improvements:

- Long-term retention by routing your log files to your own Azure storage account.
- Seamless SIEM integration, without requiring you to write or maintain custom scripts.
- Seamless integration with your own custom solutions, analytics tools, or incident management solutions.

For more information about these new capabilities, see our blog [Azure AD activity logs in Azure Monitor diagnostics is now in public preview](#) and our documentation, [Azure Active Directory activity logs in Azure Monitor \(preview\)](#).

Conditional Access information added to the Azure AD sign-ins report

Type: New feature Service category: Reporting Product capability: Identity Security & Protection

This update lets you see which policies are evaluated when a user signs in along with the policy outcome. In addition, the report now includes the type of client app used by the user, so you can identify legacy protocol traffic. Report entries can also now be searched for a correlation ID, which can be found in the user-facing error message and can be used to identify and troubleshoot the matching sign-in request.

View legacy authentications through Sign-ins activity logs

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

With the introduction of the **Client App** field in the Sign-in activity logs, customers can now see users that are using legacy authentications. Customers will be able to access this information using the Sign-ins Microsoft Graph API or through the Sign-in activity logs in Azure AD portal where you can use the **Client App** control to filter on legacy authentications. Check out the documentation for more details.

New Federated Apps available in Azure AD app gallery - July 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In July 2018, we've added these 16 new apps with Federation support to the app gallery:

[Innovation Hub](#), [Leapsome](#), [Certain Admin SSO](#), PSUC Staging, [iPass SmartConnect](#), [Screencast-O-Matic](#), PowerSchool Unified Classroom, [Eli Onboarding](#), [Bomgar Remote Support](#), [Nimblex](#), [Imagineer WebVision](#), [Insight4GRC](#), [SecureW2 JoinNow Connector](#), [Kanbanize](#), [SmartLPA](#), [Skills Base](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New user provisioning SaaS app integrations - July 2018

Type: New feature Service category: App Provisioning Product capability: 3rd Party Integration

Azure AD allows you to automate the creation, maintenance, and removal of user identities in SaaS applications such as Dropbox, Salesforce, ServiceNow, and more. For July 2018, we have added user provisioning support for the following applications in the Azure AD app gallery:

- [Cisco WebEx](#)
- [Bonusly](#)

For a list of all applications that support user provisioning in the Azure AD gallery, see [SaaS application integration with Azure Active Directory](#).

Connect Health for Sync - An easier way to fix orphaned and duplicate attribute sync errors

Type: New feature Service category: AD Connect Product capability: Monitoring & Reporting

Azure AD Connect Health introduces self-service remediation to help you highlight and fix sync errors. This feature troubleshoots duplicated attribute sync errors and fixes objects that are orphaned from Azure AD. This diagnosis has the following benefits:

- Narrows down duplicated attribute sync errors, providing specific fixes
- Applies a fix for dedicated Azure AD scenarios, resolving errors in a single step
- No upgrade or configuration is required to turn on and use this feature

For more information, see [Diagnose and remediate duplicated attribute sync errors](#)

Visual updates to the Azure AD and MSA sign-in experiences

Type: Changed feature Service category: Azure AD Product capability: User Authentication

We've updated the UI for Microsoft's online services sign-in experience, such as for Office 365 and Azure. This change makes the screens less cluttered and more straightforward. For more information about this change, see the [Upcoming improvements to the Azure AD sign-in experience](#) blog.

New release of Azure AD Connect - July 2018

Type: Changed feature Service category: App Provisioning Product capability: Identity Lifecycle Management

The latest release of Azure AD Connect includes:

- Bug fixes and supportability updates
- General Availability of the Ping-Federate integration
- Updates to the latest SQL 2012 client

For more information about this update, see [Azure AD Connect: Version release history](#)

Updates to the terms of use end-user UI

Type: Changed feature Service category: Terms of use Product capability: Governance

We're updating the acceptance string in the TOU end-user UI.

Current text. In order to access [tenantName] resources, you must accept the terms of use.

New text. In order to access [tenantName] resource, you must read the terms of use.

Current text: Choosing to accept means that you agree to all of the above terms of use.

New text: Please click Accept to confirm that you have read and understood the terms of use.

Pass-through Authentication supports legacy protocols and applications

Type: Changed feature Service category: Authentications (Logins) Product capability: User Authentication

Pass-through Authentication now supports legacy protocols and apps. The following limitations are now fully supported:

- User sign-ins to legacy Office client applications, Office 2010 and Office 2013, without requiring modern authentication.
 - Access to calendar sharing and free/busy information in Exchange hybrid environments on Office 2010 only.
 - User sign-ins to Skype for Business client applications without requiring modern authentication.
 - User sign-ins to PowerShell version 1.0.
 - The Apple Device Enrollment Program (Apple DEP), using the iOS Setup Assistant.
-

Converged security info management for self-service password reset and MultiFactor Authentication

Type: New feature Service category: SSPR Product capability: User Authentication

This new feature lets users manage their security info (for example, phone number, email address, mobile app, and so on) for self-service password reset (SSPR) and multifactor authentication (MFA) in a single experience. Users will no longer have to register the same security info for SSPR and multifactor authentication (MFA) in two different experiences. This new experience also applies to users who have either SSPR or multifactor authentication (MFA).

If an organization isn't enforcing multifactor authentication (MFA) or SSPR registration, users can register their security info through the **My Apps** portal. From there, users can register any methods enabled for multifactor authentication (MFA) or SSPR.

This is an opt-in public preview. Admins can turn on the new experience (if desired) for a selected group of users or all users in a tenant.

Use the Microsoft Authenticator app to verify your identity when you reset your password

Type: Changed feature Service category: SSPR Product capability: User Authentication

This feature lets non-admins verify their identity while resetting a password using a notification or code from Microsoft Authenticator (or any other authenticator app). After admins turn on this self-service password reset method, users who have registered a mobile app through aka.ms/mfasetup or aka.ms/setupsecurityinfo can use their mobile app as a verification method while resetting their password.

Mobile app notification can only be turned on as part of a policy that requires two methods to reset your password.

June 2018

Change notice: Security fix to the delegated authorization flow for apps using Azure AD Activity Logs API

Type: Plan for change Service category: Reporting Product capability: Monitoring & Reporting

Due to our stronger security enforcement, we've had to make a change to the permissions for apps that use a delegated authorization flow to access [Azure AD Activity Logs APIs](#). This change will occur by **June 26, 2018**.

If any of your apps use Azure AD Activity Log APIs, follow these steps to ensure the app doesn't break after the change happens.

To update your app permissions

1. Sign in to the Azure portal, select **Azure Active Directory**, and then select **App Registrations**.

2. Select your app that uses the Azure AD Activity Logs API, select **Settings**, select **Required permissions**, and then select the **Windows Azure Active Directory API**.
3. In the **Delegated permissions** area of the **Enable access** blade, select the box next to **Read directory data**, and then select **Save**.
4. Select **Grant permissions**, and then select **Yes**.

NOTE

You must be a Global administrator to grant permissions to the app.

For more information, see the [Grant permissions](#) area of the Prerequisites to access the Azure AD reporting API article.

Configure TLS settings to connect to Azure AD services for PCI DSS compliance

Type: New feature Service category: N/A Product capability: Platform

Transport Layer Security (TLS) is a protocol that provides privacy and data integrity between two communicating applications and is the most widely deployed security protocol used today.

The [PCI Security Standards Council](#) has determined that early versions of TLS and Secure Sockets Layer (SSL) must be disabled in favor of enabling new and more secure app protocols, with compliance starting on **June 30, 2018**. This change means that if you connect to Azure AD services and require PCI DSS-compliance, you must disable TLS 1.0. Multiple versions of TLS are available, but TLS 1.2 is the latest version available for Azure Active Directory Services. We highly recommend moving directly to TLS 1.2 for both client/server and browser/server combinations.

Out-of-date browsers might not support newer TLS versions, such as TLS 1.2. To see which versions of TLS are supported by your browser, go to the [Qualys SSL Labs](#) site and click **Test your browser**. We recommend you upgrade to the latest version of your web browser and preferably enable only TLS 1.2.

