Contents

Azure Active Directory FAQ

What is Azure Active Directory?

7/20/2020 • 9 minutes to read • Edit Online

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:

- External resources, such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications.
- Internal resources, such as 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 Office 365.

Who uses Azure AD?

Azure AD is intended for:

- **IT admins.** As an IT admin, you can 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. Additionally, you can use Azure AD to automate user provisioning between your existing Windows Server AD and your cloud apps, including Office 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 Office 365 or Microsoft Azure, require Azure AD for sign-in 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, providing 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, Office 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 (an on-premises identity and access management suite) 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 and 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 (also known as the Access panel), 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).

CATEGORY	DESCRIPTION
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.
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 assignment, 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	Provides 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 Office 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 cannot have an account without an identity.
Azure AD account	An identity created through Azure AD or another Microsoft cloud service, such as Office 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 has access to the Azure Account Center and enables you to manage all subscriptions in an account. For more information, see Classic subscription administrator roles, Azure Role-based access control (RBAC) 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 RBAC 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 role-base access control (RBAC) that provides fine-grained access management to Azure resources. For more information, see Classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles.
Azure AD Global administrator	This administrator role is automatically assigned to whomever created the Azure AD tenant. Global administrators can do all of the administrative functions for Azure AD and any services that federate to Azure AD, such as Exchange Online, SharePoint Online, and Skype for Business Online. You can have multiple Global administrators, but only Global administrators can assign administrator roles (including assigning other Global administrators) to users. Note that this administrator role is called Global administrator in the Azure portal, but it's called **Company administrator** in the Microsoft Graph API and Azure AD PowerShell.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.

TERM OR CONCEPT	DESCRIPTION
Azure tenant	A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription, such as Microsoft Azure, Microsoft Intune, or Office 365. An Azure tenant represents a single organization.
Single tenant	Azure tenants that access other services in a dedicated environment are considered single tenant.
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, domainname.onmicrosoft.com. In addition to that initial name, you can also add your organization's domain names, which 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 alain@contoso.com.
Microsoft account (also called, MSA)	Personal accounts that provide access to your consumer-oriented Microsoft products and cloud services, such as Outlook, OneDrive, Xbox LIVE, or Office 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

3/8/2020 • 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 role-based access control (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 is 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.
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 can't be used for other purposes to gain backdoor access.

CONCEPT	ACTIVE DIRECTORY (AD)	AZURE ACTIVE DIRECTORY
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 complaint (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?

7/20/2020 • 47 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 that are older than six months, you can find them in the Archive for What's new in Azure Active Directory.

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 multi-factor 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 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, PKIsigning 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 Office 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 riskEventsTypes_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 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 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 uses.

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 ID, 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 (AAD) 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 ADConnect 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 as 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 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, Office 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, TickitLMS 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 MFA and self-service password reset (SSPR). This has been one of

the most-requested features in the Azure 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: RBAC

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: RBAC

Product capability: Access Control

Printer Administrator: Users with this rolecan 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 rolecan 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: RBAC

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: RBAC

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 Office 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 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 multi-factor authentication for secure access
- Require MFA for administrative roles
- Enable policy to block legacy 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 multi-factor authentication and added two.

Removed improvement actions:

- Register all users for multi-factor authentication
- Require MFA for all users
- Require MFA for Azure AD privileged roles

Added improvement actions:

- Ensure all users can complete multi-factor authentication for secure access
- Require MFA for administrative roles

These new improvement actions require registering your users or admins for multi-factor 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 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, contexxt.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 Protectionexperience 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 MFA solutions face the following limitations: they work only after a password has been entered; they don't serve as 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, 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 - 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 multi-factor authentication (MFA), and adding two.

The following improvement actions will be removed:

- Register all users for MFA
- Require MFA for all users
- Require MFA for Azure AD privileged roles

The following improvement actions will be added:

- Ensure all users can complete MFA for secure access
- Require MFA for administrative roles

These new improvement actions will require registering your users or admins for 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 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, 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.

What's new for Azure Active Directory in Microsoft 365 Government

2/17/2020 • 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?

7/20/2020 • 147 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

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 MFA to Conditional Access-based 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 Multi-Factor Authentication (MFA) and then enabled for MFA through a Conditional Access policy.

To require users to re-register, you can select the **Required re-register MFA** option from the user's authentication methods in the Azure AD portal. For more information about migrating users from per-user MFA to Conditional Access-based MFA, see Convert users from per-user MFA to Conditional Access based MFA.

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, Salestim, Learnster, Dynatrace, HunchBuzz, Freshworks, eCornell, ShipHazmat, Netskope Cloud Security, Contentful, Bindtuning,

HireVue Coordinate – Europe, HireVue Coordinate - USOnly, 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
- 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:** RBAC **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. For more information about this new version, see Azure AD Connect: Version release history.

Azure 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 MFA Server prior to July 1, 2019, you can now download the latest version of 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 MFA Server for new deployments. New customers who require multi-factor authentication should use cloud-based Azure Multi-Factor Authentication. For more information, see Planning a cloud-based Azure 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:** RBAC **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 Amazon Web Services (AWS)
- 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, 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 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 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 Multi-Factor Authentication Server firewall requirements** section of the Getting started with the Azure 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 Hub, 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 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 Hub, 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 URIs, 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 URIs 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, ExpenseIn, 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 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 MFA Server for new deployments. New customers who want to require multi-factor authentication in their organization must now use cloud-based Azure Multi-Factor Authentication. Customers who activated 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 Multi-Factor Authentication Server. For more information about cloud-based Azure Multi-Factor Authentication, see Planning a cloud-based Azure 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 Multi-Factor 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, Indiggo

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 allow list 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".

For more information, see Troubleshooting Errors during synchronization.

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, ExcelityGlobal, 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

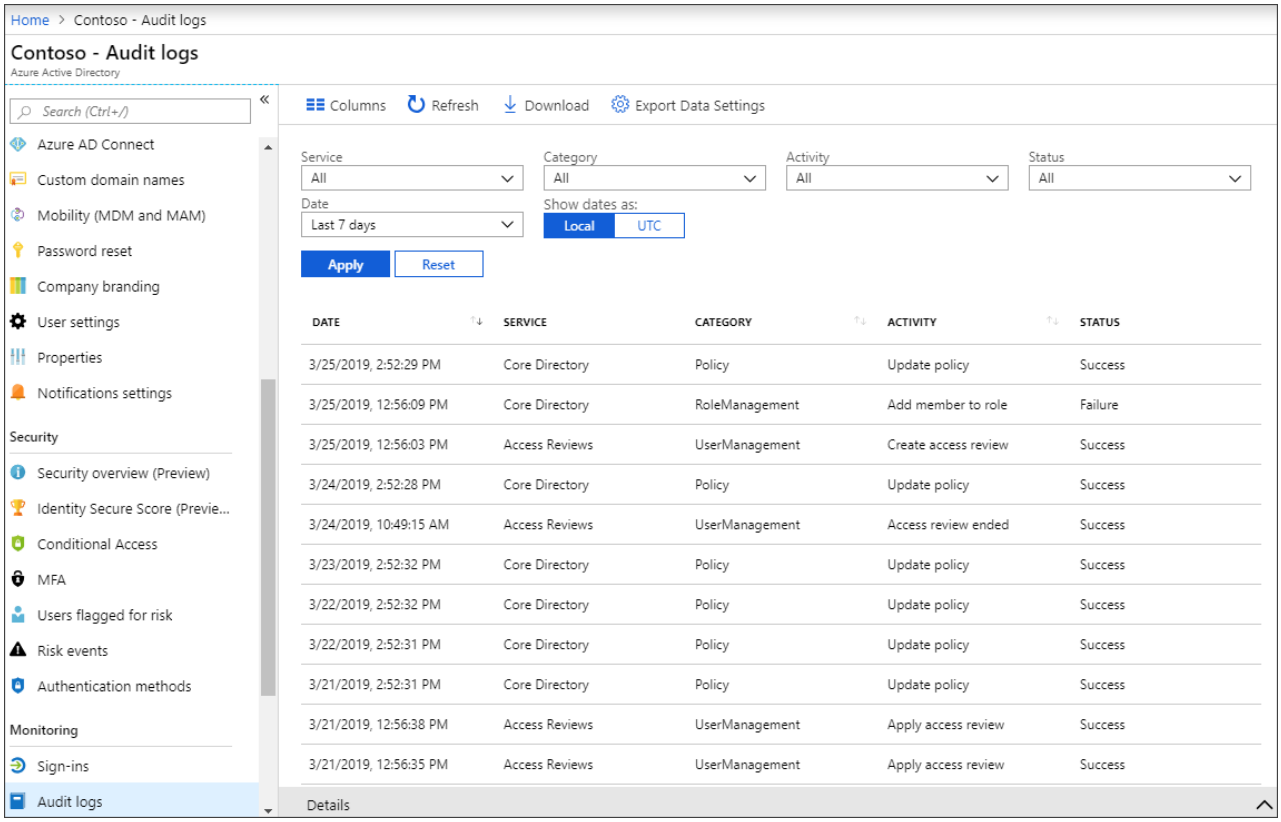
Client apps can incorrectly issue hundreds of the same login requests over a short period of time. These requests, whether they're successful or not, all contribute to a poor user experience and heightened workloads for the IDP, increasing latency for all users and reducing the availability of the IDP.

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.



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 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 MFA/SSPR registration preview experience, helping your users to more quickly register their security info for both 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 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 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.	• Account Provisioning • Core Directory • Self-service Password Reset	• User Management • Group Management • App Management
targetResources	Includes **TargetResourceType** at the top level.		• Policy • App • User • Group
loggedByService	Provides the name of the service that generated the audit log.	Null	• 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.	• 0 • 1	• 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

FIELD NAME	WHAT CHANGED	OLD VALUES	NEW VALUES
conditionalAccessStatus	Provides the result of the Conditional Access Policy Status at sign-in. Previously, this was enumerated, but we now show the actual value.	• 0 • 1 • 2 • 3	• 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.	• 0 • 1 • 2 • 3	• 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

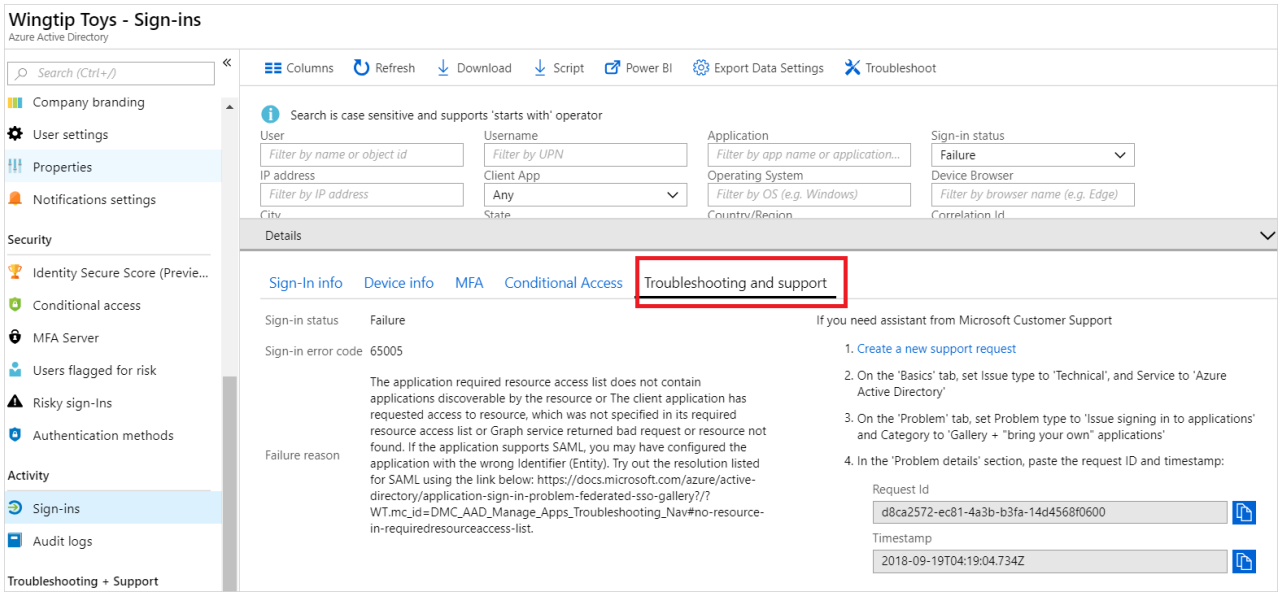
Check out the new deployment plan that's available for the My Apps Access panel (https://aka.ms/deploymentplans). The My Apps Access panel provides users with a single place to find and access their apps. This portal also provides users with self-service opportunities, such as requesting access to apps 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.



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, Nuclino, 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 Multi-Factor 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 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 MFA. Additionally, if your organization doesn't enforce MFA or SSPR registration, people can still register any 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 Multi-Factor 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 Multi-Factor Authentication (MFA) in a single experience. Users

will no longer have to register the same security info for SSPR and MFA in two different experiences. This new experience also applies to users who have either SSPR or MFA.

If an organization isn't enforcing MFA or SSPR registration, users can register their security info through the **My Apps** portal. From there, users can register any methods enabled for 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 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 Multi-Factor Authentication (MFA) in your organization.

To view the 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, and Firefox.

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 (CA), 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 AAD, 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 AAD 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 Multi-Factor 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 release 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 AAD connector export.
- Fixed a bug where a bad password attempt logged on DC when running caused the AAD 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 MFA server, but those functions have been moved into the Azure portal at portal.azure.com.

The MFA configuration is located at: **Azure Active Directory > 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 (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 RBAC 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 Multi-Factor Authentication

Type: New feature **Service category:** Multi-factor authentication **Product capability:** User authentication

The Network Policy Server extension for Azure Multi-Factor Authentication adds cloud-based Multi-Factor 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 Multi-Factor Authentication Server. The Network Policy Server extension acts as an adapter

between RADIUS and cloud-based Azure 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 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 Multi-Factor 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 Multi-Factor 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 Multi-Factor Authentication features

Type: New feature **Service category:** Multi-factor authentication **Product capability:** Identity security and protection

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:

- Multi-factor challenge results are directly integrated into the Azure AD sign-in report, which includes programmatic access to MFA results.
- The MFA configuration is more deeply integrated into the Azure AD configuration experience in the Azure portal.

With this public preview, MFA management and reporting are an integrated part of the core Azure AD configuration experience. Now you can manage the 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.

Quickstart: Create a new tenant in Azure Active Directory

3/19/2020 • 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.

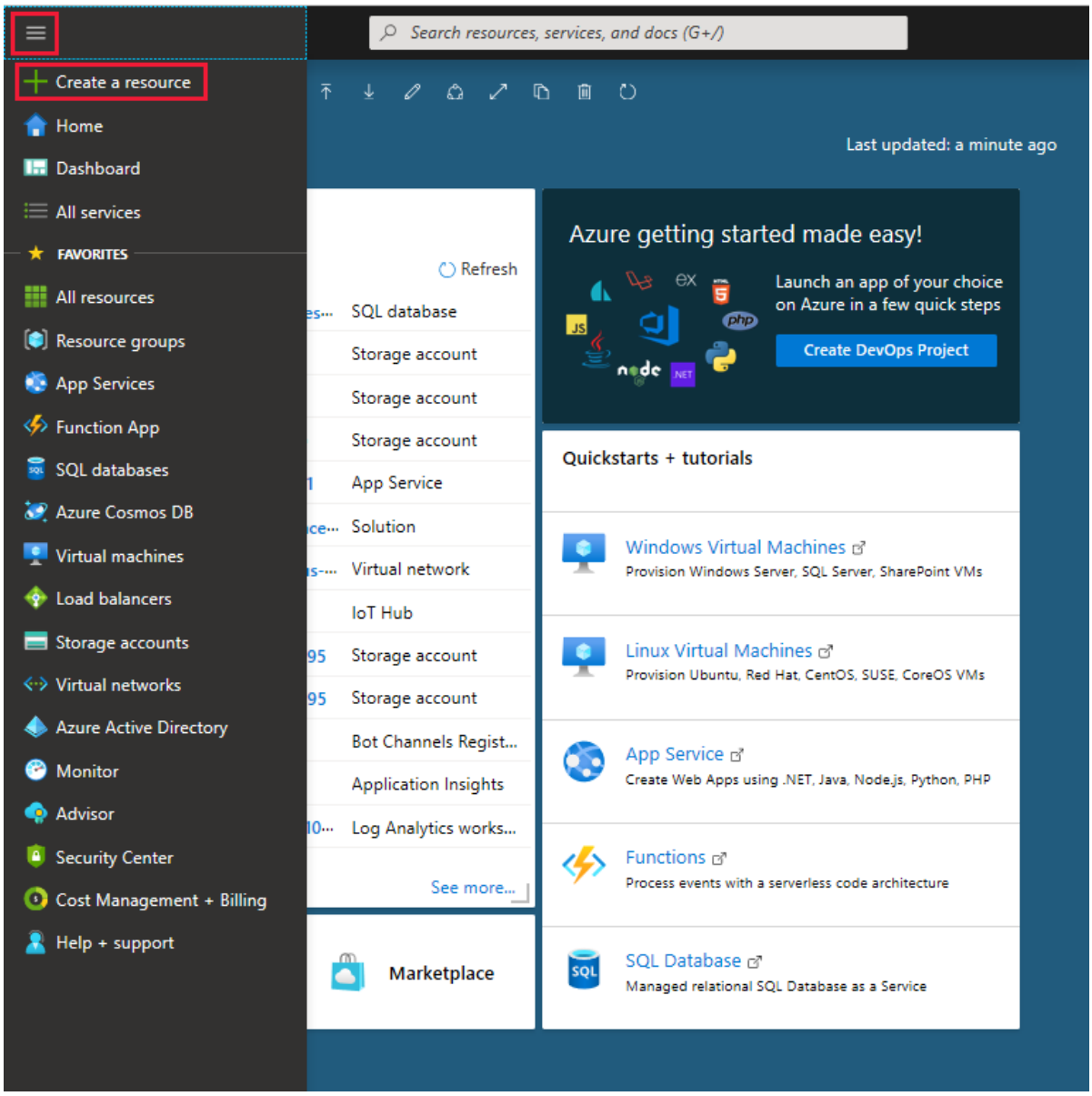
If you don't have an Azure subscription, create a free account before you begin.