To enable TLS 1.2, by browser

- **Microsoft Edge and Internet Explorer (both are set using Internet Explorer)**
 1. Open Internet Explorer, select **Tools > Internet Options > Advanced**.
 2. In the **Security** area, select **use TLS 1.2**, and then select **OK**.
 3. Close all browser windows and restart Internet Explorer.
- **Google Chrome**
 1. Open Google Chrome, type *chrome://settings/* into the address bar, and press **Enter**.
 2. Expand the **Advanced** options, go to the **System** area, and select **Open proxy settings**.
 3. In the **Internet Properties** box, select the **Advanced** tab, go to the **Security** area, select **use TLS 1.2**, and then select **OK**.
 4. Close all browser windows and restart Google Chrome.
- **Mozilla Firefox**
 1. Open Firefox, type *about:config* into the address bar, and then press **Enter**.
 2. Search for the term, *TLS*, and then select the **security.tls.version.max** entry.
 3. Set the value to 3 to force the browser to use up to version TLS 1.2, and then select **OK**.

NOTE

Firefox version 60.0 supports TLS 1.3, so you can also set the security.tls.version.max value to 4.

4. Close all browser windows and restart Mozilla Firefox.

New Federated Apps available in Azure AD app gallery - June 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In June 2018, we've added these 15 new apps with Federation support to the app gallery:

[Skytap](#), [Settling music](#), [SAML 1.1 Token enabled LOB App](#), [Supermood](#), [Autotask](#), [Endpoint Backup](#), [Skyhigh Networks](#), [Smartway2](#), [TonicDM](#), [Moconavi](#), [Zoho One](#), [SharePoint on-premises](#), [ForeSee CX Suite](#), [Vidyard](#), [ChronicX](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#). For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Azure AD Password Protection is available in public preview

Type: New feature Service category: Identity Protection Product capability: User Authentication

Use Azure AD Password Protection to help eliminate easily guessed passwords from your environment. Eliminating these passwords helps to lower the risk of compromise from a password spray type of attack.

Specifically, Azure AD Password Protection helps you:

- Protect your organization's accounts in both Azure AD and Windows Server Active Directory (AD).
- Stops your users from using passwords on a list of more than 500 of the most commonly used passwords, and over 1 million character substitution variations of those passwords.
- Administer Azure AD Password Protection from a single location in the Azure AD portal, for both Azure AD and on-premises Windows Server AD.

For more information about Azure AD Password Protection, see [Eliminate bad passwords in your organization](#).

New "all guests" Conditional Access policy template created during terms of use creation

Type: New feature Service category: Terms of use Product capability: Governance

During the creation of your terms of use, a new Conditional Access policy template is also created for "all guests" and "all apps". This new policy template applies the newly created ToU, streamlining the creation and enforcement process for guests.

For more information, see [Azure Active Directory Terms of use feature](#).

New "custom" Conditional Access policy template created during terms of use creation

Type: New feature Service category: Terms of use Product capability: Governance

During the creation of your terms of use, a new "custom" Conditional Access policy template is also created. This new policy template lets you create the ToU and then immediately go to the Conditional Access policy creation blade, without needing to manually navigate through the portal.

For more information, see [Azure Active Directory Terms of use feature](#).

New and comprehensive guidance about deploying Azure AD Multi-Factor Authentication

Type: New feature Service category: Other Product capability: Identity Security & Protection

We've released new step-by-step guidance about how to deploy Azure AD Multi-Factor Authentication (MFA) in your organization.

To view the Azure AD Multi-Factor Authentication (MFA) deployment guide, go to the [Identity Deployment Guides](#) repo on GitHub. To provide feedback about the deployment guides, use the [Deployment Plan Feedback form](#). If you have any questions about the deployment guides, contact us at [IDGitDeploy](#).

Azure AD delegated app management roles are in public preview

Type: New feature Service category: Enterprise Apps Product capability: Access Control

Admins can now delegate app management tasks without assigning the Global Administrator role. The new roles and capabilities are:

- **New standard Azure AD admin roles:**
 - **Application Administrator.** Grants the ability to manage all aspects of all apps, including registration, SSO settings, app assignments and licensing, App proxy settings, and consent (except to Azure AD resources).
 - **Cloud Application Administrator.** Grants all of the Application Administrator abilities, except for App proxy because it doesn't provide on-premises access.
 - **Application Developer.** Grants the ability to create app registrations, even if the **allow users to register apps** option is turned off.
- **Ownership (set up per-app registration and per-enterprise app, similar to the group ownership process):**
 - **App Registration Owner.** Grants the ability to manage all aspects of owned app registration, including the app manifest and adding additional owners.
 - **Enterprise App Owner.** Grants the ability to manage many aspects of owned enterprise apps, including SSO settings, app assignments, and consent (except to Azure AD resources).

For more information about public preview, see the [Azure AD delegated application management roles are in public preview!](#) blog. For more information about roles and permissions, see [Assigning administrator roles in Azure Active Directory](#).

May 2018

ExpressRoute support changes

Type: Plan for change Service category: Authentications (Logins) Product capability: Platform

Software as a Service offering, like Azure Active Directory (Azure AD) are designed to work best by going directly through the Internet, without requiring ExpressRoute or any other private VPN tunnels. Because of this, on **August 1, 2018**, we will stop supporting ExpressRoute for Azure AD services using Azure public peering and Azure communities in Microsoft peering. Any services impacted by this change might notice Azure AD traffic gradually shifting from ExpressRoute to the Internet.

While we're changing our support, we also know there are still situations where you might need to use a dedicated set of circuits for your authentication traffic. Because of this, Azure AD will continue to support per-tenant IP range restrictions using ExpressRoute and services already on Microsoft peering with the "Other Office 365 Online services" community. If your services are impacted, but you require ExpressRoute, you must do the following:

- If you're on Azure public peering. Move to Microsoft peering and sign up for the [Other Office 365 Online services \(12076:5100\)](#) community. For more info about how to move from Azure public peering to Microsoft peering, see the [Move a public peering to Microsoft peering](#) article.
- If you're on Microsoft peering. Sign up for the [Other Office 365 Online service \(12076:5100\)](#) community. For more info about routing requirements, see the [Support for BGP communities section](#) of the ExpressRoute routing requirements article.

If you must continue to use dedicated circuits, you'll need to talk to your Microsoft Account team about how to get authorization to use the [Other Office 365 Online service \(12076:5100\)](#) community. The MS Office-managed review board will verify whether you need those circuits and make sure you understand the technical implications of keeping them. Unauthorized subscriptions trying to create route filters for Office 365 will receive an error message.

Microsoft Graph APIs for administrative scenarios for TOU

Type: New feature Service category: Terms of use Product capability: Developer Experience

We've added Microsoft Graph APIs for administration operation of Azure AD terms of use. You are able to create, update, delete the terms of use object.

Add Azure AD multi-tenant endpoint as an identity provider in Azure AD B2C

Type: New feature Service category: B2C - Consumer Identity Management Product capability: B2B/B2C

Using custom policies, you can now add the Azure AD common endpoint as an identity provider in Azure AD B2C. This allows you to have a single point of entry for all Azure AD users that are signing into your applications. For more information, see [Azure Active Directory B2C: Allow users to sign in to a multi-tenant Azure AD identity provider using custom policies](#).

Use Internal URLs to access apps from anywhere with our My Apps Sign-in Extension and the Azure AD Application Proxy

Type: New feature Service category: My Apps Product capability: SSO

Users can now access applications through internal URLs even when outside your corporate network by using the My Apps Secure Sign-in Extension for Azure AD. This will work with any application that you have published using Azure AD Application Proxy, on any browser that also has the Access Panel browser extension installed. The URL redirection functionality is automatically enabled once a user logs into the extension. The extension is available for download on [Microsoft Edge](#), [Chrome](#).

Azure Active Directory - Data in Europe for Europe customers

Type: New feature Service category: Other Product capability: GoLocal

Customers in Europe require their data to stay in Europe and not replicated outside of European datacenters for meeting privacy and European laws. This [article](#) provides the specific details on what identity information will be stored within Europe and also provide details on information that will be stored outside European datacenters.

New user provisioning SaaS app integrations - May 2018

Type: New feature Service category: App Provisioning Product capability: 3rd Party Integration

Azure AD allows you to automate the creation, maintenance, and removal of user identities in SaaS applications such as Dropbox, Salesforce, ServiceNow, and more. For May 2018, we have added user provisioning support for the following applications in the Azure AD app gallery:

- [BlueJeans](#)

- [Cornerstone OnDemand](#)
- [Zendesk](#)

For a list of all applications that support user provisioning in the Azure AD gallery, see <https://aka.ms/appstutorial>.

Azure AD access reviews of groups and app access now provides recurring reviews

Type: New feature Service category: Access Reviews Product capability: Governance

Access review of groups and apps is now generally available as part of Azure AD Premium P2. Administrators will be able to configure access reviews of group memberships and application assignments to automatically recur at regular intervals, such as monthly or quarterly.

Azure AD Activity logs (sign-ins and audit) are now available through MS Graph

Type: New feature Service category: Reporting Product capability: Monitoring & Reporting

Azure AD Activity logs, which, includes Sign-ins and Audit logs, are now available through the Microsoft Graph API. We have exposed two end points through the Microsoft Graph API to access these logs. Check out our [documents](#) for programmatic access to Azure AD Reporting APIs to get started.

Improvements to the B2B redemption experience and leave an org

Type: New feature Service category: B2B Product capability: B2B/B2C

Just in time redemption: Once you share a resource with a guest user using B2B API – you don't need to send out a special invitation email. In most cases, the guest user can access the resource and will be taken through the redemption experience just in time. No more impact due to missed emails. No more asking your guest users "Did you click on that redemption link the system sent you?". This means once SPO uses the invitation manager – cloudy attachments can have the same canonical URL for all users – internal and external – in any state of redemption.

Modern redemption experience: No more split screen redemption landing page. Users will see a modern consent experience with the inviting organization's privacy statement, just like they do for third-party apps.

Guest users can leave the org: Once a user's relationship with an org is over, they can self-serve leaving the organization. No more calling the inviting org's admin to "be removed", no more raising support tickets.

New Federated Apps available in Azure AD app gallery - May 2018

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In May 2018, we've added these 18 new apps with Federation support to our app gallery:

[AwardSpring](#), Infogix Data3Sixty Govern, [Yodeck](#), [Jamf Pro](#), [KnowledgeOwl](#), [Envi MMIS](#), [LaunchDarkly](#), [Adobe Captivate Prime](#), [Montage Online](#), [まなびポケット](#), [OpenReel](#), [Arc Publishing - SSO](#), [PlanGrid](#), [iWellnessNow](#), [Proxyclick](#), [Riskware](#), [Flock](#), [Reviewsnap](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#).

For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

New step-by-step deployment guides for Azure Active Directory

Type: New feature Service category: Other Product capability: Directory

New, step-by-step guidance about how to deploy Azure Active Directory (Azure AD), including self-service

password reset (SSPR), single sign-on (SSO), Conditional Access, App proxy, User provisioning, Active Directory Federation Services (ADFS) to Pass-through Authentication (PTA), and ADFS to Password hash sync (PHS).

To view the deployment guides, go to the [Identity Deployment Guides](#) repo on GitHub. To provide feedback about the deployment guides, use the [Deployment Plan Feedback form](#). If you have any questions about the deployment guides, contact us at [IDGitDeploy](#).

Enterprise Applications Search - Load More Apps

Type: New feature Service category: Enterprise Apps Product capability: SSO

Having trouble finding your applications / service principals? We've added the ability to load more applications in your enterprise applications all applications list. By default, we show 20 applications. You can now click, **Load more** to view additional applications.

The May release of AADConnect contains a public preview of the integration with PingFederate, important security updates, many bug fixes, and new great new troubleshooting tools.

Type: Changed feature Service category: AD Connect Product capability: Identity Lifecycle Management

The May release of AADConnect contains a public preview of the integration with PingFederate, important security updates, many bug fixes, and new great new troubleshooting tools. You can find the release notes [here](#).

Azure AD access reviews: auto-apply

Type: Changed feature Service category: Access Reviews Product capability: Governance

Access reviews of groups and apps are now generally available as part of Azure AD Premium P2. An administrator can configure to automatically apply the reviewer's changes to that group or app as the access review completes. The administrator can also specify what happens to the user's continued access if reviewers didn't respond, remove access, keep access, or take system recommendations.

ID tokens can no longer be returned using the query response_mode for new apps.

Type: Changed feature Service category: Authentications (Logins) Product capability: User Authentication

Apps created on or after April 25, 2018 will no longer be able to request an `id_token` using the `query response_mode`. This brings Azure AD inline with the OIDC specifications and helps reduce your apps attack surface. Apps created before April 25, 2018 are not blocked from using the `query response_mode` with a `response_type` of `id_token`. The error returned, when requesting an `id_token` from Azure AD, is **AADSTS70007: 'query' is not a supported value of 'response_mode' when requesting a token.**

The `fragment` and `form_post` `response_modes` continue to work - when creating new application objects (for example, for App Proxy usage), ensure use of one of these `response_modes` before they create a new application.

April 2018

Azure AD B2C Access Token are GA

Type: New feature Service category: B2C - Consumer Identity Management Product capability: B2B/B2C

You can now access Web APIs secured by Azure AD B2C using access tokens. The feature is moving from public preview to GA. The UI experience to configure Azure AD B2C applications and web APIs has been improved, and other minor improvements were made.

For more information, see [Azure AD B2C: Requesting access tokens](#).

Test single sign-on configuration for SAML-based applications

Type: New feature Service category: Enterprise Apps Product capability: SSO

When configuring SAML-based SSO applications, you're able to test the integration on the configuration page. If you encounter an error during sign in, you can provide the error in the testing experience and Azure AD provides you with resolution steps to solve the specific issue.

For more information, see:

- [Configuring single sign-on to applications that are not in the Azure Active Directory application gallery](#)
 - [How to debug SAML-based single sign-on to applications in Azure Active Directory](#)
-

Azure AD terms of use now has per user reporting

Type: New feature Service category: Terms of use Product capability: Compliance

Administrators can now select a given ToU and see all the users that have consented to that ToU and what date/time it took place.

For more information, see the [Azure AD terms of use feature](#).

Azure AD Connect Health: Risky IP for AD FS extranet lockout protection

Type: New feature Service category: Other Product capability: Monitoring & Reporting

Connect Health now supports the ability to detect IP addresses that exceed a threshold of failed U/P logins on an hourly or daily basis. The capabilities provided by this feature are:

- Comprehensive report showing IP address and the number of failed logins generated on an hourly/daily basis with customizable threshold.
- Email-based alerts showing when a specific IP address has exceeded the threshold of failed U/P logins on an hourly/daily basis.
- A download option to do a detailed analysis of the data

For more information, see [Risky IP Report](#).

Easy app config with metadata file or URL

Type: New feature Service category: Enterprise Apps Product capability: SSO

On the Enterprise applications page, administrators can upload a SAML metadata file to configure SAML based sign-on for Azure AD Gallery and Non-Gallery application.

Additionally, you can use Azure AD application federation metadata URL to configure SSO with the targeted application.

For more information, see [Configuring single sign-on to applications that are not in the Azure Active Directory application gallery](#).

Azure AD Terms of use now generally available

Type: New feature Service category: Terms of use Product capability: Compliance

Azure AD terms of use have moved from public preview to generally available.

For more information, see the [Azure AD terms of use feature](#).

Allow or block invitations to B2B users from specific organizations

Type: New feature Service category: B2B Product capability: B2B/B2C

You can now specify which partner organizations you want to share and collaborate with in Azure AD B2B Collaboration. To do this, you can choose to create list of specific allow or deny domains. When a domain is blocked using these capabilities, employees can no longer send invitations to people in that domain.

This helps you to control access to your resources, while enabling a smooth experience for approved users.

This B2B Collaboration feature is available for all Azure Active Directory customers and can be used in conjunction with Azure AD Premium features like Conditional Access and identity protection for more granular control of when and how external business users sign in and gain access.

For more information, see [Allow or block invitations to B2B users from specific organizations](#).

New federated apps available in Azure AD app gallery

Type: New feature Service category: Enterprise Apps Product capability: 3rd Party Integration

In April 2018, we've added these 13 new apps with Federation support to our app gallery:

Criterion HCM, [FiscalNote](#), [Secret Server \(On-Premises\)](#), [Dynamic Signal](#), [mindWireless](#), [OrgChart Now](#), [Ziflow](#), [AppNeta Performance Monitor](#), [Elium](#), [Fluxx Labs](#), [Cisco Cloud](#), Shelf, [SafetyNet](#)

For more information about the apps, see [SaaS application integration with Azure Active Directory](#).