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.

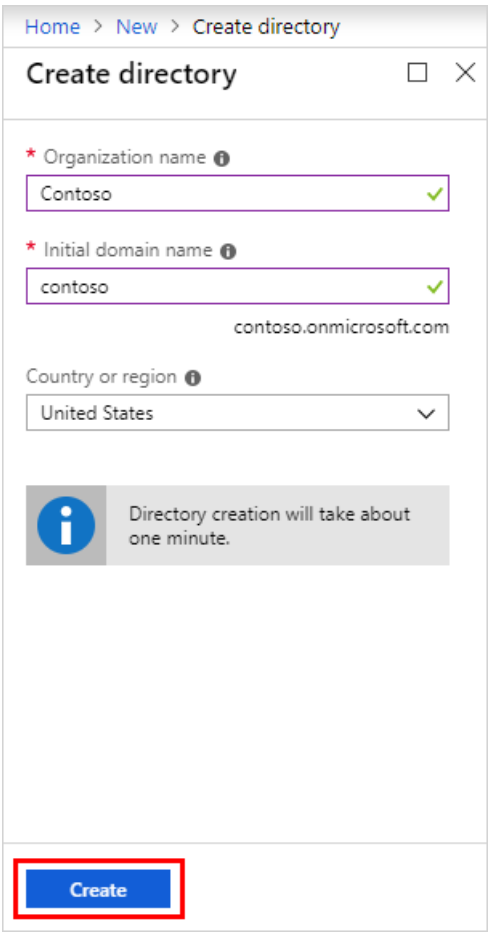
To create a new tenant

1. Sign in to your organization's Azure portal.
2. From the Azure portal menu, select **Create a resource**.



3. Select **Identity**, and then select **Azure Active Directory**.

   The **Create directory** page appears.



4. On the **Create directory** page, enter the following information:
   - Type *Contoso* into the **Organization name** box.
   - Type *Contoso* into the **Initial domain name** box.
   - Leave the *United States* option in the **Country or region** box.
5. Select **Create**.

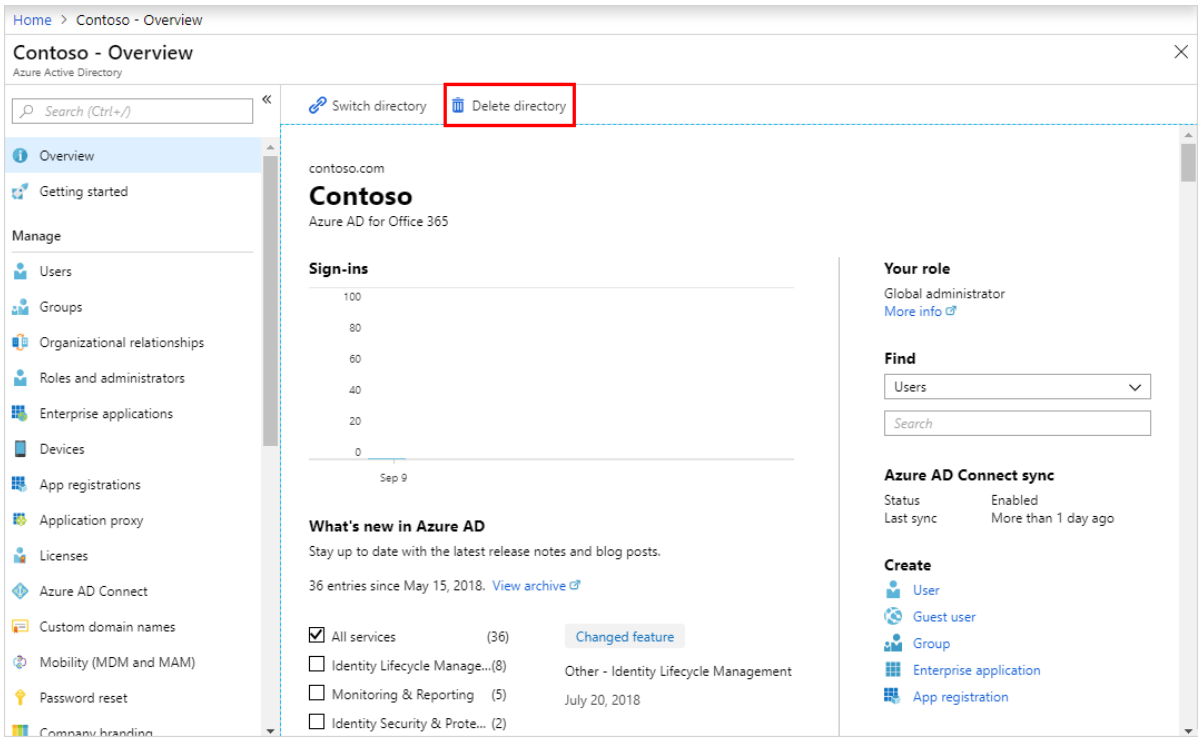
Your new tenant is created with the domain contoso.onmicrosoft.com.

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 are signed in to the directory that you want to delete through the **Directory + subscription** filter in the Azure Portal, and switching 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.



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 role-based access using Privileged Identity Management 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

12/17/2019 • 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.

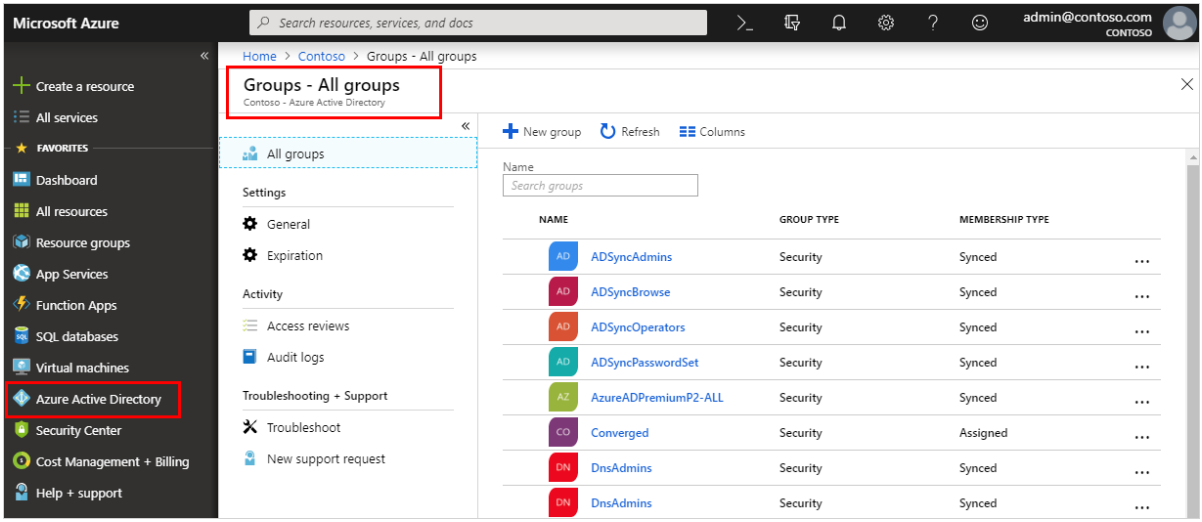
1. Select **Azure Active Directory** > **Groups**.
2. From the **Groups - All groups** page, search for and select the **MDM policy - West** group.
3. From the **MDM policy - West Overview** page, select **Members** from the **Manage** area.
4. Select **Add members**, and then search and select **Alain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

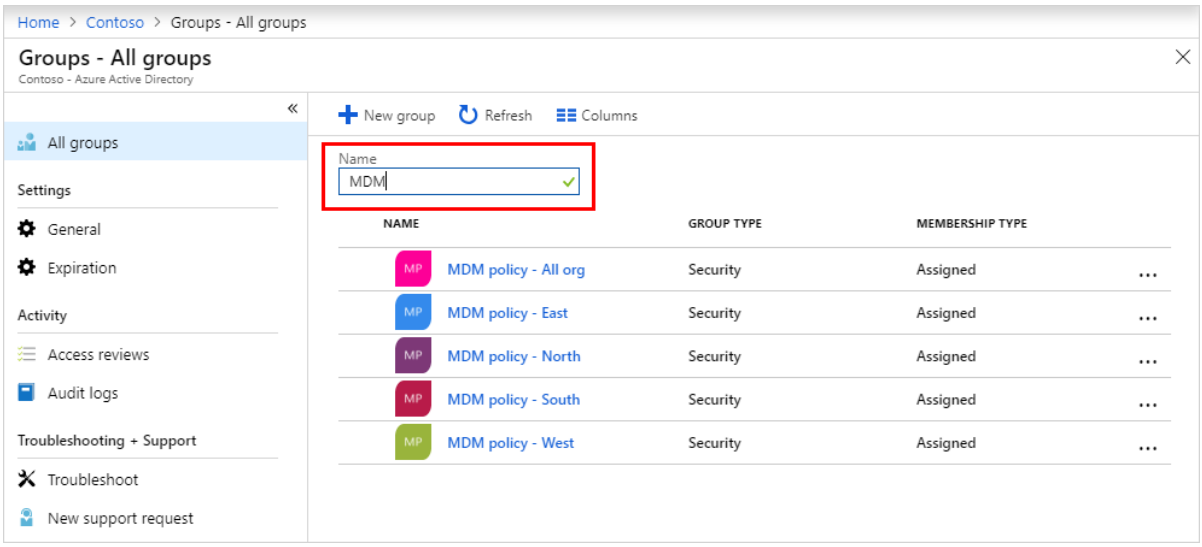


Search for the group

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

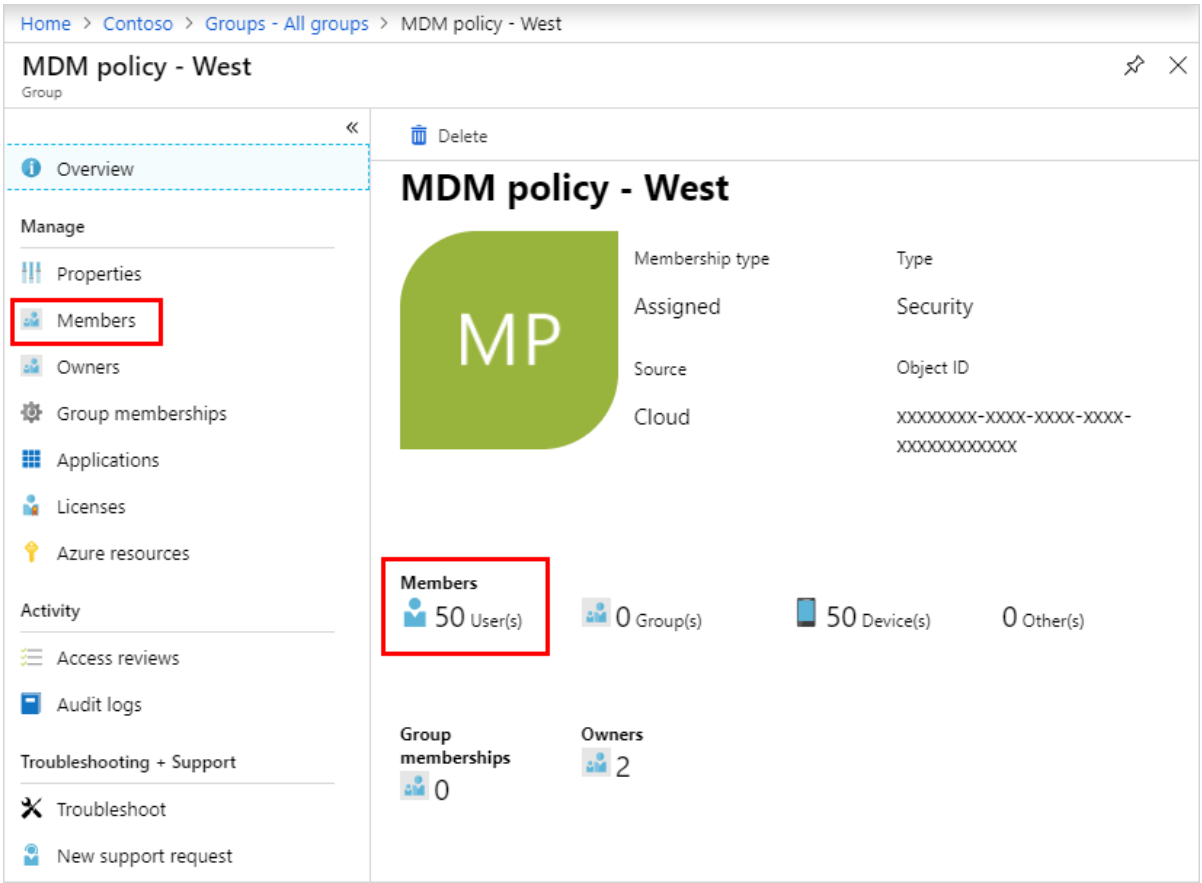
1. From the **Groups - All groups** page, type *MDM* into the **Search** box.

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



2. Select the group **MDM policy – West**.

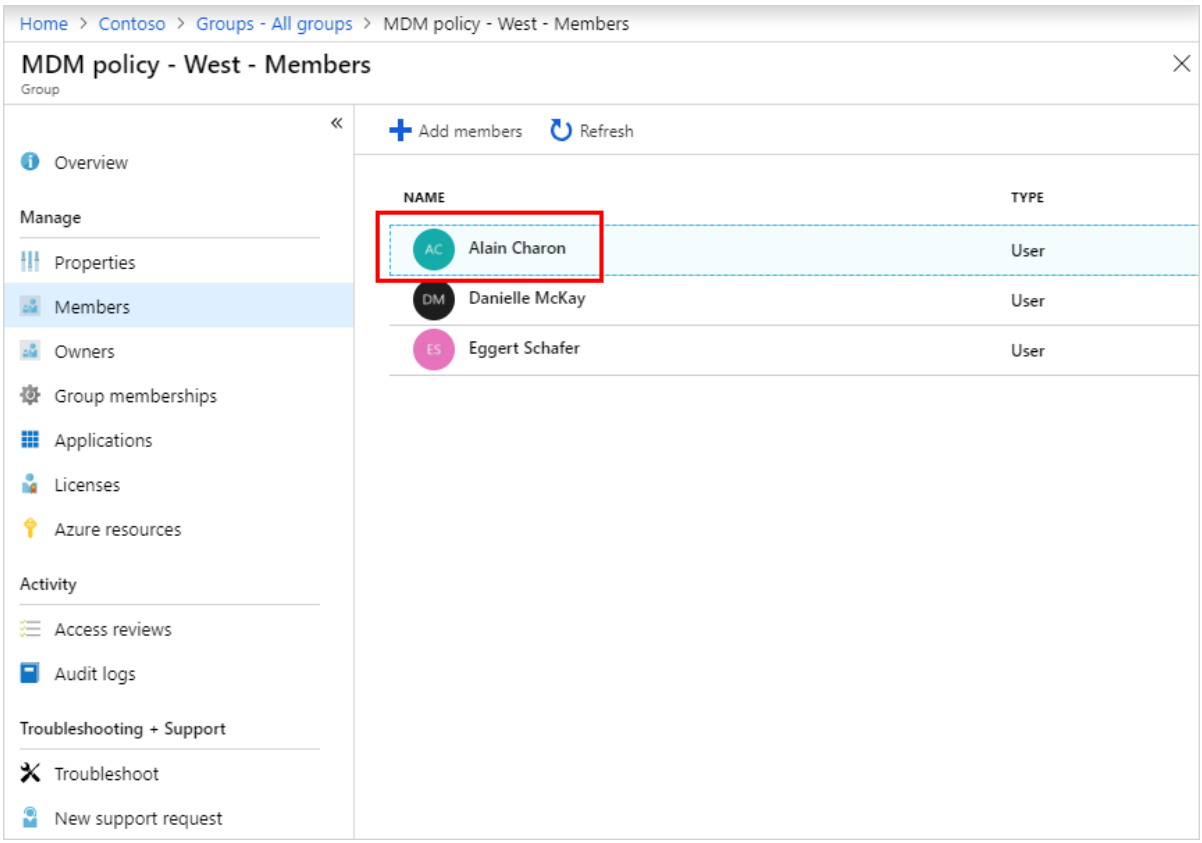
3. View the group info on the **MDM policy - West Overview** page, including the number of members of that group.



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*.



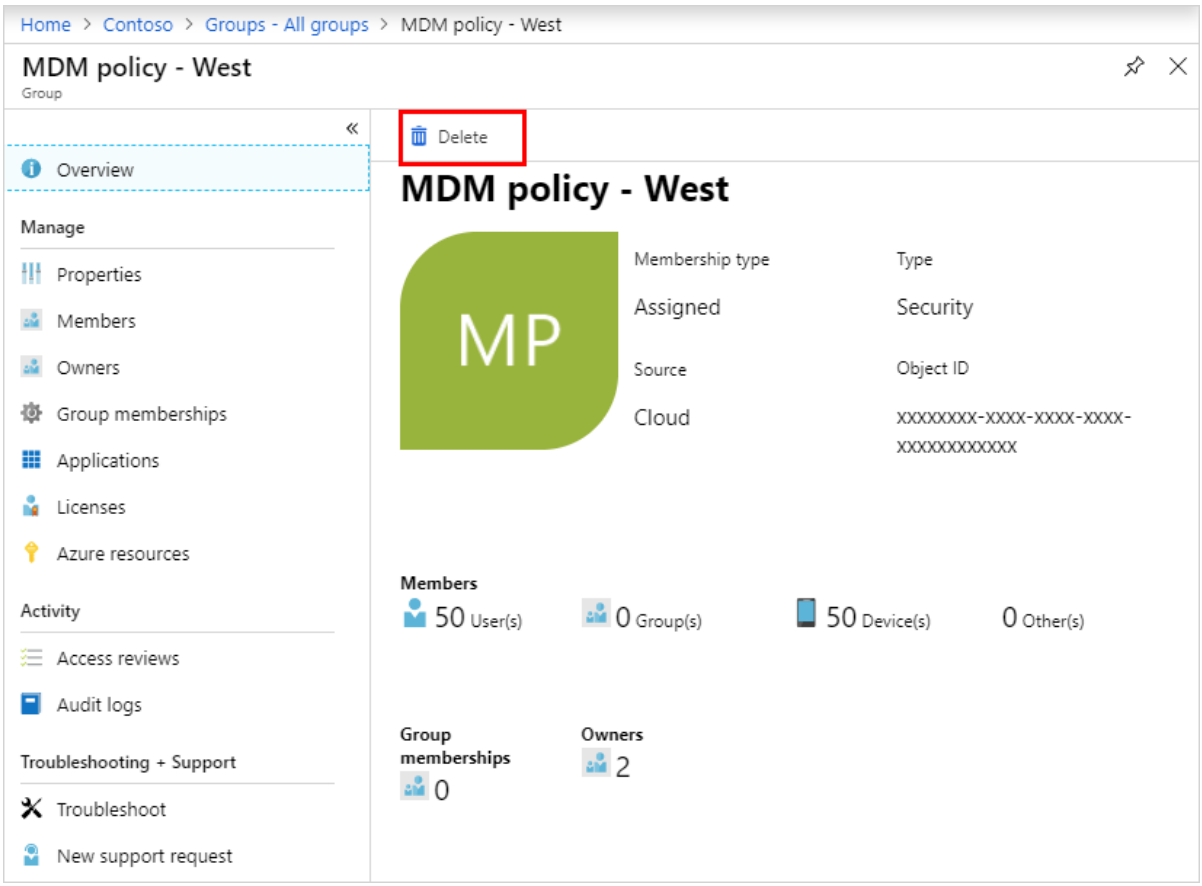
Clean up resources

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.