For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Grant B2B users in Azure AD access to your on-premises applications (public preview)

Type: New feature Service category: B2B Product capability: B2B/B2C

As an organization that uses Azure Active Directory (Azure AD) B2B collaboration capabilities to invite guest users from partner organizations to your Azure AD, you can now provide these B2B users access to on-premises apps. These on-premises apps can use SAML-based authentication or integrated Windows authentication (IWA) with Kerberos constrained delegation (KCD).

For more information, see [Grant B2B users in Azure AD access to your on-premises applications](#).

Get SSO integration tutorials from the Azure Marketplace

Type: Changed feature Service category: Other Product capability: 3rd Party Integration

If an application that is listed in the [Azure Marketplace](#) supports SAML based single sign-on, clicking **Get it now** provides you with the integration tutorial associated with that application.

Faster performance of Azure AD automatic user provisioning to SaaS applications

Type: Changed feature Service category: App Provisioning Product capability: 3rd Party Integration

Previously, customers using the Azure Active Directory user provisioning connectors for SaaS applications (for example Salesforce, ServiceNow, and Box) could experience slow performance if their Azure AD tenants contained over 100,000 combined users and groups, and they were using user and group assignments to determine which users should be provisioned.

On April 2, 2018, significant performance enhancements were deployed to the Azure AD provisioning service that greatly reduce the amount of time needed to perform initial synchronizations between Azure Active Directory and target SaaS applications.

As a result, many customers that had initial synchronizations to apps that took many days or never completed, are now completing within a matter of minutes or hours.

For more information, see [What happens during provisioning](#)

Self-service password reset from Windows 10 lock screen for hybrid Azure AD joined machines

Type: Changed feature **Service category:** Self Service Password Reset **Product capability:** User Authentication

We have updated the Windows 10 SSPR feature to include support for machines that are hybrid Azure AD joined. This feature is available in Windows 10 RS4 allows users to reset their password from the lock screen of a Windows 10 machine. Users who are enabled and registered for self-service password reset can utilize this feature.

For more information, see [Azure AD password reset from the login screen](#).

March 2018

Certificate expire notification

Type: Fixed **Service category:** Enterprise Apps **Product capability:** SSO

Azure AD sends a notification when a certificate for a gallery or non-gallery application is about to expire.

Some users did not receive notifications for enterprise applications configured for SAML-based single sign-on. This issue was resolved. Azure AD sends notification for certificates expiring in 7, 30 and 60 days. You are able to see this event in the audit logs.

For more information, see:

- [Manage Certificates for federated single sign-on in Azure Active Directory](#)
 - [Audit activity reports in the Azure Active Directory portal](#)
-

Twitter and GitHub identity providers in Azure AD B2C

Type: New feature **Service category:** B2C - Consumer Identity Management **Product capability:** B2B/B2C

You can now add Twitter or GitHub as an identity provider in Azure AD B2C. Twitter is moving from public preview to GA. GitHub is being released in public preview.

For more information, see [What is Azure AD B2B collaboration?](#).

Restrict browser access using Intune Managed Browser with Azure AD application-based Conditional Access for iOS and Android

Type: New feature **Service category:** Conditional Access **Product capability:** Identity Security & Protection

Now in public preview!

Intune Managed Browser SSO: Your employees can use single sign-on across native clients (like Microsoft Outlook) and the Intune Managed Browser for all Azure AD-connected apps.

Intune Managed Browser Conditional Access Support: You can now require employees to use the Intune Managed browser using application-based Conditional Access policies.

Read more about this in our [blog post](#).

For more information, see:

- [Setup application-based Conditional Access](#)
 - [Configure managed browser policies](#)
-

App Proxy Cmdlets in PowerShell GA Module

Type: New feature **Service category:** App Proxy **Product capability:** Access Control

Support for Application Proxy cmdlets is now in the PowerShell GA Module! This does require you to stay updated on PowerShell modules - if you become more than a year behind, some cmdlets may stop working.

For more information, see [AzureAD](#).

Office 365 native clients are supported by Seamless SSO using a non-interactive protocol

Type: New feature **Service category:** Authentications (Logins) **Product capability:** User Authentication

User using Office 365 native clients (version 16.0.8730.xxxx and above) get a silent sign-on experience using Seamless SSO. This support is provided by the addition a non-interactive protocol (WS-Trust) to Azure AD.

For more information, see [How does sign-in on a native client with Seamless SSO work?](#)

Users get a silent sign-on experience, with Seamless SSO, if an application sends sign-in requests to Azure AD's tenant endpoints

Type: New feature **Service category:** Authentications (Logins) **Product capability:** User Authentication

Users get a silent sign-on experience, with Seamless SSO, if an application (for example,

<https://contoso.sharepoint.com>) sends sign-in requests to Azure AD's tenant endpoints - that is,

<https://login.microsoftonline.com/contoso.com/<...>> or https://login.microsoftonline.com/<tenant_ID>/<...> -

instead of Azure AD's common endpoint (<https://login.microsoftonline.com/common/<...>>).

For more information, see [Azure Active Directory Seamless Single Sign-On](#).

Need to add only one Azure AD URL, instead of two URLs previously, to users' Intranet zone settings to roll out Seamless SSO

Type: New feature **Service category:** Authentications (Logins) **Product capability:** User Authentication

To roll out Seamless SSO to your users, you need to add only one Azure AD URL to the users' Intranet zone settings by using group policy in Active Directory: <https://autologon.microsoftazuread-sso.com>. Previously, customers were required to add two URLs.

For more information, see [Azure Active Directory Seamless Single Sign-On](#).

New Federated Apps available in Azure AD app gallery

Type: New feature **Service category:** Enterprise Apps **Product capability:** 3rd Party Integration

In March 2018, we've added these 15 new apps with Federation support to our app gallery:

[Boxcryptor](#), [CylancePROTECT](#), [Wrike](#), [SignalFx](#), [Assistant by FirstAgenda](#), [YardiOne](#), [Vtiger CRM](#), [inwink](#), [Amplitude](#), [Spacio](#), [ContractWorks](#), [Bersin](#), [Mercell](#), [Trisotech Digital Enterprise Server](#), [Qumu Cloud](#).

For more information about the apps, see [SaaS application integration with Azure Active Directory](#).

For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

PIM for Azure Resources is generally available

Type: New feature **Service category:** Privileged Identity Management **Product capability:** Privileged Identity Management

If you are using Azure AD Privileged Identity Management for directory roles, you can now use PIM's time-bound access and assignment capabilities for Azure Resource roles such as Subscriptions, Resource Groups, Virtual Machines, and any other resource supported by Azure Resource Manager. Enforce multifactor

authentication when activating roles Just-In-Time, and schedule activations in coordination with approved change windows. In addition, this release adds enhancements not available during public preview including an updated UI, approval workflows, and the ability to extend roles expiring soon and renew expired roles.

For more information, see [PIM for Azure resources \(Preview\)](#)

Adding Optional Claims to your apps tokens (public preview)

Type: New feature Service category: Authentications (Logins) Product capability: User Authentication

Your Azure AD app can now request custom or optional claims in JWTs or SAML tokens. These are claims about the user or tenant that are not included by default in the token, due to size or applicability constraints. This is currently in public preview for Azure AD apps on the v1.0 and v2.0 endpoints. See the documentation for information on what claims can be added and how to edit your application manifest to request them.

For more information, see [Optional claims in Azure AD](#).

Azure AD supports PKCE for more secure OAuth flows

Type: New feature Service category: Authentications (Logins) Product capability: User Authentication

Azure AD docs have been updated to note support for PKCE, which allows for more secure communication during the OAuth 2.0 Authorization Code grant flow. Both S256 and plaintext code_challenges are supported on the v1.0 and v2.0 endpoints.

For more information, see [Request an authorization code](#).

Support for provisioning all user attribute values available in the Workday Get_Workers API

Type: New feature Service category: App Provisioning Product capability: 3rd Party Integration

The public preview of inbound provisioning from Workday to Active Directory and Azure AD now supports the ability to extract and provisioning all attribute values available in the Workday Get_Workers API. This adds supports for hundreds of additional standard and custom attributes beyond the ones shipped with the initial version of the Workday inbound provisioning connector.