IMPORTANT

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

Next steps

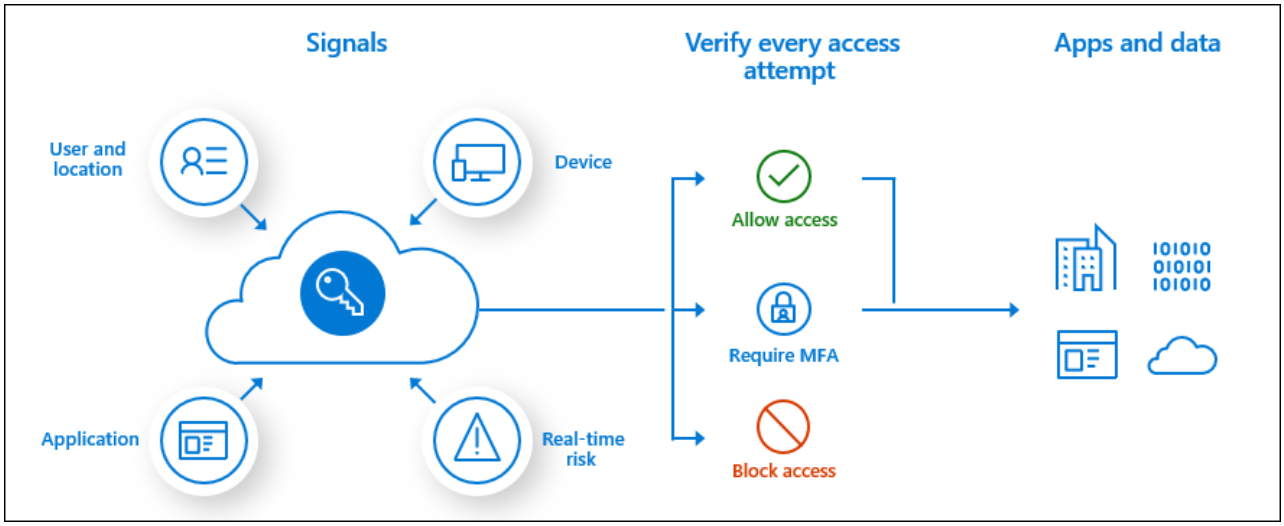
Advance to the next article to learn how to associate a subscription to your Azure AD directory.

Associate an Azure subscription

Overview of Azure Multi-Factor Authentication for your organization

7/20/2020 • 2 minutes to read • Edit Online

There are multiple ways to enable Azure 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 Office 365, there are two options:

- Azure 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 Office 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 Multi-Factor Authentication.

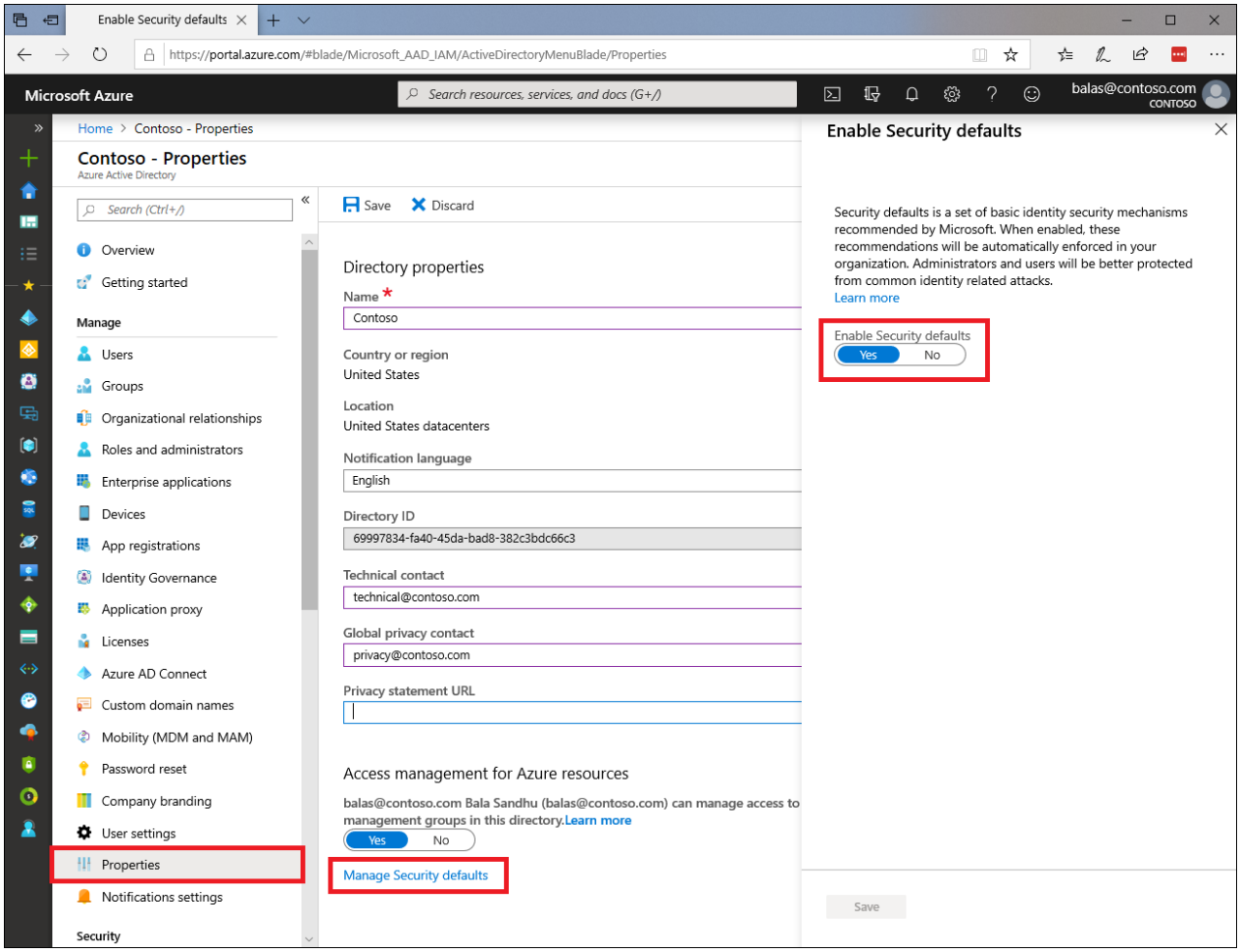
For more information on licensing, see Features and licenses for Azure Multi-Factor Authentication.

What are security defaults?

7/20/2020 • 7 minutes to read • Edit Online

Managing security can be difficult with common identity-related attacks like password spray, replay, and phishing are becoming more and 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 Multi-Factor Authentication.
- Requiring administrators to perform multi-factor authentication.
- Blocking legacy authentication protocols.
- Requiring users to perform multi-factor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.



More details on why security defaults are being made available can be found in Alex Weinert's blog post, Introducing security defaults.

Availability

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, it is possible security defaults are already enabled in your tenant. In an effort to protect all of our users, security defaults is being rolled out to all new tenants created.

Who's it for?

- If you are an organization that wants to increase your security posture but you don't know how or where to start, security defaults are for you.
- If you are an organization utilizing the free tier of Azure Active Directory licensing, security defaults are for you.

Who should use Conditional Access?

- If you are an organization currently using Conditional Access policies to bring signals together, to make decisions, and enforce organizational policies, security defaults are probably not right for you.
- If you are 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 Multi-Factor Authentication. Users have 14 days to register for Azure Multi-Factor Authentication by using the Microsoft Authenticator app. After the 14 days have passed, the user won't be able to 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. Due to 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.

After registration with Azure Multi-Factor Authentication is finished, the following nine Azure AD administrator roles will be required to perform additional authentication every time they sign in:

- Global administrator
- SharePoint administrator
- Exchange administrator
- Conditional Access administrator
- Security administrator
- Helpdesk administrator
- Billing administrator
- User administrator
- Authentication 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 on behalf of the original account holder. They can even download the entire directory to perform 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 additional authentication whenever necessary. 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 a variety of 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, the majority of compromising sign-in attempts come from legacy authentication. Legacy authentication does not 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 Office 365 and Microsoft 365

Protecting privileged actions

Organizations use a variety of 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 a variety of 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 additional authentication before you allow access.

After you enable security defaults in your tenant, any user who's accessing the Azure portal, Azure PowerShell, or the Azure CLI will need to complete additional authentication. This policy applies to all users who are accessing Azure Resource Manager, 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 additional considerations are related to deployment of security defaults.

Authentication methods

These free security defaults allow registration and use of Azure 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***

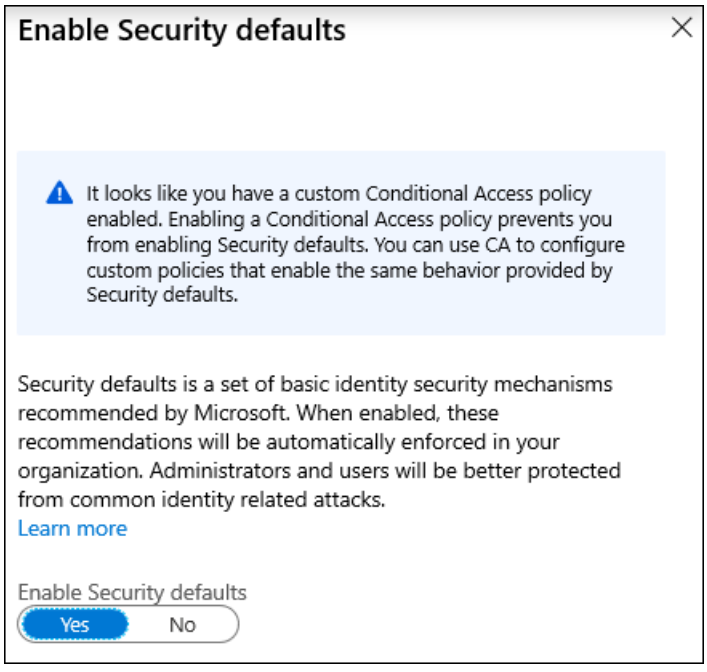
- ** Users may use verification codes from the Microsoft Authenticator app but can only register using the notification option.
- *** App passwords are only available in per-user MFA with legacy authentication scenarios only if enabled by administrators.

Disabled MFA status

If your organization is a previous user of per-user based Azure Multi-Factor Authentication, do not 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 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 are not 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. If you have a license that provides Conditional Access but don't have any Conditional Access policies enabled in your environment, you are welcome to use security defaults until you enable Conditional Access policies. More information about Azure AD licensing can be found on the Azure AD pricing page.



Here are step-by-step guides on how you can use Conditional Access to configure equivalent policies to those

policies enabled by security defaults:

- Require MFA for administrators
- Require MFA for Azure management
- Block legacy authentication
- Require MFA for all users
- Require Azure MFA registration - Requires Azure AD Identity Protection part of Azure AD Premium P2.

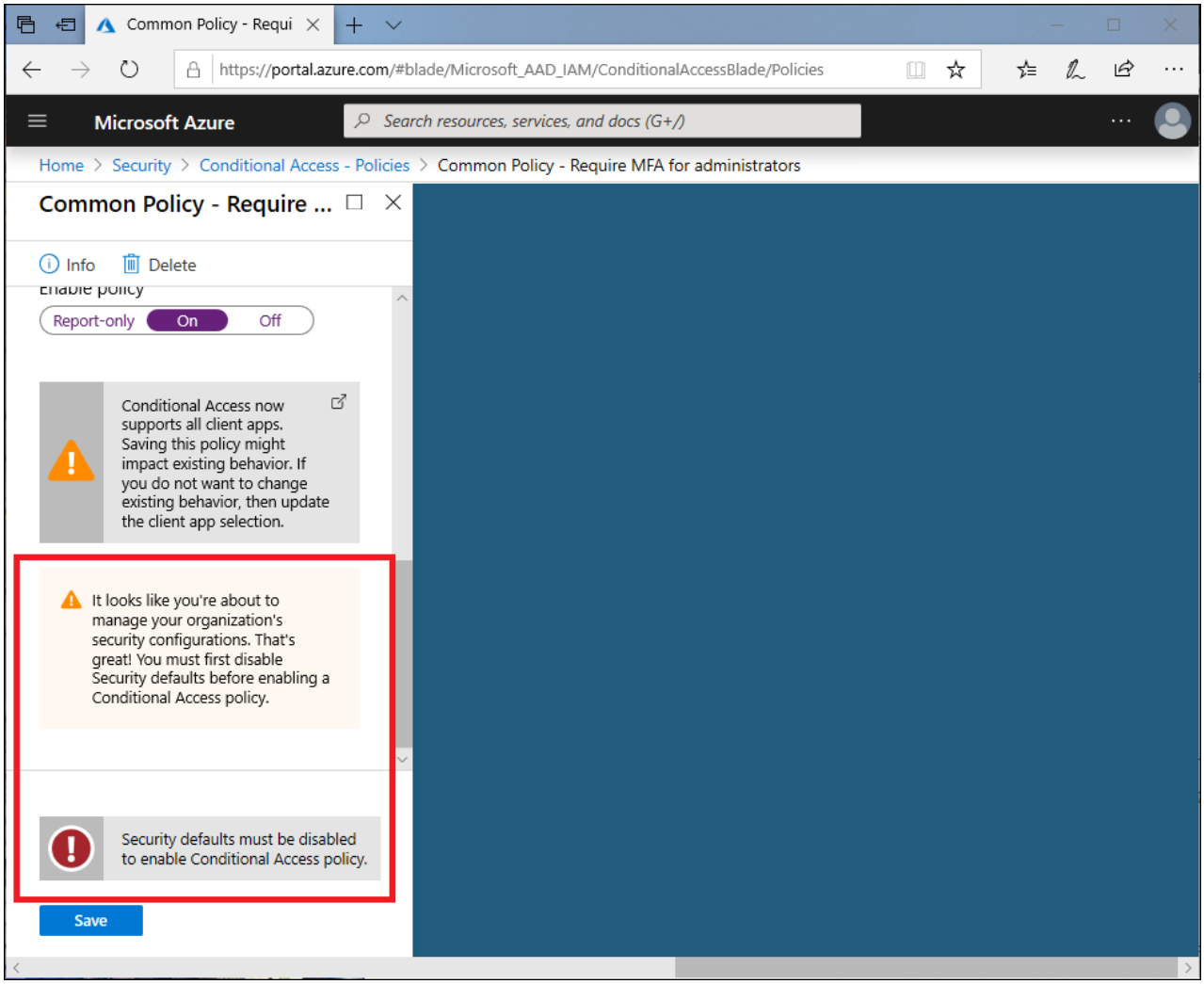
Enabling security defaults

To enable security defaults in your directory:

1. Sign in to theAzure portalas 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**.

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 theAzure portalas 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

7/20/2020 • 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.

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. TheClient Appcolumn or the Client App field under theBasic Infotab 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 theBaseline policy: block legacy authenticationfor 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 pre-requisites. 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

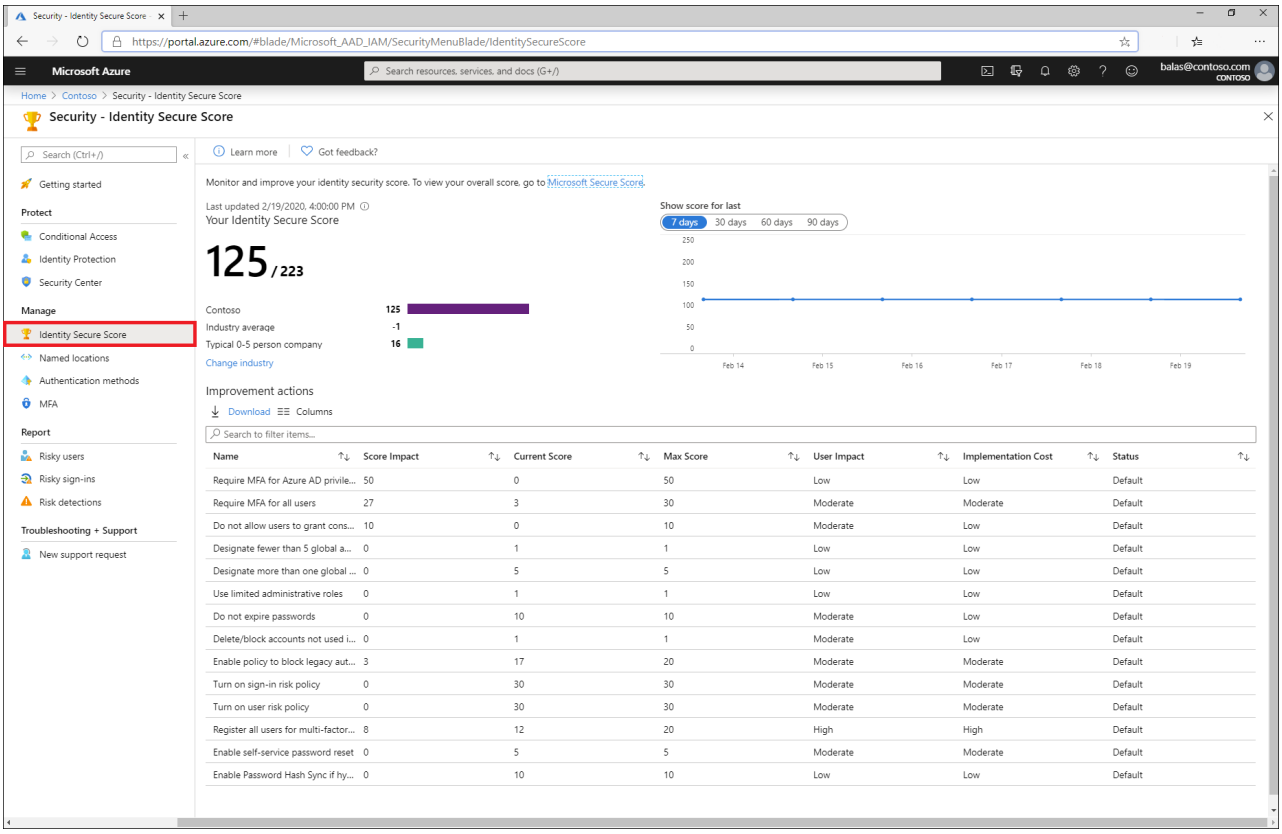
What is the identity secure score in Azure Active Directory?