For more information, see: [Customizing the list of Workday user attributes](#)

Changing group membership from dynamic to static, and vice versa

Type: New feature Service category: Group Management Product capability: Collaboration

It is possible to change how membership is managed in a group. This is useful when you want to keep the same group name and ID in the system, so any existing references to the group are still valid; creating a new group would require updating those references. We've updated the Azure AD Admin center to support this functionality. Now, customers can convert existing groups from dynamic membership to assigned membership and vice-versa. The existing PowerShell cmdlets are also still available.

For more information, see [Dynamic membership rules for groups in Azure Active Directory](#)

Improved sign-out behavior with Seamless SSO

Type: Changed feature Service category: Authentications (Logins) Product capability: User Authentication

Previously, even if users explicitly signed out of an application secured by Azure AD, they would be automatically signed back in using Seamless SSO if they were trying to access an Azure AD application again within their corpnet from their domain joined devices. With this change, sign out is supported. This allows users to choose the same or different Azure AD account to sign back in with, instead of being automatically signed in using Seamless SSO.

For more information, see [Azure Active Directory Seamless Single Sign-On](#)

Application Proxy Connector Version 1.5.402.0 Released

Type: Changed feature **Service category:** App Proxy **Product capability:** Identity Security & Protection

This connector version is gradually being rolled out through November. This new connector version includes the following changes:

- The connector now sets domain level cookies instead subdomain level. This ensures a smoother SSO experience and avoids redundant authentication prompts.
- Support for chunked encoding requests
- Improved connector health monitoring
- Several bug fixes and stability improvements

For more information, see [Understand Azure AD Application Proxy connectors](#).

February 2018

Improved navigation for managing users and groups

Type: Plan for change **Service category:** Directory Management **Product capability:** Directory

The navigation experience for managing users and groups has been streamlined. You can now navigate from the directory overview directly to the list of all users, with easier access to the list of deleted users. You can also navigate from the directory overview directly to the list of all groups, with easier access to group management settings. And also from the directory overview page, you can search for a user, group, enterprise application, or app registration.

Availability of sign-ins and audit reports in Microsoft Azure operated by 21Vianet (Azure China 21Vianet)

Type: New feature **Service category:** Azure Stack Product **capability:** Monitoring & Reporting

Azure AD Activity log reports are now available in Microsoft Azure operated by 21Vianet (Azure China 21Vianet) instances. The following logs are included:

- **Sign-ins activity logs** - Includes all the sign-ins logs associated with your tenant.
- **Self service Password Audit Logs** - Includes all the SSPR audit logs.
- **Directory Management Audit logs** - Includes all the directory management-related audit logs like User management, App Management, and others.

With these logs, you can gain insights into how your environment is doing. The provided data enables you to:

- Determine how your apps and services are utilized by your users.
- Troubleshoot issues preventing your users from getting their work done.

For more information about how to use these reports, see [Azure Active Directory reporting](#).

Use "Report Reader" role (non-admin role) to view Azure AD Activity Reports

Type: New feature **Service category:** Reporting **Product capability:** Monitoring & Reporting

As part of customers feedback to enable non-admin roles to have access to Azure AD activity logs, we have enabled the ability for users who are in the "Report Reader" role to access Sign-ins and Audit activity within the Azure portal as well as using the Microsoft Graph API.

For more information, how to use these reports, see [Azure Active Directory reporting](#).

EmployeeID claim available as user attribute and user identifier

Type: New feature Service category: Enterprise Apps Product capability: SSO

You can configure EmployeeID as the User identifier and User attribute for member users and B2B guests in SAML-based sign-on applications from the Enterprise application UI.

For more information, see [Customizing claims issued in the SAML token for enterprise applications in Azure Active Directory](#).

Simplified Application Management using Wildcards in Azure AD Application Proxy

Type: New feature Service category: App Proxy Product capability: User Authentication

To make application deployment easier and reduce your administrative overhead, we now support the ability to publish applications using wildcards. To publish a wildcard application, you can follow the standard application publishing flow, but use a wildcard in the internal and external URLs.

For more information, see [Wildcard applications in the Azure Active Directory application proxy](#)

New cmdlets to support configuration of Application Proxy

Type: New feature Service category: App Proxy Product capability: Platform

The latest release of the AzureAD PowerShell Preview module contains new cmdlets that allow customers to configure Application Proxy Applications using PowerShell.

The new cmdlets are:

- `Get-AzureADApplicationProxyApplication`
- `Get-AzureADApplicationProxyApplicationConnectorGroup`
- `Get-AzureADApplicationProxyConnector`
- `Get-AzureADApplicationProxyConnectorGroup`
- `Get-AzureADApplicationProxyConnectorGroupMembers`
- `Get-AzureADApplicationProxyConnectorMemberOf`
- `New-AzureADApplicationProxyApplication`
- `New-AzureADApplicationProxyConnectorGroup`
- `Remove-AzureADApplicationProxyApplication`
- `Remove-AzureADApplicationProxyApplicationConnectorGroup`
- `Remove-AzureADApplicationProxyConnectorGroup`
- `Set-AzureADApplicationProxyApplication`
- `Set-AzureADApplicationProxyApplicationConnectorGroup`
- `Set-AzureADApplicationProxyApplicationCustomDomainCertificate`
- `Set-AzureADApplicationProxyApplicationSingleSignOn`
- `Set-AzureADApplicationProxyConnector`
- `Set-AzureADApplicationProxyConnectorGroup`

New cmdlets to support configuration of groups

Type: New feature Service category: App Proxy Product capability: Platform

The latest release of the AzureAD PowerShell module contains cmdlets to manage groups in Azure AD. These cmdlets were previously available in the AzureADPreview module and are now added to the AzureAD module

The Group cmdlets that are now released for General Availability are:

- Get-AzureADMSGroup
- New-AzureADMSGroup
- Remove-AzureADMSGroup
- Set-AzureADMSGroup
- Get-AzureADMSGroupLifecyclePolicy
- New-AzureADMSGroupLifecyclePolicy
- Remove-AzureADMSGroupLifecyclePolicy
- Add-AzureADMSLifecyclePolicyGroup
- Remove-AzureADMSLifecyclePolicyGroup
- Reset-AzureADMSLifeCycleGroup
- Get-AzureADMSLifecyclePolicyGroup

A new release of Azure AD Connect is available

Type: New feature Service category: AD Sync Product capability: Platform

Azure AD Connect is the preferred tool to synchronize data between Azure AD and on premises data sources, including Windows Server Active Directory and LDAP.

IMPORTANT

This build introduces schema and sync rule changes. The Azure AD Connect Synchronization Service triggers a Full Import and Full Synchronization steps after an upgrade. For information on how to change this behavior, see [How to defer full synchronization after upgrade](#).

This release has the following updates and changes:

Fixed issues

- Fix timing window on background tasks for Partition Filtering page when switching to next page.
- Fixed a bug that caused Access violation during the ConfigDB custom action.
- Fixed a bug to recover from sql connection timeout.
- Fixed a bug where certificates with SAN wildcards fail pre-req check.
- Fixed a bug that causes miiserver.exe crash during Azure AD connector export.
- Fixed a bug where a bad password attempt logged on DC when running caused the Azure AD connect wizard to change configuration

New features and improvements

- Application telemetry - Administrators can switch this class of data on/off.
- Azure AD Health data - Administrators must visit the health portal to control their health settings. Once the service policy has been changed, the agents will read and enforce it.
- Added device writeback configuration actions and a progress bar for page initialization.
- Improved general diagnostics with HTML report and full data collection in a ZIP-Text / HTML Report.
- Improved reliability of auto upgrade and added additional telemetry to ensure the health of the server can be determined.
- Restrict permissions available to privileged accounts on AD Connector account. For new installations, the wizard restricts the permissions that privileged accounts have on the MSOL account after creating the

MSOL account. The changes affect express installations and custom installations with Auto-Create account.

- Changed the installer to not require SA privilege on clean install of AADConnect.
- New utility to troubleshoot synchronization issues for a specific object. Currently, the utility checks for the following things:
 - UserPrincipalName mismatch between synchronized user object and the user account in Azure AD Tenant.
 - If the object is filtered from synchronization due to domain filtering
 - If the object is filtered from synchronization due to organizational unit (OU) filtering
- New utility to synchronize the current password hash stored in the on-premises Active Directory for a specific user account. The utility does not require a password change.