2/21/2020 • 4 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 number between 1 and 223 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

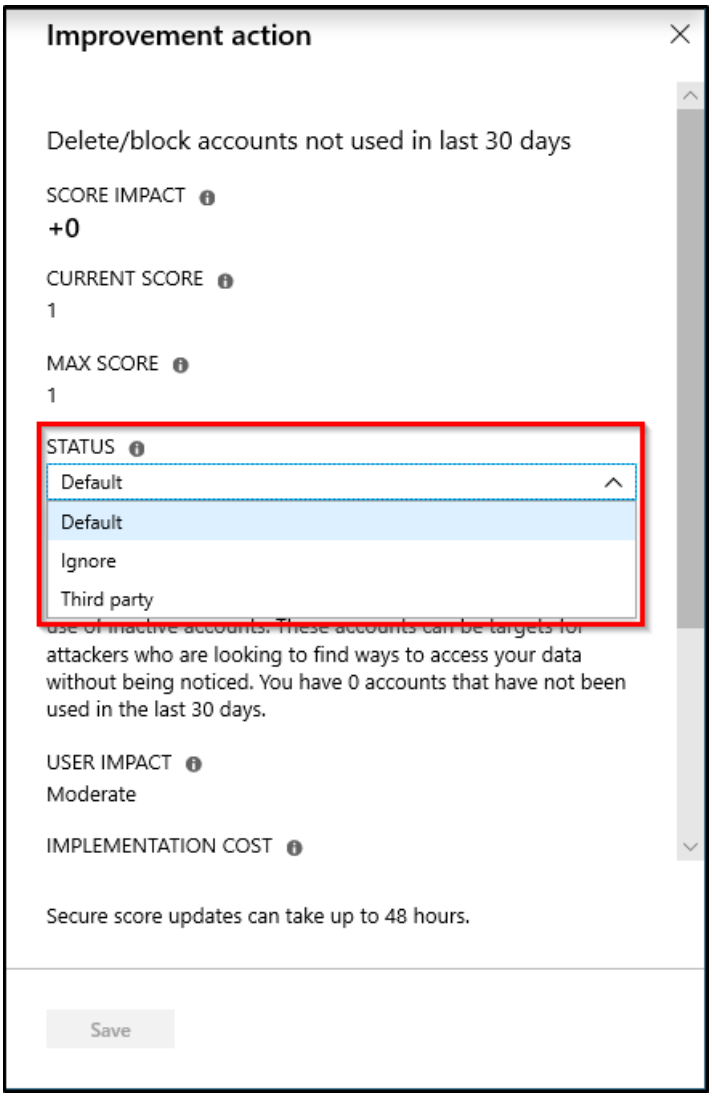
How do I get my secure score?

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.



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 30 points 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 2 points (5 protected / 100 total * 30 max pts = 2 pts 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 security center, 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?

You're given points 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 security center and review your overall Microsoft secure score. You can review changes to your overall secure score be 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 Office 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

4/28/2020 • 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 or Office 365 customers.

There are a number of recommendations that Azure AD Free or Office 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 (O365 E1, E3, E5, F1, A1, A3, A5)
- Office 365 Business (Essentials, Business, Business Premium)
- Microsoft 365 (M365 Business, 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 MFA and SSPR to simplify user registration experience	Allow your users to register from one common experience for both Azure 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	MFA for admins to protect accounts that are assigned administrative rights. Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols. MFA for all users and applications to create a balanced MFA policy for your environment, securing your users and applications. Require MFA for Azure Management to protect your privileged resources by requiring multi-factor authentication for any user accessing Azure resources.
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 MFA and SSPR to simplify user registration experience	Allow your users to register from one common experience for both Azure 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 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.
Create and enable Conditional Access policies	MFA for admins to protect accounts that are assigned administrative rights. Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols. Require MFA for Azure Management to protect your privileged resources by requiring multi-factor authentication for any user accessing Azure resources.
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

Continuous access evaluation

7/20/2020 • 5 minutes to read • Edit Online

Microsoft services, like Azure Active Directory (Azure AD) and Office 365, use open standards and protocols to maximize interoperability. One of the most critical ones is Open ID Connect (OIDC). When a client application like Outlook connects to a service like Exchange Online, the API requests are authorized using OAuth 2.0 access tokens. By default, those access tokens are valid for one hour. When they expire, the client is redirected back to Azure AD to refresh them. That also provides an opportunity to reevaluate policies for user access – we might choose not to refresh the token because of a Conditional Access policy, or because the user has been disabled in the directory.

Token expiration and refresh is a standard mechanism in the industry. That said, customers have expressed concerns about the lag between when risk conditions change for the user (for example: moving from the corporate office to the local coffee shop, or user credentials discovered on the black market) and when policies can be enforced related to that change. We have experimented with the "blunt object" approach of reduced token lifetimes but found they can degrade user experiences and reliability without eliminating risks.

Timely response to policy violations or security issues really requires a "conversation" between the token issuer, like Azure AD, and the relying party, like Exchange Online. This two-way conversation gives us two important capabilities. The relying party can notice when things have changed, like a client coming from a new location, and tell the token issuer. It also gives the token issuer a way to tell the relying party to stop respecting tokens for a given user due to account compromise, disablement, or other concerns. The mechanism for this conversation is Continuous Access Evaluation (CAE).

Microsoft has been an early participant in the Continuous Access Evaluation Protocol (CAEP) initiative as part of the Shared Signals and Events working group at the OpenID Foundation. Identity providers and relying parties will be able to leverage the security events and signals defined by the working group to reauthorize or terminate access. It is exciting work and will improve security across many platforms and applications.

Because the security benefits are so great, we are rolling out a Microsoft-specific initial implementation in parallel to our continued work within the standards bodies. As we work to deploy these continuous access evaluation (CAE) capabilities across Microsoft services, we have learned a lot and are sharing this information with the standards community. We hope our experience in deployment can help inform an even better industry standard and are committed to implementing that standard once ratified, allowing all participating services to benefit.

How does CAE work in Microsoft services?

We are focusing our initial implementation of continuous access evaluation to Exchange and Teams. We hope to expand support to other Microsoft services in the future. We will start to enable continuous access evaluation only for tenants with no Conditional Access policies. We will use our learnings from this phase of CAE to inform our ongoing rollout of CAE.

Service side requirements

Continuous access evaluation is implemented by enabling services (resource providers) to subscribe to critical events in Azure AD so that those events can be evaluated and enforced near real time. The following events will be enforced in this initial CAE rollout:

- User Account is deleted or disabled
- Password for a user is changed or reset
- MFA is enabled for the user
- Admin explicitly revokes all refresh tokens for a user

- Elevated user risk detected by Azure AD Identity Protection

In the future we hope to add more events, including events like location and device state changes. **While our goal is for enforcement to be instant, in some cases latency of up to 15 minutes may be observed due to event propagation time**.

Client-side claim challenge

Before continuous access evaluation, clients would always try to replay the access token from its cache as long as it was not expired. With CAE, we are introducing a new case that a resource provider can reject a token even when it is not expired. In order to inform clients to bypass their cache even though the cached tokens have not expired, we introduce a mechanism called **claim challenge**. CAE requires a client update to understand claim challenge. The latest version of the following applications below support claim challenge:

- Outlook for Windows
- Outlook for iOS
- Outlook for Android
- Outlook for Mac
- Teams for Windows
- Teams for iOS
- Teams for Android
- Teams for Mac

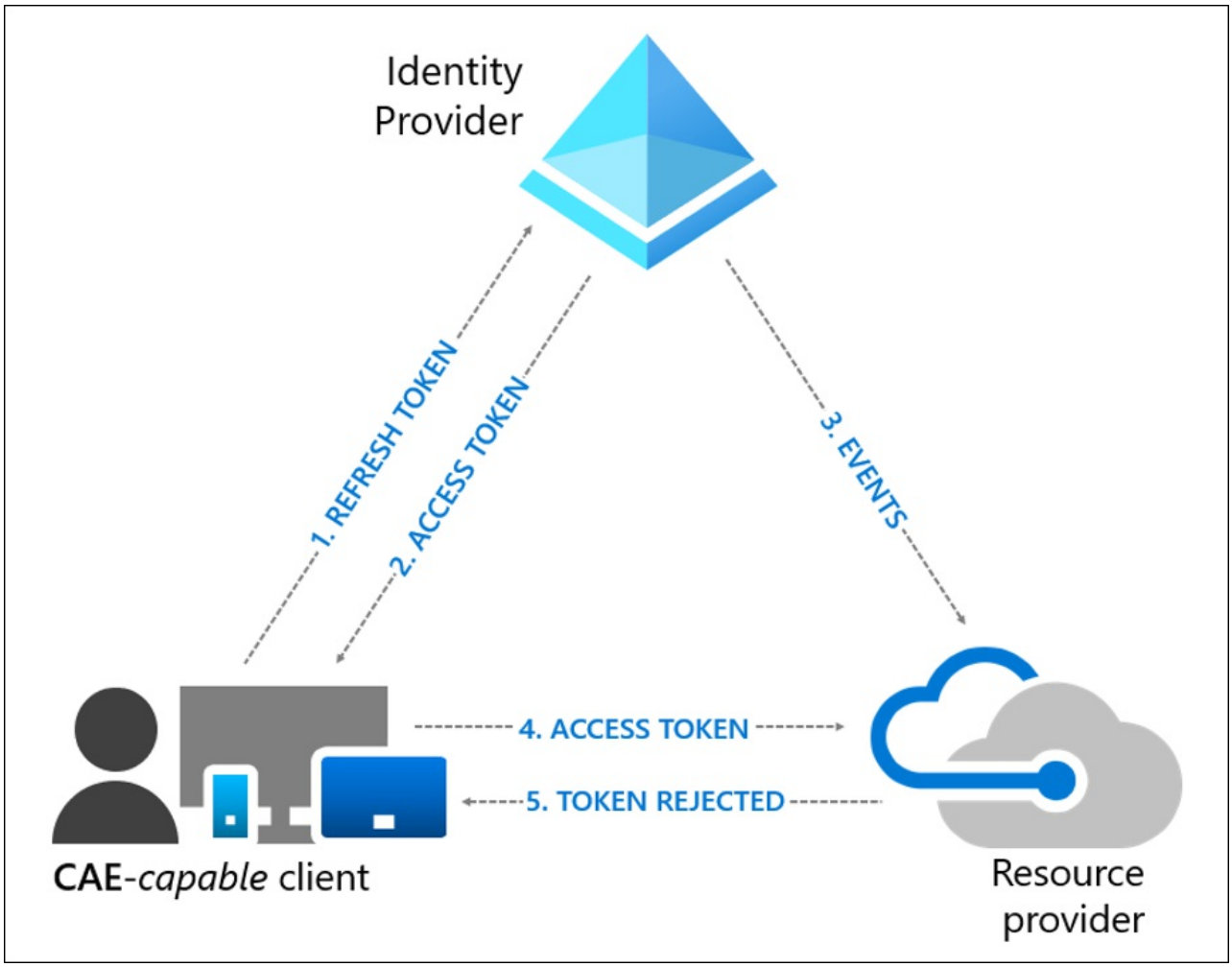
Token Lifetime

Because risk and policy are evaluated in real time, clients that negotiate continuous access evaluation aware sessions will rely on CAE instead of existing static access token lifetime policies, which means that configurable token lifetime policy will not be honored anymore for CAE-capable clients that negotiate CAE-aware sessions.

We will increase access token lifetime to 24 hours in CAE sessions. Revocation is driven by critical events and policy evaluation, not an arbitrary time period. This change increases the stability of your applications without affecting your security posture.

Example flows

User revocation event flow:



1. A CAE-capable client presents credentials or a refresh token to AAD asking for an access token for some resource.
2. An access token is returned along with other artifacts to the client.
3. An Administrator explicitly revokes all refresh tokens for the user. A revocation event will be sent to the resource provider from Azure AD.
4. An access token is presented to the resource provider. The resource provider evaluates the validity of the token and checks whether there is any revocation event for the user. The resource provider uses this information to decide to grant access to the resource or not.
5. In this case, the resource provider denies access, and sends a 401+ claim challenge back to the client
6. The CAE-capable client understands the 401+ claim challenge. It bypasses the caches and goes back to step 1, sending its refresh token along with the claim challenge back to Azure AD. Azure AD will then reevaluate all the conditions and prompt the user to reauthenticate in this case.

FAQs

What is the lifetime of my Access Token?

If you are not using CAE-capable clients, your default Access Token lifetime will still be 1 hour unless you have configured your Access Token lifetime with the Configurable Token Lifetime (CTL) preview feature.

If you are using CAE-capable clients that negotiate CAE-aware sessions, your CTL settings for Access Token lifetime will be overwritten and Access Token lifetime will be 24 hours.

How quick is enforcement?

While our goal is for enforcement to be instant, in some cases latency of up to 15 minutes may be observed due to event propagation time.

How will CAE work with Sign-in Frequency?

Sign-in Frequency will be honored with or without CAE.

Next steps

Announcing continuous access evaluation

Manage app and resource access using Azure Active Directory groups

4/8/2020 • 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.

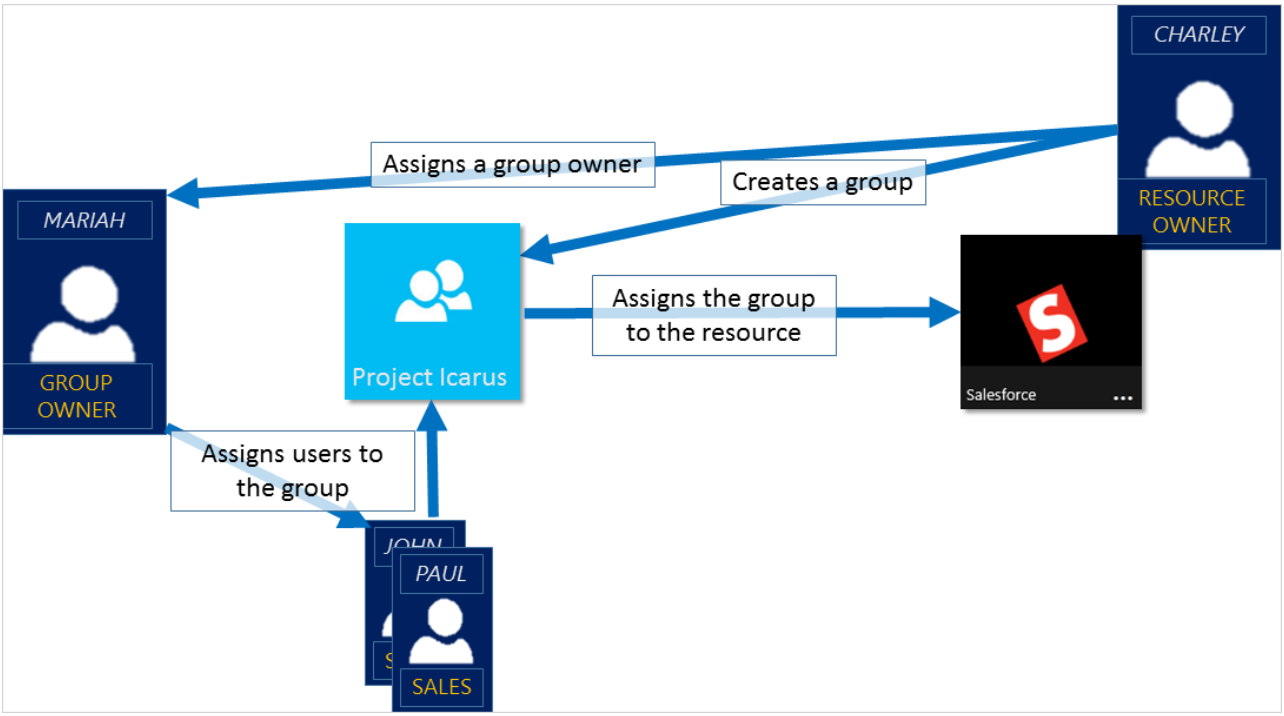
NOTE

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



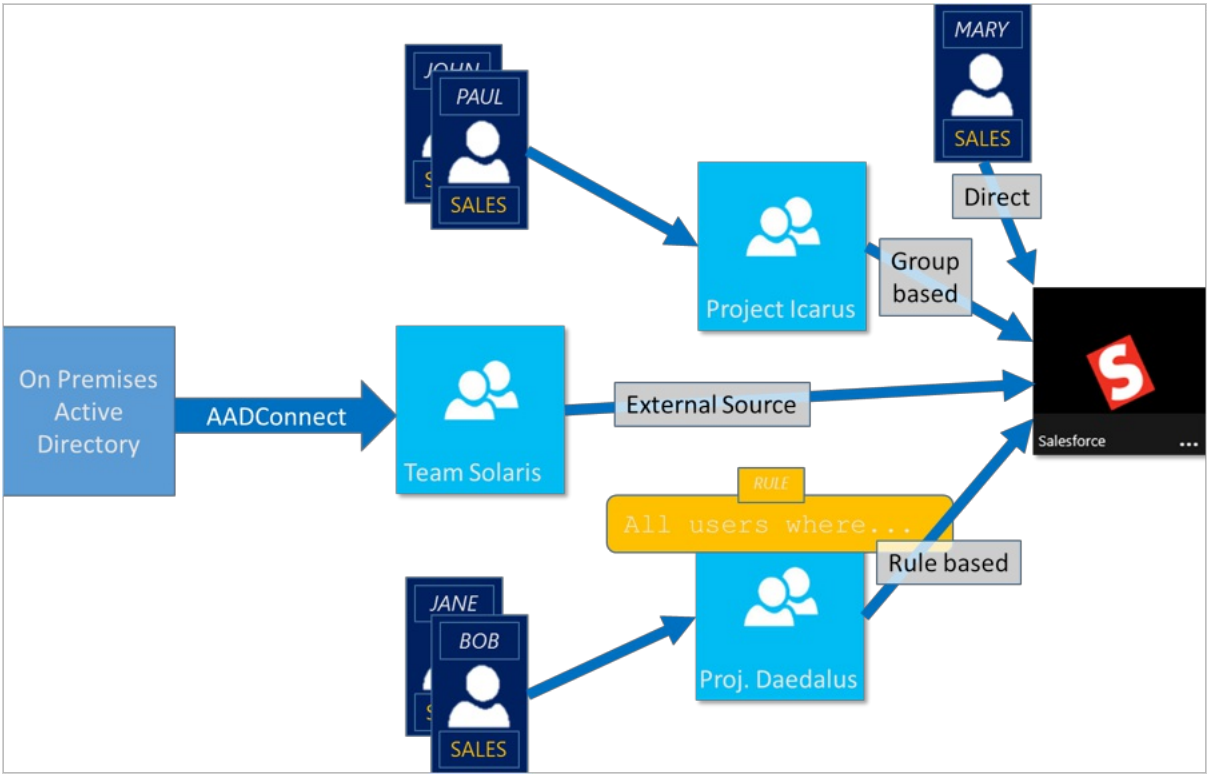
Ways to assign access rights

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 the resource. For more information, see Create a dynamic group and check status.

  You can also Watch this short video for a quick explanation about creating and using dynamic groups:

- **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?

2/21/2020 • 3 minutes to read • Edit Online

Microsoft paid cloud services, such as Office 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 to use group-based licensing:

- Paid or trial subscription for Azure AD Premium P1 and above
- Paid or trial edition of 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 Office 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 Office 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?

3/27/2020 • 8 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 contains a comparison of 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 received depends on whether the user is a native member of the tenant (member user) or if the user is brought over from another directory as a B2B collaboration guest (guest user). See What is Azure AD B2B collaboration? for more information about adding guest users.

- Member users can register applications, manage their own profile photo and mobile phone number, change their own password, and invite B2B guests. In addition, users can read all directory information (with a few exceptions).
- Guest users have restricted directory permissions. For example, guest users cannot browse information from the tenant beyond their own profile information. However, a guest user can retrieve information about another user by providing the User Principal Name or objectId. A guest user can read properties of groups they belong to, including group membership, regardless of the **Guest users permissions are limited** setting. A guest cannot view information about any other tenant objects.

Default permissions for guests are restrictive by default. Guests can be added to administrator roles, which grant them full read and write permissions contained in the role. There is one additional restriction available, the ability for guests to invite other guests. Setting **Guests can invite** to **No** prevents guests from inviting other guests. See Delegate invitations for B2B collaboration to learn how. To grant guest users the same permissions as member users by default, set **Guest users permissions are limited** to **No**. This setting grants all member user permissions to guest users by default, as well as to allow guests to be added to administrative roles.

Compare member and guest default permissions

AREA	MEMBER USER PERMISSIONS	GUEST USER PERMISSIONS
Users and contacts	Read all public properties of users and contacts Invite guests Change own password Manage own mobile phone number Manage own photo Invalidate own refresh tokens	Read own properties Read display name, email, sign in name, photo, user principal name, and user type properties of other users and contacts Change own password

AREA	MEMBER USER PERMISSIONS	GUEST USER PERMISSIONS
Groups	Create security groups Create Office 365 groups Read all properties of groups Read non-hidden group memberships Read hidden Office 365 group memberships for joined group Manage properties, ownership, and membership of groups the user owns Add guests to owned groups Manage dynamic membership settings Delete owned groups Restore owned Office 365 groups	Read all properties of groups Read non-hidden group memberships Read hidden Office 365 group memberships for joined groups Manage owned groups Add guests to owned groups (if allowed) Delete owned groups Restore owned Office 365 groups Read properties of groups they belong to, including membership.
Applications	Register (create) new application Read properties of registered and enterprise applications Manage application properties, assignments, and credentials for owned applications Create or delete application password for user Delete owned applications Restore owned applications	Read properties of registered and enterprise applications Manage application properties, assignments, and credentials for owned applications Delete owned applications Restore owned applications
Devices	Read all properties of devices Manage all properties of owned devices	No permissions Delete owned devices
Directory	Read all company information Read all domains Read all partner contracts	Read display name and verified domains
Roles and Scopes	Read all administrative roles and memberships Read all properties and membership of administrative units	No permissions
Subscriptions	Read all subscriptions Enable Service Plan Member	No permissions
Policies	Read all properties of policies Manage all properties of owned policy	No permissions

To restrict the default permissions for member users

Default permissions for member users can be restricted in the following ways.

PERMISSION	SETTING EXPLANATION
Users can register application	Setting this option to No prevents users from creating application registrations. The ability can then be granted 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.
Ability to create security groups	Setting this option to No prevents users from creating security groups. Global administrators and User administrators can still create security groups. See Azure Active Directory cmdlets for configuring group settings to learn how.
Ability to create Office 365 groups	Setting this option to No prevents users from creating Office 365 groups. Setting this option to Some allows a select set of users to create Office 365 groups. Global administrators and User administrators will still be able to create Office 365 groups. See Azure Active Directory cmdlets for configuring group settings to learn how.
Restrict access to Azure AD administration portal	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. Important to note: this setting does not restrict access to Azure AD data using PowerShell or other clients such as Visual Studio. When set 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 Readers role. This role allows reading basic directory information, which member users have by default (guests and service principals do not).
Ability to read other users	This setting is available in PowerShell only. Setting this flag to $false 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. This setting is meant for special circumstances, and setting this flag to $false is not recommended.

Object ownership

Application registration owner permissions

When a user registers an application, they are 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 the app requests. They can also manage the tenant-specific configuration of the application, such as the SSO configuration and user assignments. An owner can also add or remove other owners. Unlike Global Administrators, owners can only manage applications they own.

Enterprise application owner permissions

When a user adds a new enterprise application, they are 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 they own.

Group owner permissions

When a user creates a group, they are automatically added as an owner for that group. As an owner, they can manage properties of the group such as the name, as well as manage group membership. An owner can also add or remove other owners. Unlike Global administrators and User administrators, owners can only manage groups

they own. To assign a group owner, see Managing owners for a group.

Ownership Permissions

The following tables describe the specific permissions in Azure Active Directory member users have over owned objects. The user only has these permissions on objects they own.

Owned application registrations

Users can perform the following actions on owned application registrations.

ACTIONS	DESCRIPTION
microsoft.directory/applications/audience/update	Update applications.audience property in Azure Active Directory.
microsoft.directory/applications/authentication/update	Update applications.authentication property in Azure Active Directory.
microsoft.directory/applications/basic/update	Update basic properties on applications in Azure Active Directory.
microsoft.directory/applications/credentials/update	Update applications.credentials property in Azure Active Directory.
microsoft.directory/applications/delete	Delete applications in Azure Active Directory.
microsoft.directory/applications/owners/update	Update applications.owners property in Azure Active Directory.
microsoft.directory/applications/permissions/update	Update applications.permissions property in Azure Active Directory.
microsoft.directory/applications/policies/update	Update applications.policies property in Azure Active Directory.
microsoft.directory/applications/restore	Restore applications in Azure Active Directory.

Owned enterprise applications

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

ACTIONS	DESCRIPTION
microsoft.directory/auditLogs/allProperties/read	Read all properties (including privileged properties) on auditLogs in Azure Active Directory.
microsoft.directory/policies/basic/update	Update basic properties on policies in Azure Active Directory.
microsoft.directory/policies/delete	Delete policies in Azure Active Directory.
microsoft.directory/policies/owners/update	Update policies.owners property in Azure Active Directory.
microsoft.directory/servicePrincipals/appRoleAssignedTo/update	Update servicePrincipals.appRoleAssignedTo property in Azure Active Directory.

ACTIONS	DESCRIPTION
microsoft.directory/servicePrincipals/appRoleAssignments/update	Update users.appRoleAssignments property in Azure Active Directory.
microsoft.directory/servicePrincipals/audience/update	Update servicePrincipals.audience property in Azure Active Directory.
microsoft.directory/servicePrincipals/authentication/update	Update servicePrincipals.authentication property in Azure Active Directory.
microsoft.directory/servicePrincipals/basic/update	Update basic properties on servicePrincipals in Azure Active Directory.
microsoft.directory/servicePrincipals/credentials/update	Update servicePrincipals.credentials property in Azure Active Directory.
microsoft.directory/servicePrincipals/delete	Delete servicePrincipals in Azure Active Directory.
microsoft.directory/servicePrincipals/owners/update	Update servicePrincipals.owners property in Azure Active Directory.
microsoft.directory/servicePrincipals/permissions/update	Update servicePrincipals.permissions property in Azure Active Directory.
microsoft.directory/servicePrincipals/policies/update	Update servicePrincipals.policies property in Azure Active Directory.
microsoft.directory/signInReports/allProperties/read	Read all properties (including privileged properties) on signInReports in Azure Active Directory.

Owned devices

Users can perform the following actions on owned devices.

ACTIONS	DESCRIPTION
microsoft.directory/devices/bitLockerRecoveryKeys/read	Read devices.bitLockerRecoveryKeys property in Azure Active Directory.
microsoft.directory/devices/disable	Disable devices in Azure Active Directory.

Owned groups

Users can perform the following actions on owned groups.

ACTIONS	DESCRIPTION
microsoft.directory/groups/appRoleAssignments/update	Update groups.appRoleAssignments property in Azure Active Directory.
microsoft.directory/groups/basic/update	Update basic properties on groups in Azure Active Directory.
microsoft.directory/groups/delete	Delete groups in Azure Active Directory.
microsoft.directory/groups/dynamicMembershipRule/update	Update groups.dynamicMembershipRule property in Azure Active Directory.

ACTIONS	DESCRIPTION
microsoft.directory/groups/members/update	Update groups.members property in Azure Active Directory.
microsoft.directory/groups/owners/update	Update groups.owners property in Azure Active Directory.
microsoft.directory/groups/restore	Restore groups in Azure Active Directory.
microsoft.directory/groups/settings/update	Update groups.settings property in Azure Active Directory.

Next steps

- 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 Active Directory relates to your Azure subscription, see How Azure subscriptions are associated with Azure Active Directory
- Manage users

What is the Azure Active Directory architecture?

2/14/2020 • 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.

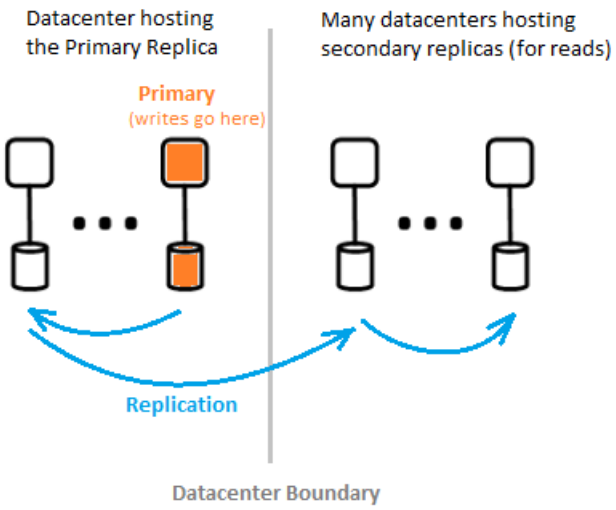
The following architecture elements are covered in this article:

- 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.

Backup protection

The directory implements soft deletes, instead of hard deletes, for users and tenants for easy recovery in case of accidental deletes by a customer. If your tenant administrator accidental deletes users, they can easily undo and restore the deleted users.

Azure AD implements daily backups of all data, and therefore can authoritatively restore data in case of any logical deletions or corruptions. The data tier employs error correcting codes, so that it can check for errors and automatically correct particular types of disk errors.

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

Azure Active Directory developer's guide

Azure Active Directory feature deployment guide

7/20/2020 • 6 minutes to read • Edit Online

It can seem daunting 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 are 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 are to Microsoft best practices. Check your secure score before and after implementing these recommendations to see how well you are 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 B2B licensing guidance

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
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.	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.	
Create an organization specific custom banned password list	Prevent users from creating passwords that include common words or phrases from your organization or area.	
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	
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 perform 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 converged registration for self-service password reset and Azure AD Multi-Factor Authentication (preview)	Allow your users to register from one common experience for both Azure 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 additional 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.	
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 B2B licensing guidance
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.	

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 designated 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.	
Implement group based application provisioning	Use group-based access management provisioning to automatically provision users for SaaS applications.	
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.	

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

7/20/2020 • 5 minutes to read • Edit Online

Looking for end-to-end 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.

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 theplan 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 a capability on 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 out to your organization as a whole.

In your first wave, target IT, usability, and other appropriate users who can test and provide feedback. This feedback should be used 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).

Deploy authentication

CAPABILITY	DESCRIPTION
Multi-Factor Authentication	Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution. Using admin-approved authentication methods, Azure MFA helps safeguard access to your data and applications while meeting the demand for a simple sign-in process.
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 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.
Access panel	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.
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
ADFS to Password Hash Sync	With Password Hash Synchronization, hashes of user passwords are synchronized from on-premises Active Directory to Azure AD, letting Azure AD authenticate users with no interaction with the on-premises Active Directory
ADFS to Pass Through Authentication	Azure AD Pass-through Authentication helps your users sign in to both on-premises and cloud-based applications using the same passwords. This feature provides users with a better experience - one less password to remember - and reduces IT helpdesk costs because users are less likely to forget how to sign in. When people sign in using Azure AD, this feature validates users' passwords directly against your on-premises Active Directory.
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 additional 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.

Identity data storage for European customers in Azure Active Directory

12/17/2019 • 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 subscribing for a Microsoft Online service such as Office 365 and Azure. For information on where your identity data is stored, you can use the Where is your data 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 multi-factor authentication (MFA)

- All two-factor authentication using phone calls or SMS originate from US datacenters and are also routed by global providers.
- Push notifications using the Microsoft Authenticator app originate from US datacenters. In addition, device vendor specific services may also come into play and these services maybe outside Europe.
- OATH codes are always validated in the U.S.

For more information about what user information is collected by Azure Multi-Factor Authentication Server (MFA Server) and cloud-based Azure MFA, see Azure Multi-Factor Authentication user data collection.

Microsoft Azure Active Directory B2C (Azure AD B2C)

Azure AD B2C policy configuration data and Key Containers are stored in U.S. datacenters. These do not contain any user personal data. For more info about policy configurations, see the Azure Active Directory B2C: Built-in policies article.

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.

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 is your data 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

Identity data storage for Australian customers in Azure Active Directory

7/20/2020 • 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 subscribing for a Microsoft Online service such as Office 365 and Azure. For information on where your Identity Customer Data is stored, you can use the Where is your data located? section of the Microsoft Trust Center.

> **NOTE**
>
> Services and applications that integrate with Azure AD have access to Identity Customer Data. Evaluate each service and application you use to determine how Identity Customer 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 is your data located? section of the Microsoft Trust Center.

For customers who provided an address in Australia and New Zealand and uses Azure AD free edition, Azure AD keeps PII data at rest within Australian datacenters.

All other Azure AD premium services store customer data in global datacenters. To locate the datacenter for a service, see Azure Active Directory – Where is your data located?

Microsoft Azure multi-factor authentication (MFA)

MFA service in Azure AD stores Identity Customer Data in global datacenters at rest. To learn more about the user information collected and stored by cloud-based Azure MFA and Azure MFA Server, see Azure Multi-Factor Authentication user data collection. If customers use MFA their data will be stored outside of Australia datacenters at rest.

Next steps

For more information about any of the features and functionality described above, see these articles:

- What is Multi-Factor Authentication?

Azure Active Directory operations reference guide

11/26/2019 • 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

3/13/2020 • 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 Office 365 licenses	Productivity Team
Decide who gets other licenses, for example, Dynamics, VSO	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.