Applications supporting Intune App Protection policies added for use with Azure AD application-based Conditional Access

Type: Changed feature **Service category:** Conditional Access **Product capability:** Identity Security & Protection

We have added more applications that support application-based Conditional Access. Now, you can get access to Office 365 and other Azure AD-connected cloud apps using these approved client apps.

The following applications will be added by the end of February:

- Microsoft Power BI
- Microsoft Launcher
- Microsoft Invoicing

For more information, see:

- [Approved client app requirement](#)
- [Azure AD app-based Conditional Access](#)

Terms of use update to mobile experience

Type: Changed feature **Service category:** Terms of use **Product capability:** Compliance

When the terms of use are displayed, you can now click **Having trouble viewing? Click here**. Clicking this link opens the terms of use natively on your device. Regardless of the font size in the document or the screen size of device, you can zoom and read the document as needed.

January 2018

New Federated Apps available in Azure AD app gallery

Type: New feature **Service category:** Enterprise Apps **Product capability:** 3rd Party Integration

In January 2018, the following new apps with federation support were added in the app gallery:

[IBM OpenPages](#), [OneTrust Privacy Management Software](#), [Dealpath](#), [\[IriusRisk Federated Directory](#), and [Fidelity NetBenefits](#).

For more information about the apps, see [SaaS application integration with Azure Active Directory](#).

For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Sign in with additional risk detected

Type: New feature **Service category:** Identity Protection **Product capability:** Identity Security & Protection

The insight you get for a detected risk detection is tied to your Azure AD subscription. With the Azure AD Premium P2 edition, you get the most detailed information about all underlying detections.

With the Azure AD Premium P1 edition, detections that are not covered by your license appear as the risk detection Sign-in with additional risk detected.

For more information, see [Azure Active Directory risk detections](#).

Hide Office 365 applications from end user's access panels

Type: New feature **Service category:** My Apps **Product capability:** SSO

You can now better manage how Office 365 applications show up on your user's access panels through a new user setting. This option is helpful for reducing the number of apps in a user's access panels if you prefer to only show Office apps in the Office portal. The setting is located in the **User Settings** and is labeled, **Users can only see Office 365 apps in the Office 365 portal**.

For more information, see [Hide an application from user's experience in Azure Active Directory](#).

Seamless sign into apps enabled for Password SSO directly from app's URL

Type: New feature **Service category:** My Apps **Product capability:** SSO

The My Apps browser extension is now available via a convenient tool that gives you the My Apps single-sign on capability as a shortcut in your browser. After installing, user's will see a waffle icon in their browser that provides them quick access to apps. Users can now take advantage of:

- The ability to directly sign in to password-SSO based apps from the app's sign-in page
- Launch any app using the quick search feature
- Shortcuts to recently used apps from the extension
- The extension is available for Microsoft Edge, Chrome, and Firefox.

For more information, see [My Apps Secure Sign-in Extension](#).

Azure AD administration experience in Azure Classic Portal has been retired

Type: Deprecated **Service category:** Azure AD **Product capability:** Directory

As of January 8, 2018, the Azure AD administration experience in the Azure classic portal has been retired. This took place in conjunction with the retirement of the Azure classic portal itself. In the future, you should use the [Azure AD admin center](#) for all your portal-based administration of Azure AD.

The PhoneFactor web portal has been retired

Type: Deprecated **Service category:** Azure AD **Product capability:** Directory

As of January 8, 2018, the PhoneFactor web portal has been retired. This portal was used for the administration of multi-factor authentication (MFA) server, but those functions have been moved into the Azure portal at [portal.azure.com](#).

The multifactor authentication (MFA) configuration is located at: [Azure Active Directory > multi-factor authentication \(MFA\) Server](#)

Deprecate Azure AD reports

Type: Deprecated Service category: Reporting Product capability: Identity Lifecycle Management

With the general availability of the new Azure Active Directory Administration console and new APIs now available for both activity and security reports, the report APIs under "/reports" endpoint have been retired as of end of December 31, 2017.

What's available?

As part of the transition to the new admin console, we have made 2 new APIs available for retrieving Azure AD Activity Logs. The new set of APIs provides richer filtering and sorting functionality in addition to providing richer audit and sign-in activities. The data previously available through the security reports can now be accessed through the Identity Protection risk detections API in Microsoft Graph.

For more information, see:

- [Get started with the Azure Active Directory reporting API](#)
 - [Get started with Azure Active Directory Identity Protection and Microsoft Graph](#)
-

December 2017

Terms of use in the Access Panel

Type: New feature Service category: Terms of use Product capability: Compliance

You now can go to the Access Panel and view the terms of use that you previously accepted.

Follow these steps:

1. Go to the [MyApps portal](#), and sign in.
2. In the upper-right corner, select your name, and then select **Profile** from the list.
3. On your **Profile**, select **Review terms of use**.
4. Now you can review the terms of use you accepted.

For more information, see the [Azure AD terms of use feature \(preview\)](#).

New Azure AD sign-in experience

Type: New feature Service category: Azure AD Product capability: User authentication

The Azure AD and Microsoft account identity system UIs were redesigned so that they have a consistent look and feel. In addition, the Azure AD sign-in page collects the user name first, followed by the credential on a second screen.

For more information, see [The new Azure AD sign-in experience is now in public preview](#).

Fewer sign-in prompts: A new "keep me signed in" experience for Azure AD sign-in

Type: New feature Service category: Azure AD Product capability: User authentication

The **Keep me signed in** check box on the Azure AD sign-in page was replaced with a new prompt that shows up after you successfully authenticate.

If you respond **Yes** to this prompt, the service gives you a persistent refresh token. This behavior is the same as when you selected the **Keep me signed in** check box in the old experience. For federated tenants, this prompt shows after you successfully authenticate with the federated service.

For more information, see [Fewer sign-in prompts: The new "keep me signed in" experience for Azure AD is in preview](#).

Add configuration to require the terms of use to be expanded prior to accepting

Type: New feature Service category: Terms of use Product capability: Compliance

An option for administrators requires their users to expand the terms of use prior to accepting the terms.

Select either **On** or **Off** to require users to expand the terms of use. The **On** setting requires users to view the terms of use prior to accepting them.

For more information, see the [Azure AD terms of use feature \(preview\)](#).

Scoped activation for eligible role assignments

Type: New feature Service category: Privileged Identity Management Product capability: Privileged Identity Management

You can use scoped activation to activate eligible Azure resource role assignments with less autonomy than the original assignment defaults. An example is if you're assigned as the owner of a subscription in your tenant. With scoped activation, you can activate the owner role for up to five resources contained within the subscription (such as resource groups and virtual machines). Scoping your activation might reduce the possibility of executing unwanted changes to critical Azure resources.

For more information, see [What is Azure AD Privileged Identity Management?](#).

New federated apps in the Azure AD app gallery

Type: New feature Service category: Enterprise apps Product capability: 3rd Party Integration

In December 2017, we've added these new apps with Federation support to our app gallery:

[Accredible](#), [Adobe Experience Manager](#), [EFI Digital StoreFront](#), [Communifire](#), [CybSafe](#), [FactSet](#), [IMAGE WORKS](#), [MOBI](#), [MobileIron Azure AD integration](#), [Reflektive](#), [SAML SSO for Bamboo by resolution GmbH](#), [SAML SSO for Bitbucket by resolution GmbH](#), [Vodeclic](#), [WebHR](#), [Zenegy Azure AD Integration](#).

For more information about the apps, see [SaaS application integration with Azure Active Directory](#).

For more information about listing your application in the Azure AD app gallery, see [List your application in the Azure Active Directory application gallery](#).

Approval workflows for Azure AD directory roles

Type: Changed feature Service category: Privileged Identity Management Product capability: Privileged Identity Management

Approval workflow for Azure AD directory roles is generally available.

With approval workflow, privileged-role administrators can require eligible-role members to request role activation before they can use the privileged role. Multiple users and groups can be delegated approval responsibilities. Eligible role members receive notifications when approval is finished and their role is active.

Pass-through authentication: Skype for Business support

Type: Changed feature Service category: Authentications (Logins) Product capability: User authentication

Pass-through authentication now supports user sign-ins to Skype for Business client applications that support modern authentication, which includes online and hybrid topologies.

For more information, see [Skype for Business topologies supported with modern authentication](#).