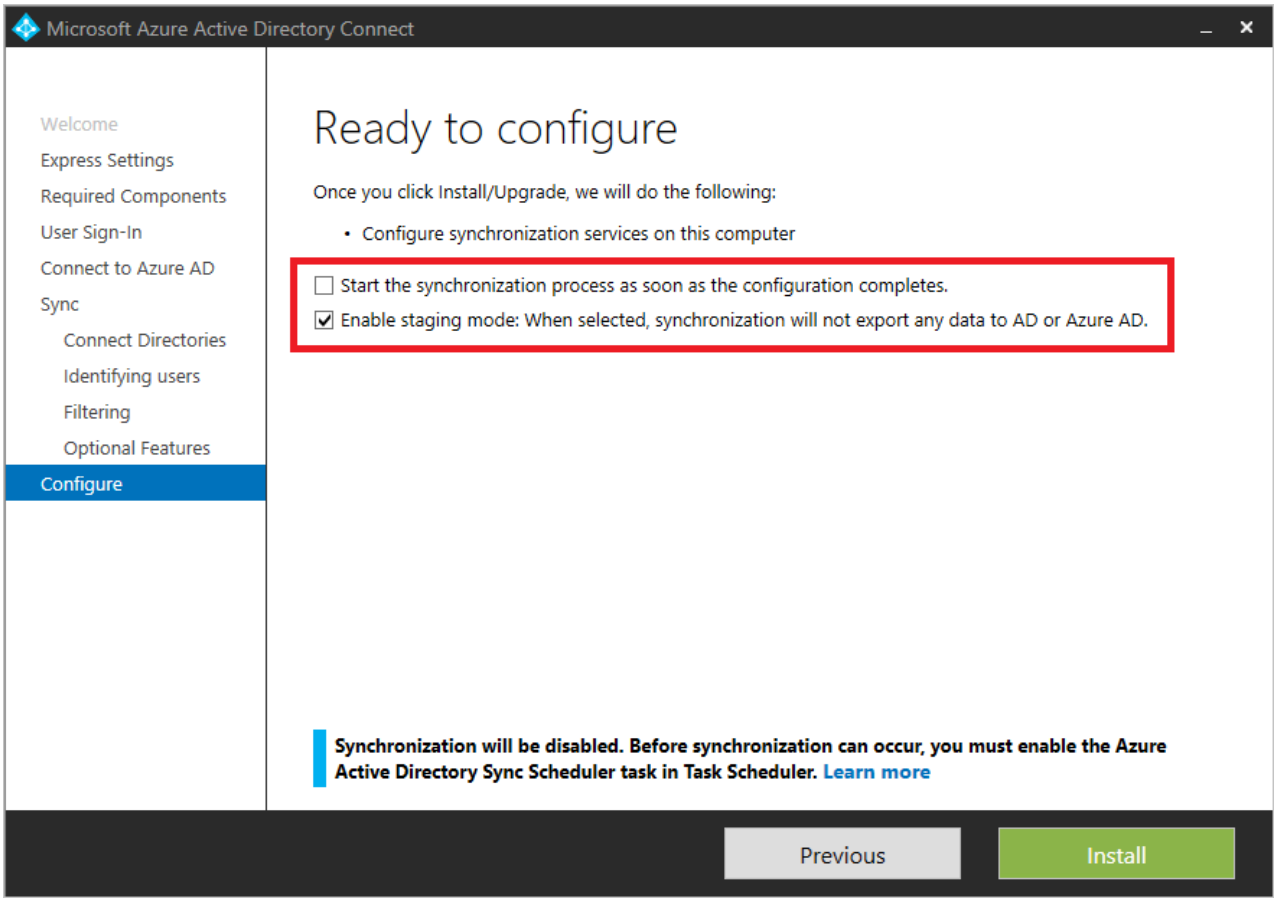
Sync failover or disaster recovery

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 office 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.

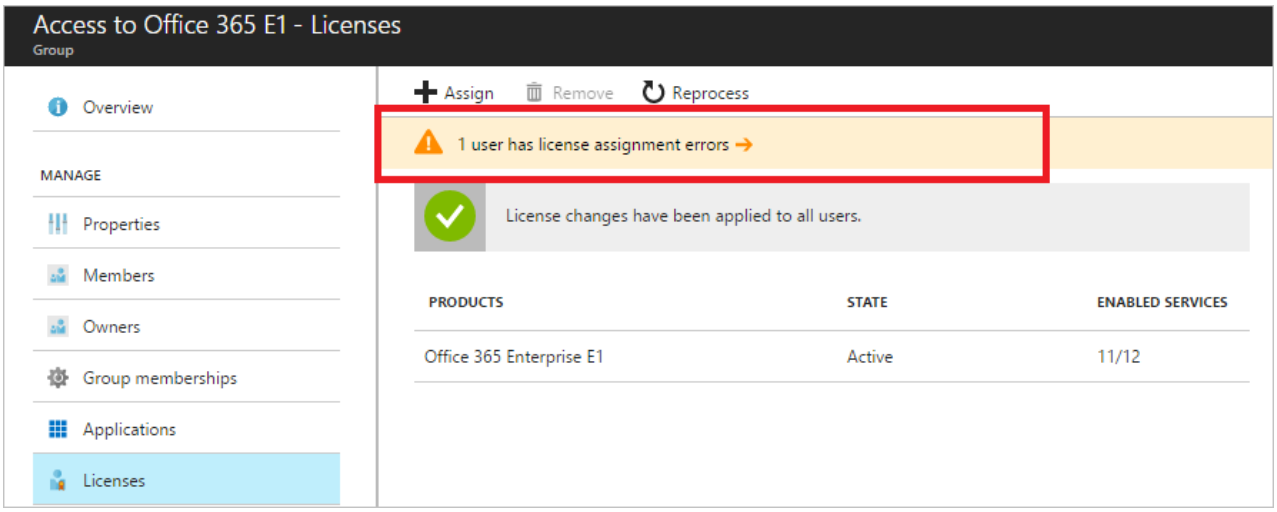
Another aspect of license management is the definition of service plans (components of the license) that should be

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.



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

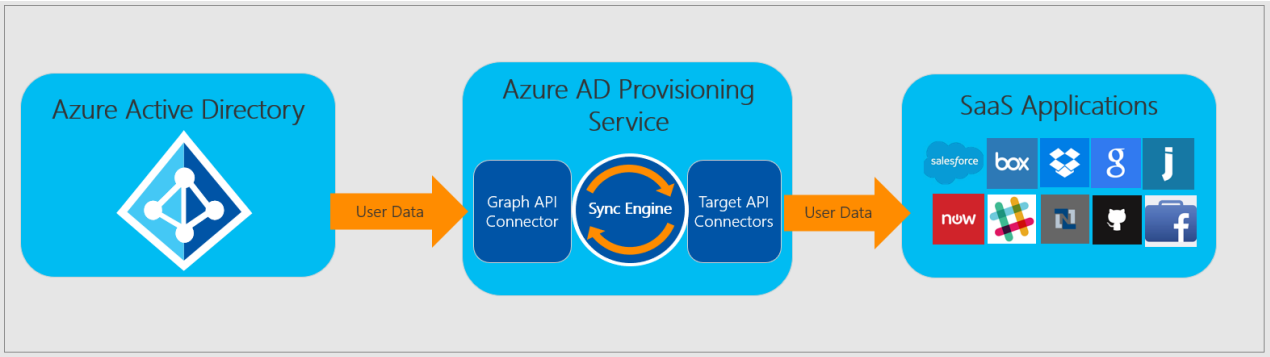
Resource owners may believe that the **All users** group contains only **Enterprise Employees** when they may actually contain both **Enterprise Employees** and **Guests**. As a result, you should take special care when using the **All users** group for application assignment and granting access to resources 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 Office 365 by using the IdFix tool - Office 365
- 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

4/7/2020 • 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.

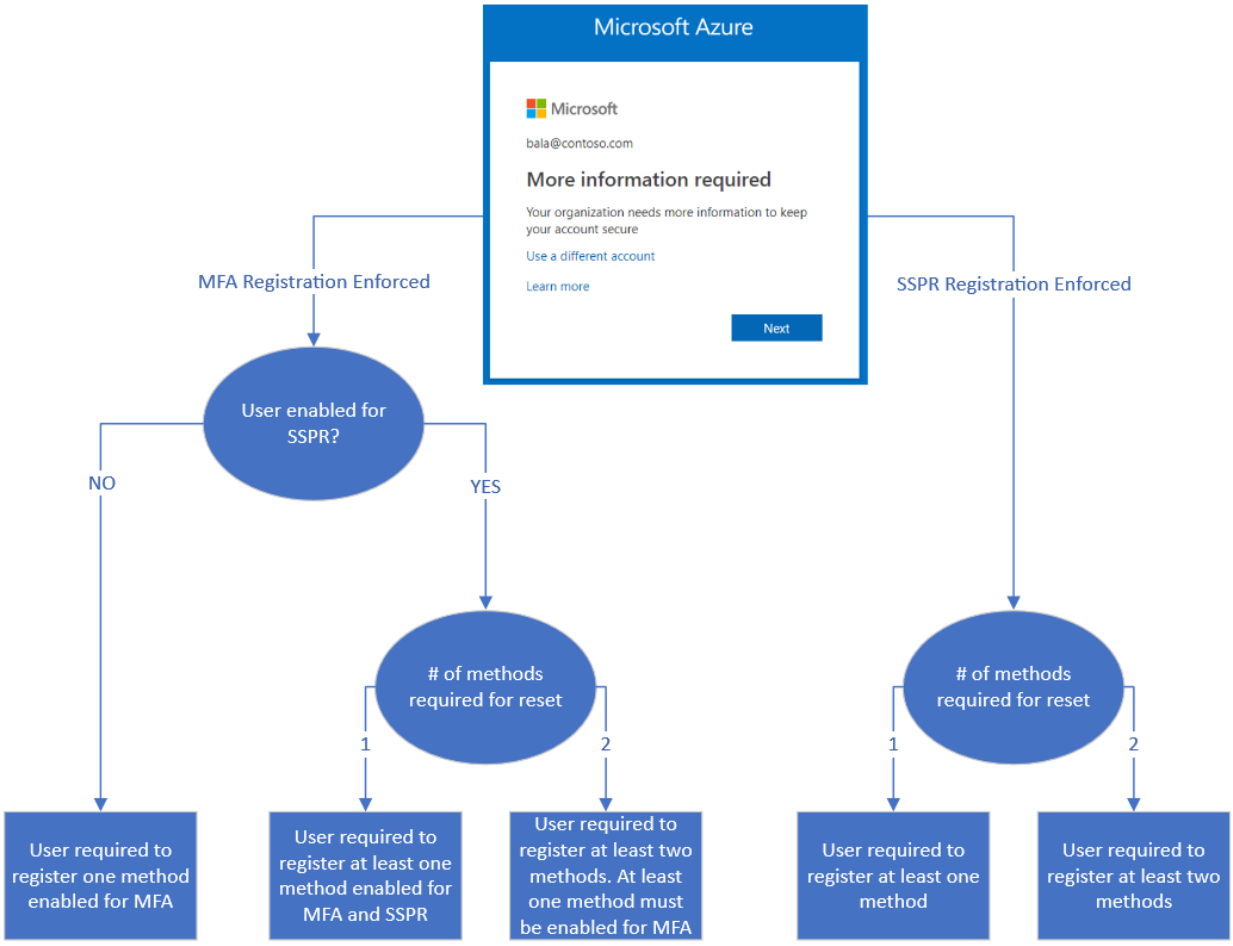
At a minimum, it is recommended you deploy Azure AD self-service password reset (SSPR) and on-premises password protection to accomplish:

- 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

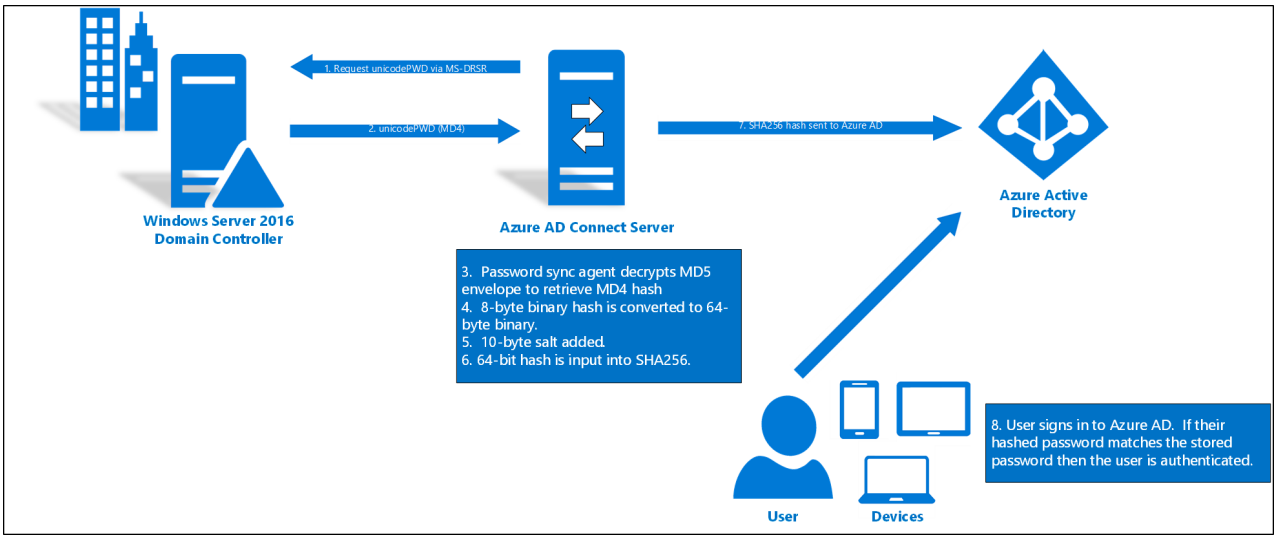
Passwords by themselves aren't secure enough to prevent bad actors from gaining access to your environment. At a minimum, any user with a privileged account must be enabled for multi-factor authentication (MFA). Ideally, you should enable combined registration and require all users to register for MFA 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 MFA allow users to access SaaS applications and Office 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:

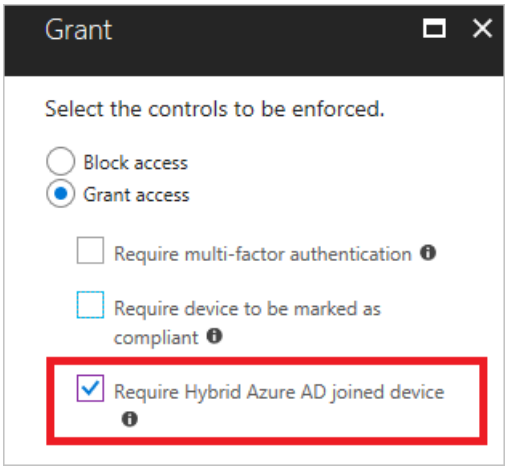
- Avoiding friction, for example, with MFA, when the device is trusted
- Blocking access from untrusted devices
- For Windows 10 devices, provide single sign-on to on-premises resources seamlessly.

You can carry out this goal by bringing device identities and managing them in Azure AD by using one of the

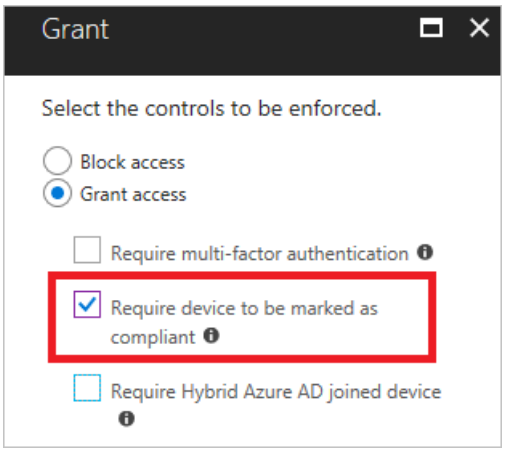
following methods:

- 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

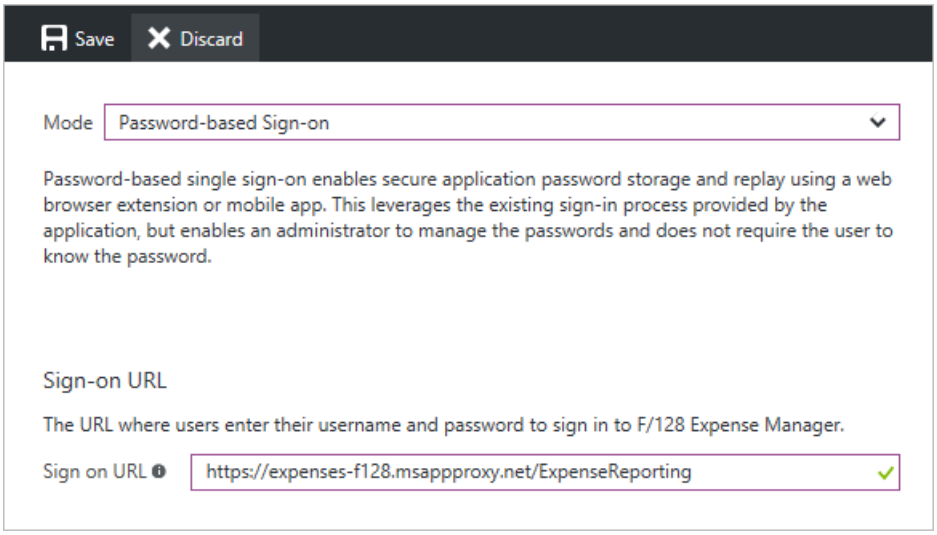
In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs. Windows Hello for Business enables a more streamlined MFA experience for users and reduces your dependency on passwords. If you haven't begun rolling out Windows 10 devices, or have only partially 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.



> **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 Cloud App Security.

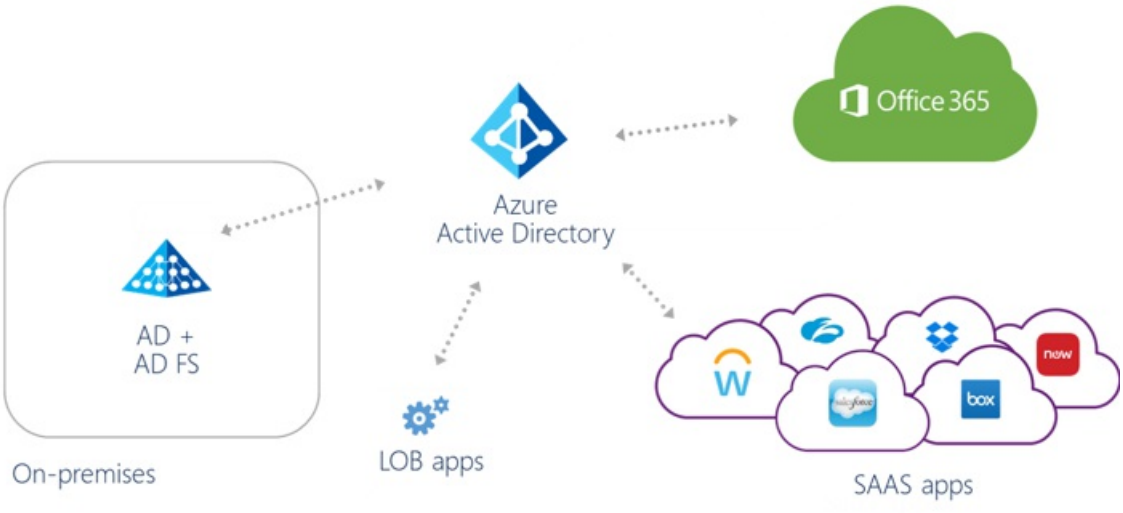
Finally, if you have an Azure AD app gallery and use applications that support SSO with Azure AD, we recommend listing the application in the app gallery.

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

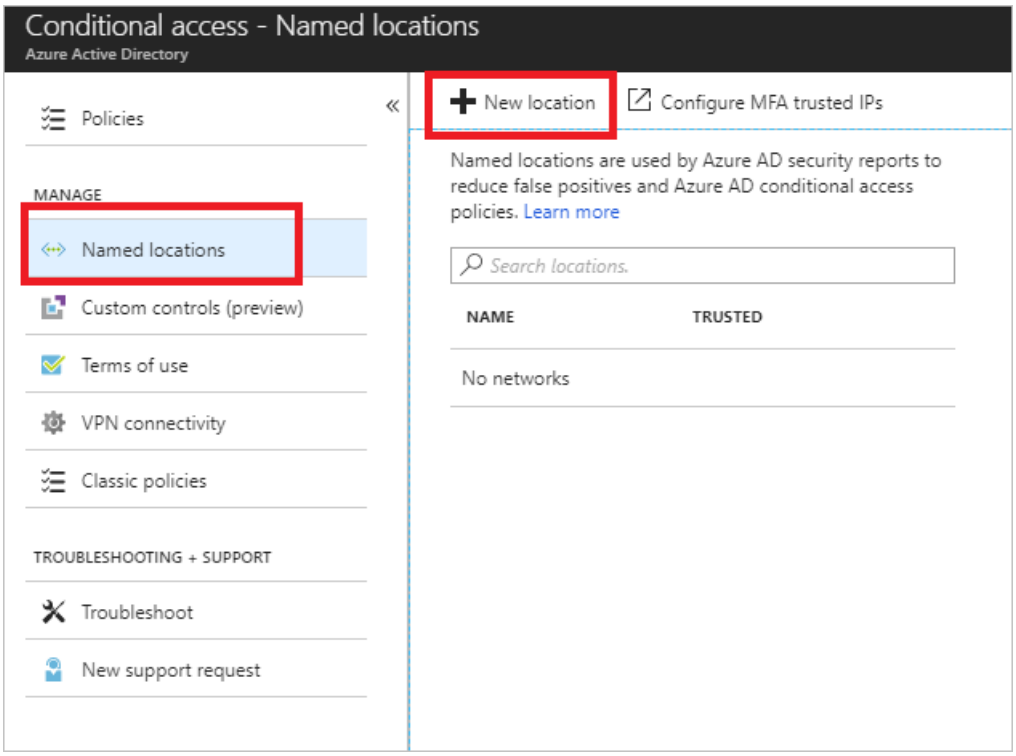
- Assign users and groups to an application in Azure Active Directory
- Delegate app registration permissions in Azure Active Directory
- Dynamic membership rules for groups in Azure Active Directory

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.

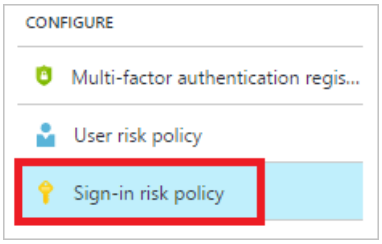


Based on priority, use the table below to find the recommended solution that best meets your organization's needs:

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 Office 365 client applications, for example, Teams, OneDrive for Business, 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
Office 365 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

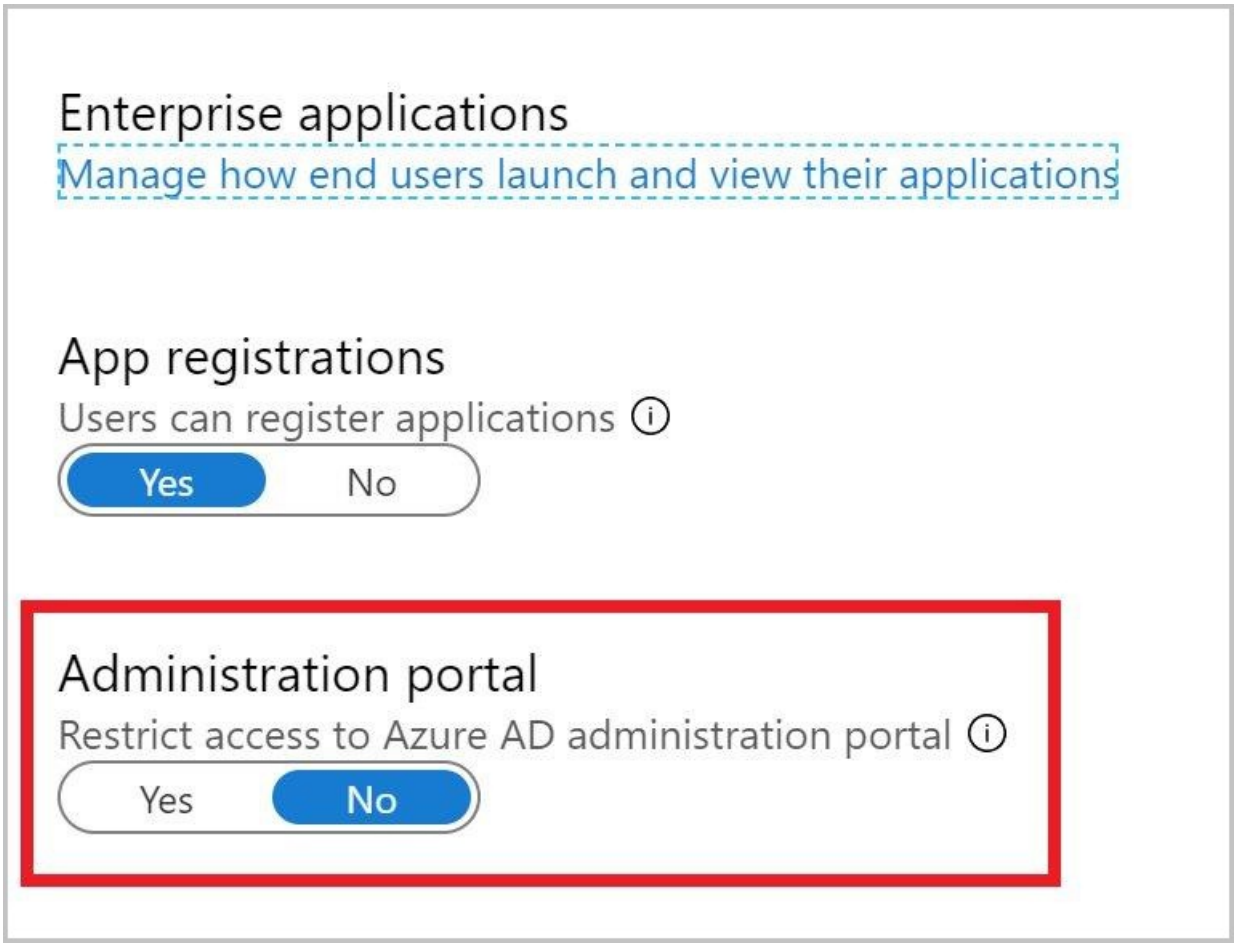
Below are the user and group settings that can be locked down if there isn't an explicit business need:

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:



> **NOTE**
> Non-adminstrators 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 / O365 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.

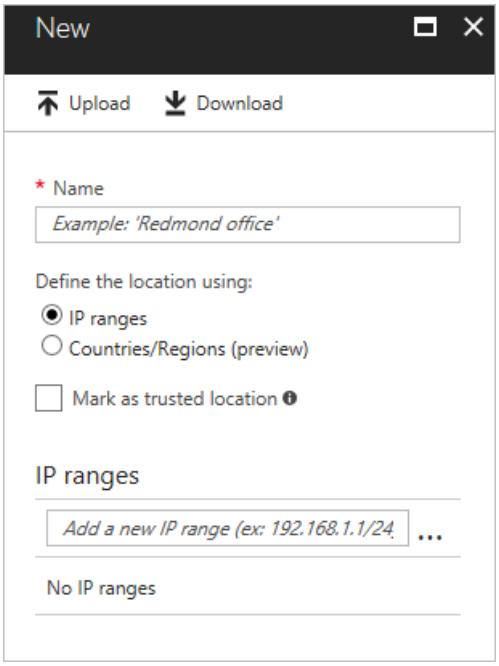
Groups recommended reading

- 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

11/26/2019 • 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:

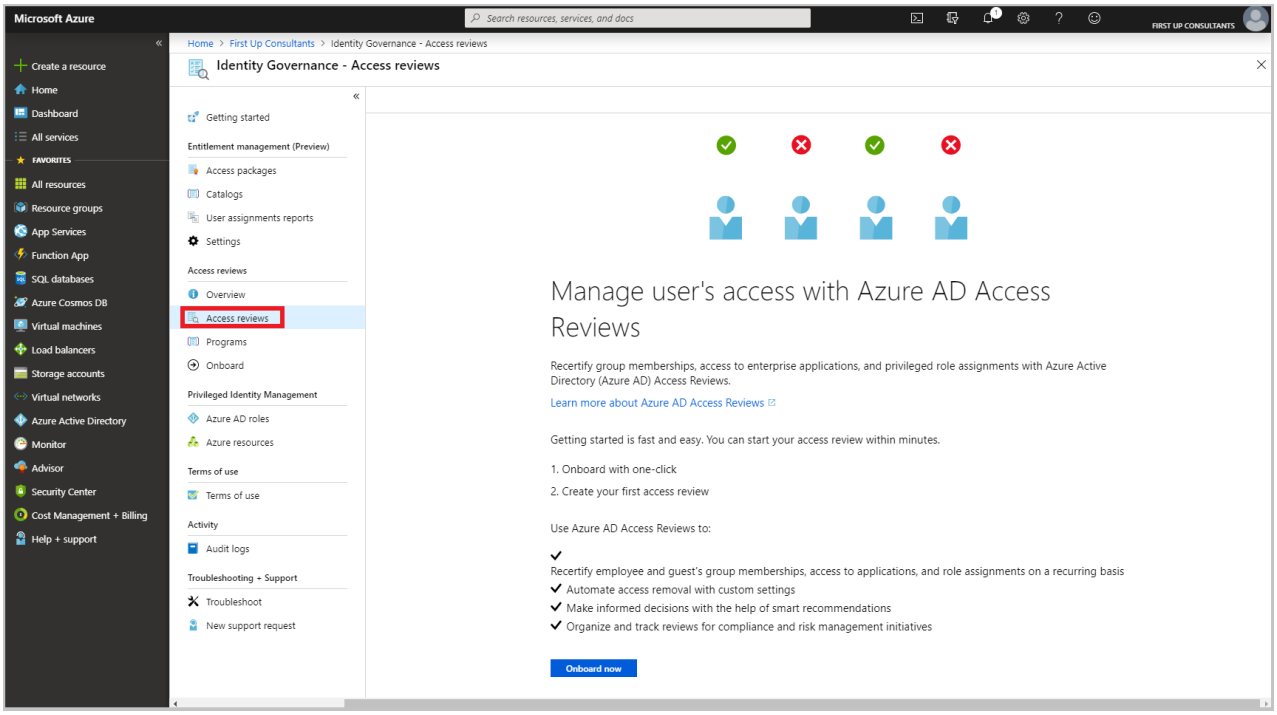
SCENARIO	RECOMMENDATION
Changing the authentication type from federated to PHS/PTA or vice-versa	Use staged rollout to test the impact of changing the authentication type.
Rolling out a new conditional access (CA) policy or Identity Protection Policy	Create a new CA Policy and assign to test users.
Onboarding a test environment of an application	Add the application to a production environment, hide it from the MyApps 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 CSExport 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.

SCENARIO	RECOMMENDATION

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.



> **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

12/11/2019 • 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 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

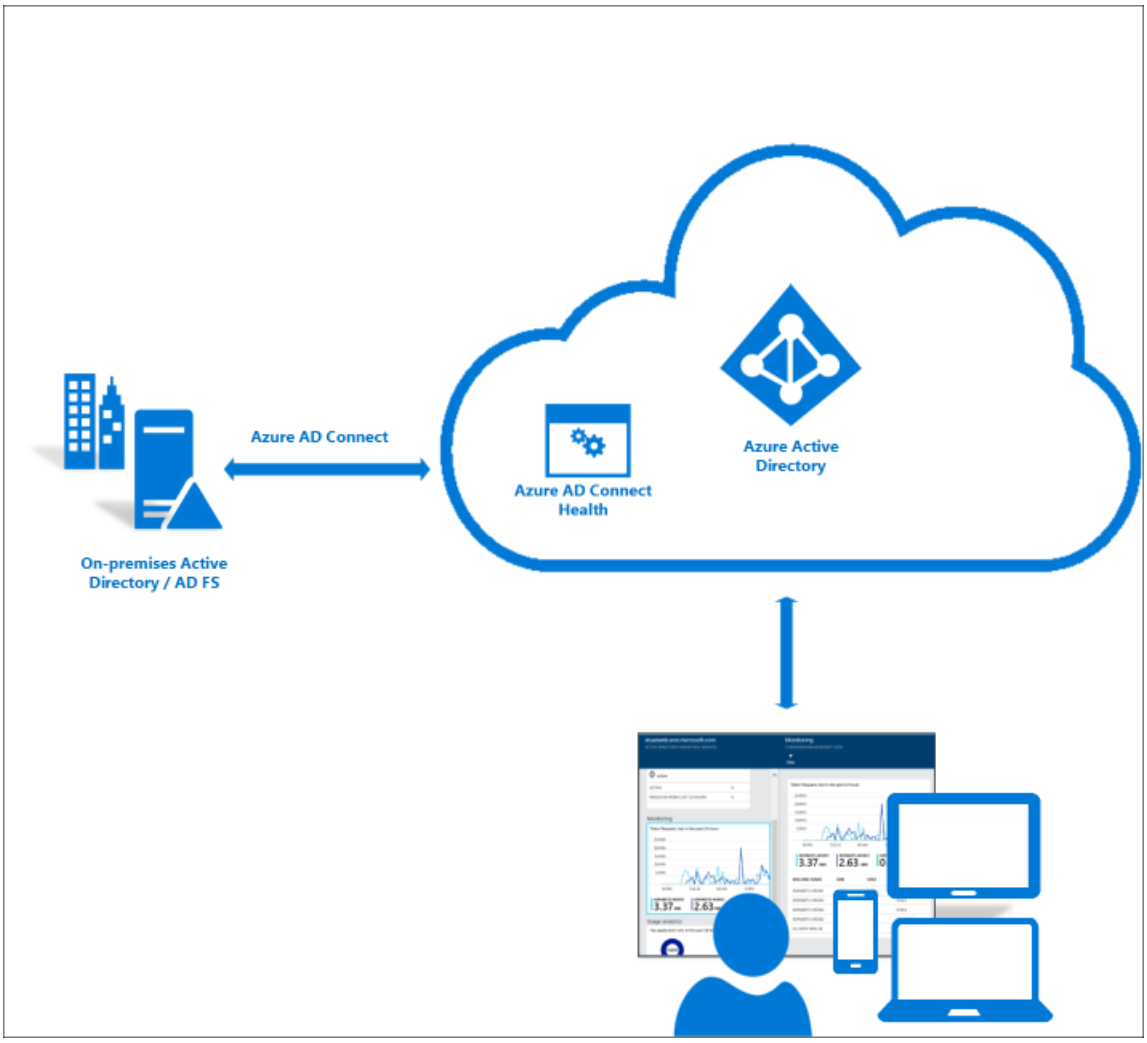
Unless one has been established, you should define a process to upgrade these components and rely on the automatic upgrade feature whenever possible. If you find components that are six or more months behind, you should upgrade as soon as possible.