Updates to Azure AD Privileged Identity Management for Azure RBAC (preview)

Type: Changed feature **Service category:** Privileged Identity Management **Product capability:** Privileged Identity Management

With the public preview refresh of Azure AD Privileged Identity Management (PIM) for Azure role-based access control (Azure RBAC), you can now:

- Use Just Enough Administration.
- Require approval to activate resource roles.
- Schedule a future activation of a role that requires approval for both Azure AD and Azure roles.

For more information, see [Privileged Identity Management for Azure resources \(preview\)](#).

November 2017

Access Control service retirement

Type: Plan for change **Service category:** Access Control service **Product capability:** Access Control service

Azure Active Directory Access Control (also known as the Access Control service) will be retired in late 2018. More information that includes a detailed schedule and high-level migration guidance will be provided in the next few weeks. You can leave comments on this page with any questions about the Access Control service, and a team member will answer them.

Restrict browser access to the Intune Managed Browser

Type: Plan for change **Service category:** Conditional Access **Product capability:** Identity security and protection

You can restrict browser access to Office 365 and other Azure AD-connected cloud apps by using the Intune Managed Browser as an approved app.

You now can configure the following condition for application-based Conditional Access:

Client apps: Browser

What is the effect of the change?

Today, access is blocked when you use this condition. When the preview is available, all access will require the use of the managed browser application.

Look for this capability and more information in upcoming blogs and release notes.

For more information, see [Conditional Access in Azure AD](#).

New approved client apps for Azure AD app-based Conditional Access

Type: Plan for change **Service category:** Conditional Access **Product capability:** Identity security and protection

The following apps are on the list of [approved client apps](#):

- [Microsoft Kaizala](#)
- Microsoft StaffHub

For more information, see:

- [Approved client app requirement](#)
- [Azure AD app-based Conditional Access](#)

Terms-of-use support for multiple languages

Type: New feature Service category: Terms of use Product capability: Compliance

Administrators now can create new terms of use that contain multiple PDF documents. You can tag these PDF documents with a corresponding language. Users are shown the PDF with the matching language based on their preferences. If there is no match, the default language is shown.

Real-time password writeback client status

Type: New feature Service category: Self-service password reset Product capability: User authentication

You now can review the status of your on-premises password writeback client. This option is available in the **On-premises integration** section of the [Password reset](#) page.

If there are issues with your connection to your on-premises writeback client, you see an error message that provides you with:

- Information on why you can't connect to your on-premises writeback client.
- A link to documentation that assists you in resolving the issue.

For more information, see [on-premises integration](#).

Azure AD app-based Conditional Access

Type: New feature Service category: Azure AD Product capability: Identity security and protection

You now can restrict access to Office 365 and other Azure AD-connected cloud apps to [approved client apps](#) that support Intune app protection policies by using [Azure AD app-based Conditional Access](#). Intune app protection policies are used to configure and protect company data on these client applications.

By combining [app-based](#) with [device-based](#) Conditional Access policies, you have the flexibility to protect data for personal and company devices.

The following conditions and controls are now available for use with app-based Conditional Access:

Supported platform condition

- iOS
- Android

Client apps condition

- Mobile apps and desktop clients

Access control

- Require approved client app

For more information, see [Azure AD app-based Conditional Access](#).

Manage Azure AD devices in the Azure portal

Type: New feature Service category: Device registration and management Product capability: Identity security and protection

You now can find all your devices connected to Azure AD and the device-related activities in one place. There is a new administration experience to manage all your device identities and settings in the Azure portal. In this release, you can:

- View all your devices that are available for Conditional Access in Azure AD.

- View properties, which include your hybrid Azure AD-joined devices.
- Find BitLocker keys for your Azure AD-joined devices, manage your device with Intune, and more.
- Manage Azure AD device-related settings.

For more information, see [Manage devices by using the Azure portal](#).

Support for macOS as a device platform for Azure AD Conditional Access

Type: New feature Service category: Conditional Access Product capability: Identity security and protection

You now can include (or exclude) macOS as a device platform condition in your Azure AD Conditional Access policy. With the addition of macOS to the supported device platforms, you can:

- **Enroll and manage macOS devices by using Intune.** Similar to other platforms like iOS and Android, a company portal application is available for macOS to do unified enrollments. You can use the new company portal app for macOS to enroll a device with Intune and register it with Azure AD.
- **Ensure macOS devices adhere to your organization's compliance policies defined in Intune.** In Intune on the Azure portal, you now can set up compliance policies for macOS devices.
- **Restrict access to applications in Azure AD to only compliant macOS devices.** Conditional Access policy authoring has macOS as a separate device platform option. Now you can author macOS-specific Conditional Access policies for the targeted application set in Azure.

For more information, see:

- [Create a device compliance policy for macOS devices with Intune](#)
 - [Conditional Access in Azure AD](#)
-

Network Policy Server extension for Azure AD Multi-Factor Authentication

Type: New feature Service category: Multifactor authentication Product capability: User authentication

The Network Policy Server extension for Azure Active Directory (Azure AD) Multi-Factor Authentication adds cloud-based multifactor authentication capabilities to your authentication infrastructure by using your existing servers. With the Network Policy Server extension, you can add phone call, text message, or phone app verification to your existing authentication flow. You don't have to install, configure, and maintain new servers.

This extension was created for organizations that want to protect virtual private network connections without deploying the Azure Active Directory Multi-Factor Authentication Server. The Network Policy Server extension acts as an adapter between RADIUS and cloud-based Azure AD Multi-Factor Authentication to provide a second factor of authentication for federated or synced users.

For more information, see [Integrate your existing Network Policy Server infrastructure with Azure AD Multi-Factor Authentication](#).

Restore or permanently remove deleted users

Type: New feature Service category: User management Product capability: Directory

In the Azure AD admin center, you can now:

- Restore a deleted user.
- Permanently delete a user.

To try it out:

1. In the Azure AD admin center, select [All users](#) in the **Manage** section.
2. From the **Show** list, select [Recently deleted users](#).

3. Select one or more recently deleted users, and then either restore them or permanently delete them.

New approved client apps for Azure AD app-based Conditional Access

Type: Changed feature **Service category:** Conditional Access **Product capability:** Identity security and protection

The following apps were added to the list of [approved client apps](#):

- Microsoft Planner
- Azure Information Protection

For more information, see:

- [Approved client app requirement](#)
 - [Azure AD app-based Conditional Access](#)
-

Use "OR" between controls in a Conditional Access policy

Type: Changed feature **Service category:** Conditional Access **Product capability:** Identity security and protection

You now can use "OR" (require one of the selected controls) for Conditional Access controls. You can use this feature to create policies with "OR" between access controls. For example, you can use this feature to create a policy that requires a user to sign in by using multifactor authentication "OR" to be on a compliant device.

For more information, see [Controls in Azure AD Conditional Access](#).

Aggregation of real-time risk detections

Type: Changed feature **Service category:** Identity protection **Product capability:** Identity security and protection

In Azure AD Identity Protection, all real-time risk detections that originated from the same IP address on a given day are now aggregated for each risk detection type. This change limits the volume of risk detections shown without any change in user security.

The underlying real-time detection works each time the user signs in. If you have a sign-in risk security policy set up to multifactor authentication or block access, it is still triggered during each risky sign-in.

October 2017

Deprecate Azure AD reports

Type: Plan for change **Service category:** Reporting **Product capability:** Identity Lifecycle Management

The Azure portal provides you with:

- A new Azure AD administration console.
- New APIs for activity and security reports.

Due to these new capabilities, the report APIs under the /reports endpoint were retired on December 10, 2017.

Automatic sign-in field detection

Type: Fixed **Service category:** My Apps **Product capability:** Single sign-on

Azure AD supports automatic sign-in field detection for applications that render an HTML user name and password field. These steps are documented in [How to automatically capture sign-in fields for an application](#).

You can find this capability by adding a *Non-Gallery* application on the **Enterprise Applications** page in the [Azure portal](#). Additionally, you can configure the **Single Sign-on** mode on this new application to **Password-based Single Sign-on**, enter a web URL, and then save the page.

Due to a service issue, this functionality was temporarily disabled. The issue was resolved, and the automatic sign-in field detection is available again.

New Multifactor Authentication features

Type: New feature **Service category:** Multifactor authentication **Product capability:** Identity security and protection

Azure Active Directory Multi-Factor Authentication (MFA) is an essential part of protecting your organization. To make credentials more adaptive and the experience more seamless, the following features were added:

- Multifactor challenge results are directly integrated into the Azure AD sign-in report, which includes programmatic access to multifactor authentication (MFA) results.
- The multifactor authentication (MFA) configuration is more deeply integrated into the Azure AD configuration experience in the Azure portal.

With this public preview, multifactor authentication (MFA) management and reporting are an integrated part of the core Azure AD configuration experience. Now you can manage the multifactor authentication (MFA) management portal functionality within the Azure AD experience.

For more information, see [Reference for MFA reporting in the Azure portal](#).

Terms of use

Type: New feature **Service category:** Terms of use **Product capability:** Compliance

You can use Azure AD terms of use to present information such as relevant disclaimers for legal or compliance requirements to users.

You can use Azure AD terms of use in the following scenarios:

- General terms of use for all users in your organization
- Specific terms of use based on a user's attributes (for example, doctors vs. nurses or domestic vs. international employees, done by dynamic groups)
- Specific terms of use for accessing high-impact business apps, like Salesforce

For more information, see [Azure AD terms of use](#).

Enhancements to Privileged Identity Management

Type: New feature **Service category:** Privileged Identity Management **Product capability:** Privileged Identity Management

With Azure AD Privileged Identity Management, you can manage, control, and monitor access to Azure resources (preview) within your organization to:

- Subscriptions
- Resource groups
- Virtual machines

All resources within the Azure portal that use the Azure RBAC functionality can take advantage of all the security and lifecycle management capabilities that Azure AD Privileged Identity Management has to offer.

For more information, see [Privileged Identity Management for Azure resources](#).

Access reviews

Type: New feature Service category: Access reviews Product capability: Compliance

Organizations can use access reviews (preview) to efficiently manage group memberships and access to enterprise applications:

- You can recertify guest user access by using access reviews of their access to applications and memberships of groups. Reviewers can efficiently decide whether to allow guests continued access based on the insights provided by the access reviews.
- You can recertify employee access to applications and group memberships with access reviews.

You can collect the access review controls into programs relevant for your organization to track reviews for compliance or risk-sensitive applications.

For more information, see [Azure AD access reviews](#).

Hide third-party applications from My Apps and the Office 365 app launcher

Type: New feature Service category: My Apps Product capability: Single sign-on

You now can better manage apps that show up on your users' portals through a new **hide app** property. You can hide apps to help in cases where app tiles show up for back-end services or duplicate tiles and clutter users' app launchers. The toggle is in the **Properties** section of the third-party app and is labeled **Visible to user?** You also can hide an app programmatically through PowerShell.

For more information, see [Hide a third-party application from a user's experience in Azure AD](#).

What's available?

As part of the transition to the new admin console, two new APIs for retrieving Azure AD activity logs are available. The new set of APIs provides richer filtering and sorting functionality in addition to providing richer audit and sign-in activities. The data previously available through the security reports now can be accessed through the Identity Protection Risk Detections API in Microsoft Graph.

September 2017

Hotfix for Identity Manager

Type: Changed feature Service category: Identity Manager Product capability: Identity lifecycle management

A hotfix roll-up package (build 4.4.1642.0) is available as of September 25, 2017, for Identity Manager 2016 Service Pack 1. This roll-up package:

- Resolves issues and adds improvements.
- Is a cumulative update that replaces all Identity Manager 2016 Service Pack 1 updates up to build 4.4.1459.0 for Identity Manager 2016.
- Requires you to have Identity Manager 2016 build 4.4.1302.0.

For more information, see [Hotfix rollup package \(build 4.4.1642.0\) is available for Identity Manager 2016 Service Pack 1](#).

Identity data storage for European customers in Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Identity data is stored by Azure AD in a geographical location based on the address provided by your organization when it subscribed for a Microsoft Online service such as Microsoft 365 and Azure. For information on where your identity data is stored, you can use the [Where your data is located](#) section of the Microsoft Trust Center.

For customers who provided an address in Europe, Azure AD keeps most of the identity data within European datacenters. This document provides information on any data that is stored outside of Europe by Azure AD services.

Microsoft Azure AD Multi-Factor Authentication

For cloud-based Azure AD Multi-Factor Authentication, authentication is complete in the closest datacenter to the user. Datacenters for Azure AD Multi-Factor Authentication exist in North America, Europe, and Asia Pacific.

- Multi-factor authentication using phone calls originate from datacenters in the customer's region and are routed by global providers.
- Multi-factor authentication using SMS is routed by global providers.
- Multi-factor authentication requests using the Microsoft Authenticator app push notifications that originate from EU datacenters are processed in EU datacenters.
 - Device vendor-specific services, such as Apple Push Notifications, may be outside Europe.
- Multi-factor authentication requests using OATH codes that originate from EU datacenters are validated in the EU.

For more information about what user information is collected by Azure Multi-Factor Authentication Server (MFA Server) and cloud-based Azure AD MFA, see [Azure Multi-Factor Authentication user data collection](#).

Password-based Single Sign-On for Enterprise Applications

If a customer creates a new enterprise application (whether through Azure AD Gallery or non-Gallery) and enables password-based SSO, the Application sign in URL, and custom capture sign in fields are stored in the United States. For more information, see [Configure password-based single sign-on](#)

Microsoft Azure Active Directory B2B (Azure AD B2B)

Azure AD B2B stores invitations with redeem link and redirect URL information in US datacenters. In addition, email address of users that unsubscribe from receiving B2B invitations are also stored in U.S. datacenters.

Microsoft Azure Active Directory Domain Services (Azure AD DS)

Azure AD DS stores user data in the same location as the customer-selected Azure Virtual Network. So, if the network is outside Europe, the data is replicated and stored outside Europe.

Azure role-based access control (Azure RBAC)

Role definitions, role assignments, and deny assignments are stored globally to ensure that you have access to

your resources regardless of the region you created the resource. For more information, see [What is Azure role-based access control \(Azure RBAC\)?](#)

Federation in Microsoft Exchange Server 2013

- Application identifier (AppID) - A unique number generated by the Azure Active Directory authentication system to identify Exchange organizations.
- Approved Federated domains list for Application
- Application's token signing Public Key

For more info about federation in Microsoft Exchange server, see the [Federation: Exchange 2013 Help](#) article.

Other considerations

Services and applications that integrate with Azure AD have access to identity data. Evaluate each service and application you use to determine how identity data is processed by that specific service and application, and whether they meet your company's data storage requirements.

For more information about Microsoft services' data residency, see the [Where your data is located](#) section of the Microsoft Trust Center.

Next steps

For more information about any of the features and functionality described above, see these articles:

- [What is Multi-Factor Authentication?](#)
- [Azure AD self-service password reset](#)
- [What is Azure Active Directory B2C?](#)
- [What is Azure AD B2B collaboration?](#)
- [Azure Active Directory \(AD\) Domain Services](#)

Customer Data storage for Australian and New Zealand customers in Azure Active Directory

4/10/2022 • 2 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) stores its Customer Data in a geographical location based on the country you provided when you signed up for a Microsoft Online service. Microsoft Online services include Microsoft 365 and Azure.

For information about where Azure AD and other Microsoft services' data is located, see the [Where your data is located](#) section of the Microsoft Trust Center.

From February 26, 2020, Microsoft began storing Azure AD's Customer Data for new tenants with an Australian or New Zealand billing address within the Australian datacenters.

Additionally, certain Azure AD features do not yet support storage of Customer Data in Australia. Please go to the [Azure AD data map](#), for specific feature information. For example, Microsoft Azure AD Multi-Factor Authentication stores Customer Data in the US and processes it globally. See [Data residency and customer data for Azure AD Multi-Factor Authentication](#).

NOTE

Microsoft products, services, and third-party applications that integrate with Azure AD have access to Customer Data. Evaluate each product, service, and application you use to determine how Customer Data is processed by that specific product, service, and application, and whether they meet your company's data storage requirements. For more information about Microsoft services' data residency, see the [Where your data is located](#) section of the Microsoft Trust Center.

Azure role-based access control (Azure RBAC)

Role definitions, role assignments, and deny assignments are stored globally to ensure that you have access to your resources regardless of the region you created the resource. For more information, see [What is Azure role-based access control \(Azure RBAC\)?](#)