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 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 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

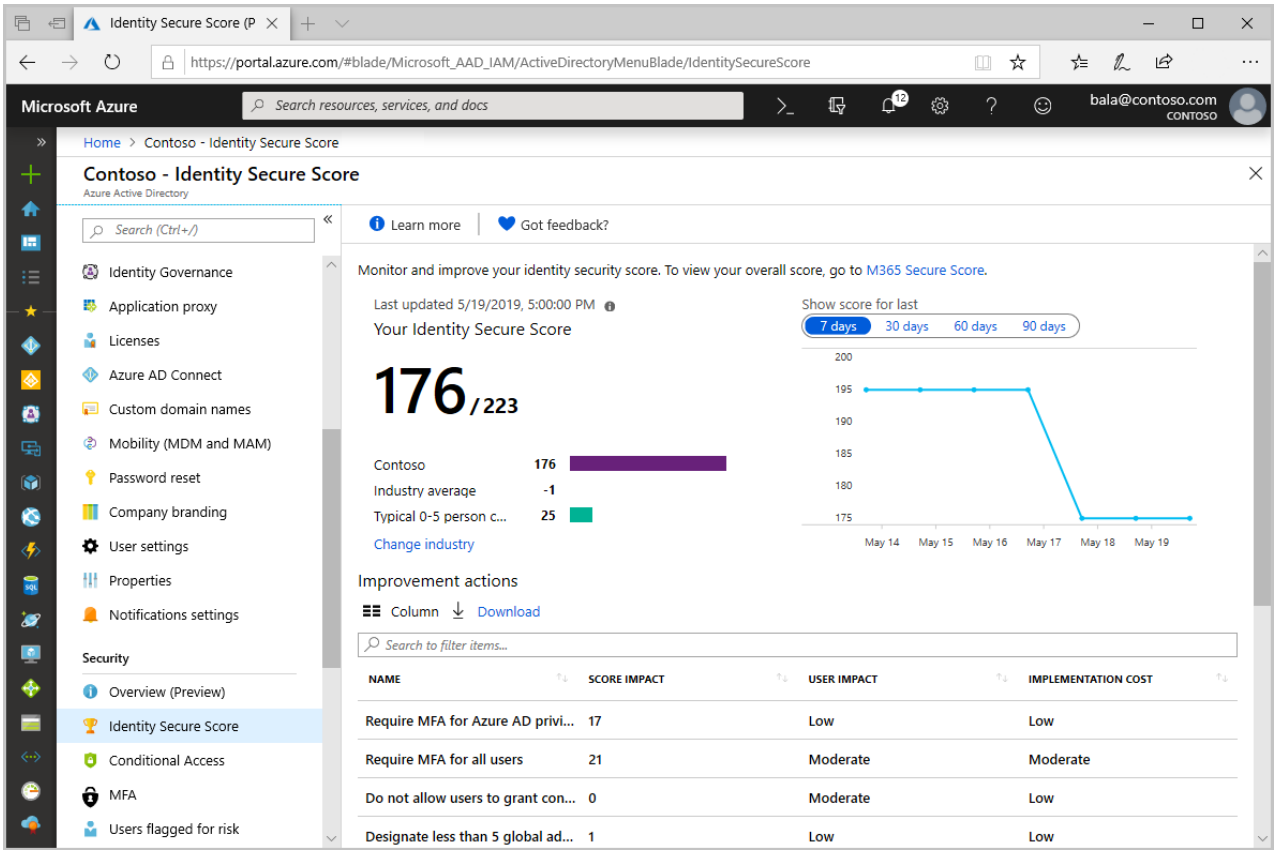
- Understand Azure AD Application Proxy connectors
- Azure AD Pass-through Authentication - quickstart

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 Office 365 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 Office 365 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
Office 365 Message Center	Incident and degradation notices of Identity Services and O365 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 - Office 365

Operational surface area

AD FS lockdown

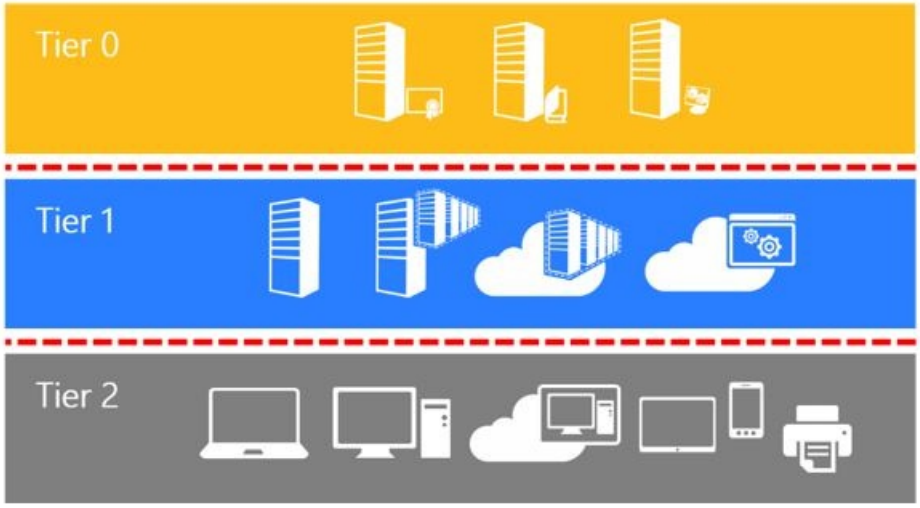
Organizations, which configure applications to authenticate directly to Azure AD benefit from Azure AD smart lockout. If you use AD FS in Windows Server 2012 R2, implement AD FS extranet lockout protection. If you use AD FS on Windows Server 2016 or later, implement extranet smart lockout. At a minimum, 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.

Sign up your organization to use Azure Active Directory

7/26/2019 • 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 Office 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 Office 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

7/20/2020 • 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.

> **NOTE**
>
> Azure AD Premium and Basic editions are available for customers in China using the worldwide instance of Azure Active Directory. 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 Active Directory Forum.

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 Office 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 Office 365 subscription

As an Azure or Office 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

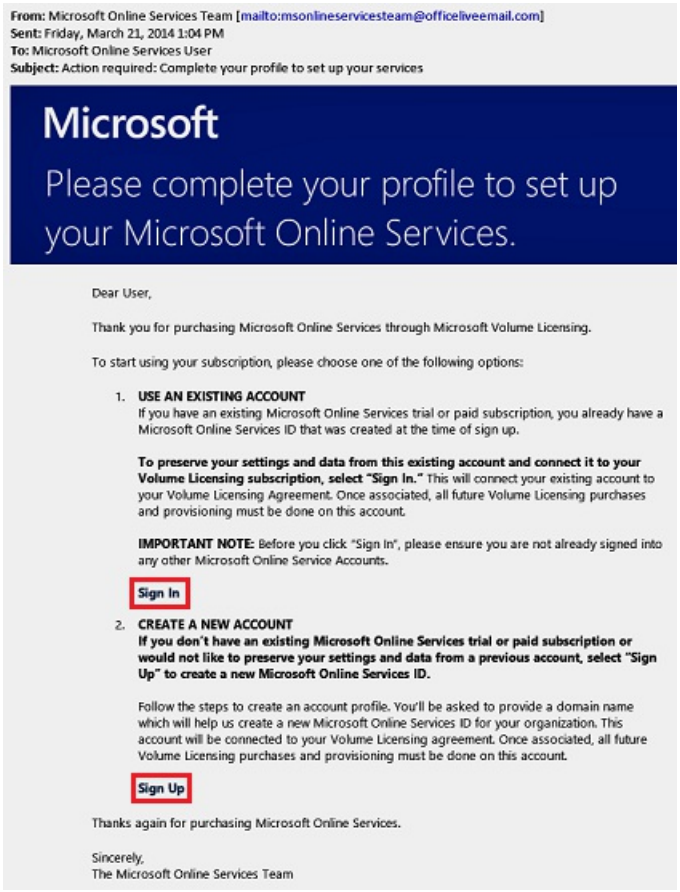
For more information about volume licensing purchase options, see How to purchase through Volume Licensing.

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**.



From: Microsoft Online Services Team [mailto:msonlineservicesteam@officeliveemail.com]
Sent: Friday, March 21, 2014 1:04 PM
To: Microsoft Online Services User
Subject: Action required: Complete your profile to set up your services

Microsoft

Please complete your profile to set up your Microsoft Online Services.

Dear User,

Thank you for purchasing Microsoft Online Services through Microsoft Volume Licensing.

To start using your subscription, please choose one of the following options:

1. **USE AN EXISTING ACCOUNT**
   If you have an existing Microsoft Online Services trial or paid subscription, you already have a Microsoft Online Services ID that was created at the time of sign up.

   To preserve your settings and data from this existing account and connect it to your Volume Licensing subscription, select "Sign In." This will connect your existing account to your Volume Licensing Agreement. Once associated, all future Volume Licensing purchases and provisioning must be done on this account.

   IMPORTANT NOTE: Before you click "Sign In", please ensure you are not already signed into any other Microsoft Online Service Accounts.

   Sign In

2. **CREATE A NEW ACCOUNT**
   If you don't have an existing Microsoft Online Services trial or paid subscription or would not like to preserve your settings and data from a previous account, select "Sign Up" to create a new Microsoft Online Services ID.

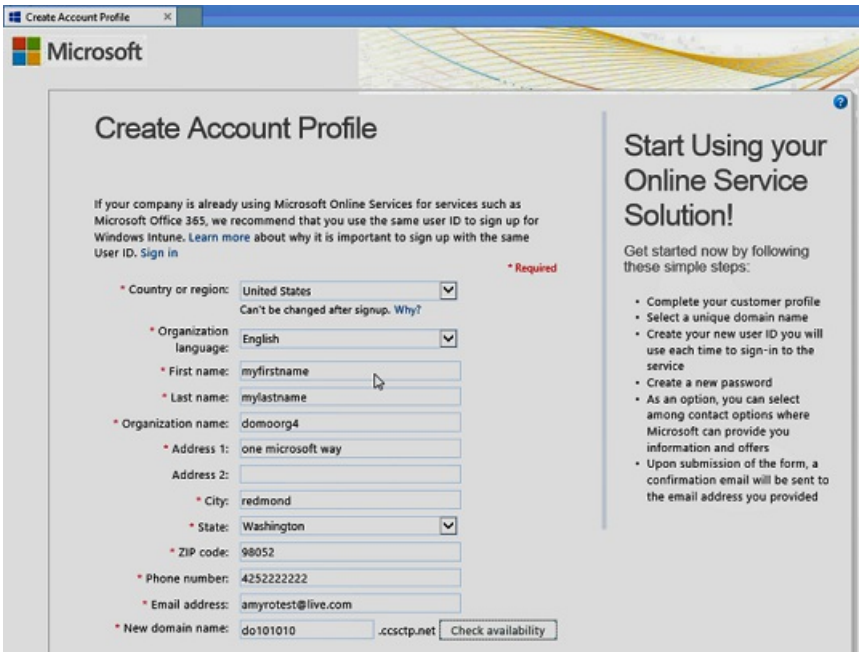
   Follow the steps to create an account profile. You'll be asked to provide a domain name which will help us create a new Microsoft Online Services ID for your organization. This account will be connected to your Volume Licensing agreement. Once associated, all future Volume Licensing purchases and provisioning must be done on this account.

   Sign Up

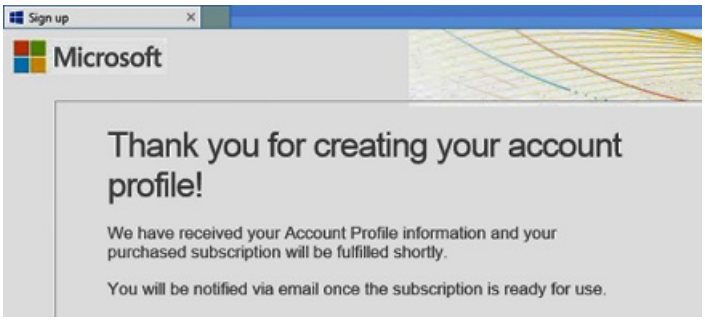
Thanks again for purchasing Microsoft Online Services.

Sincerely,
The Microsoft Online Services Team

  - **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.



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

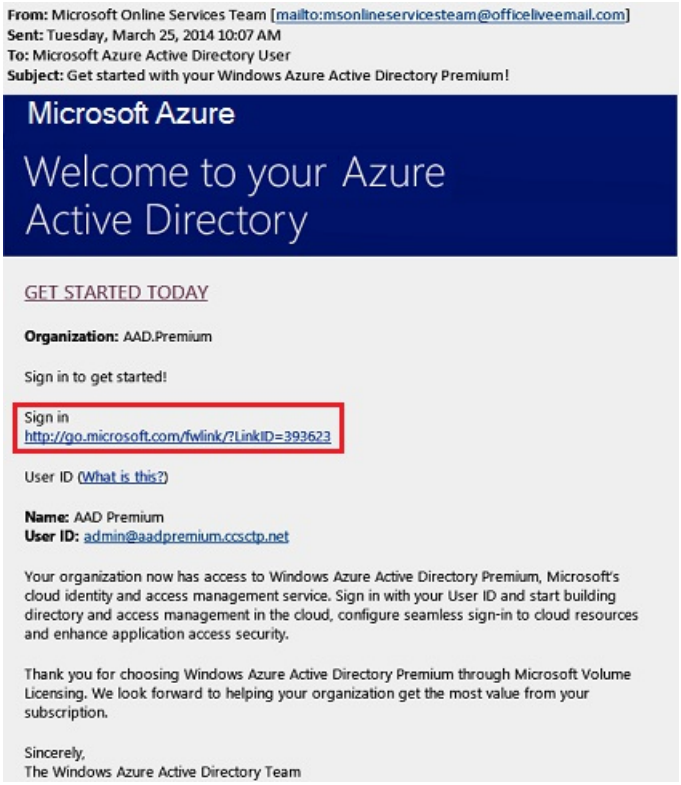
If you're adding new Azure AD Premium licenses to an existing subscription, your Azure AD access should already be activated. Otherwise, you need to activate Azure AD access after you receive the **Welcome email**.

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:msonlineservicesteam@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?)

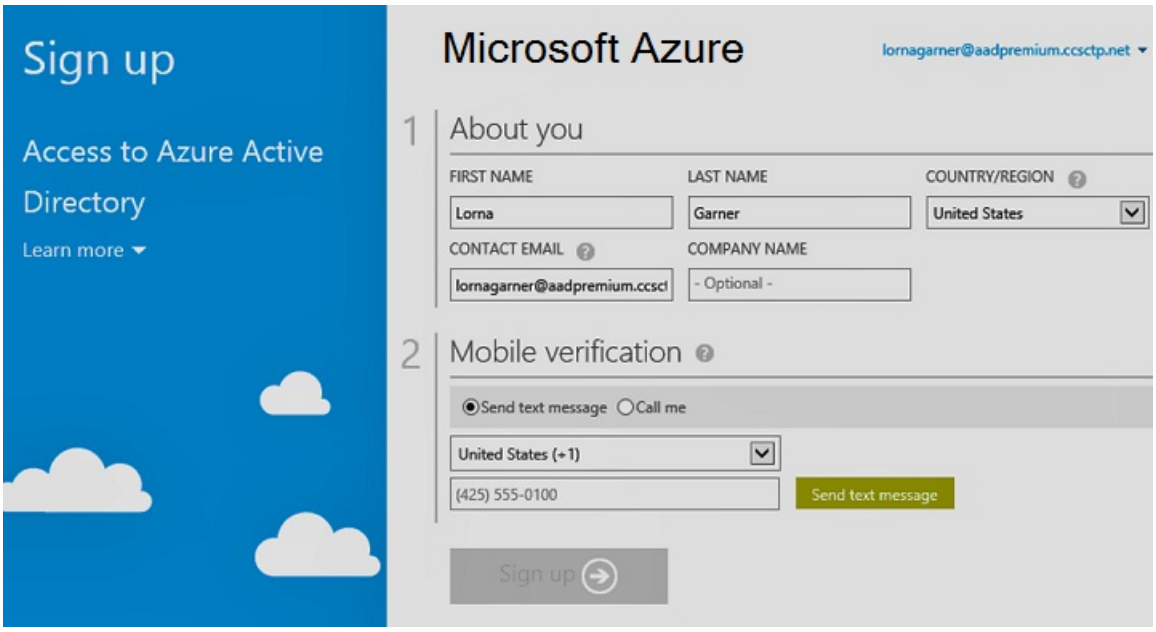
Name: AAD Premium
User ID: admin@aadpremium.ccsctp.net

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

2. After successfully signing in, you'll go through two-step verification using a mobile device.



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

7/20/2020 • 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.

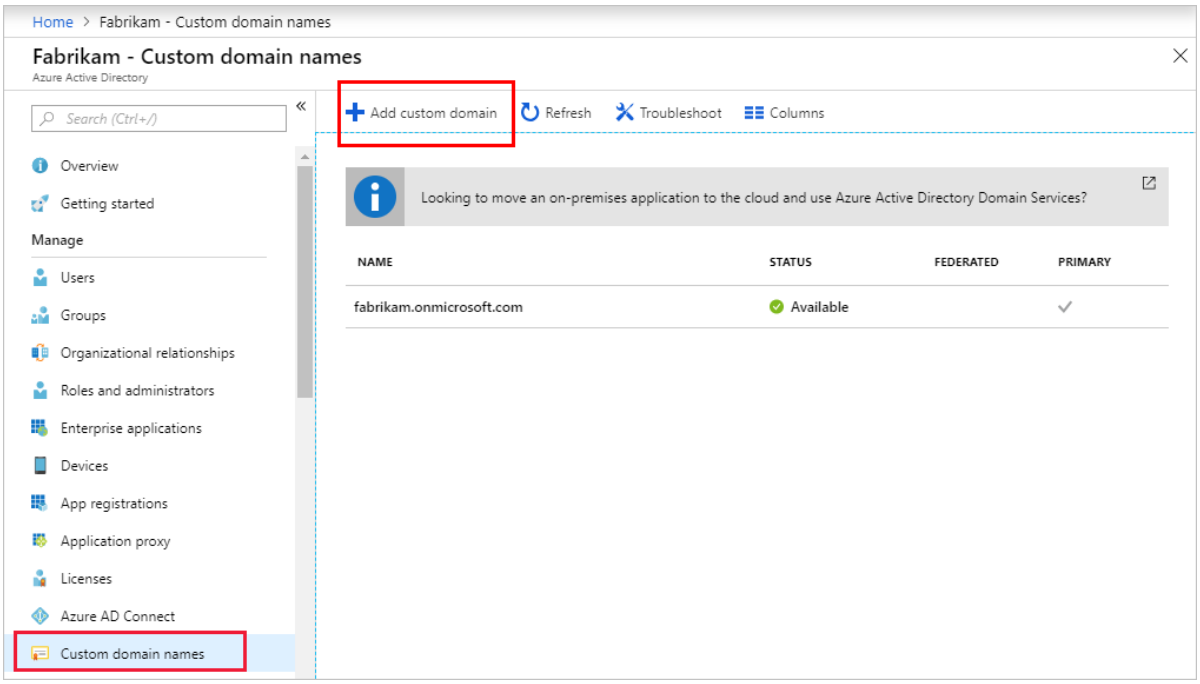
For more information about subscription roles, see Azure roles.

> **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.

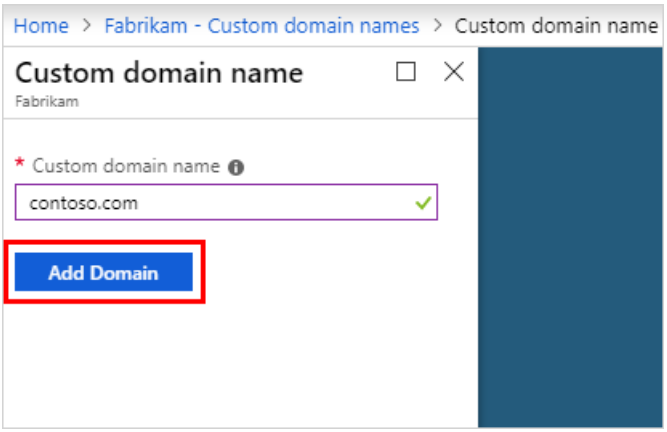
Add your custom domain name to Azure AD

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**.

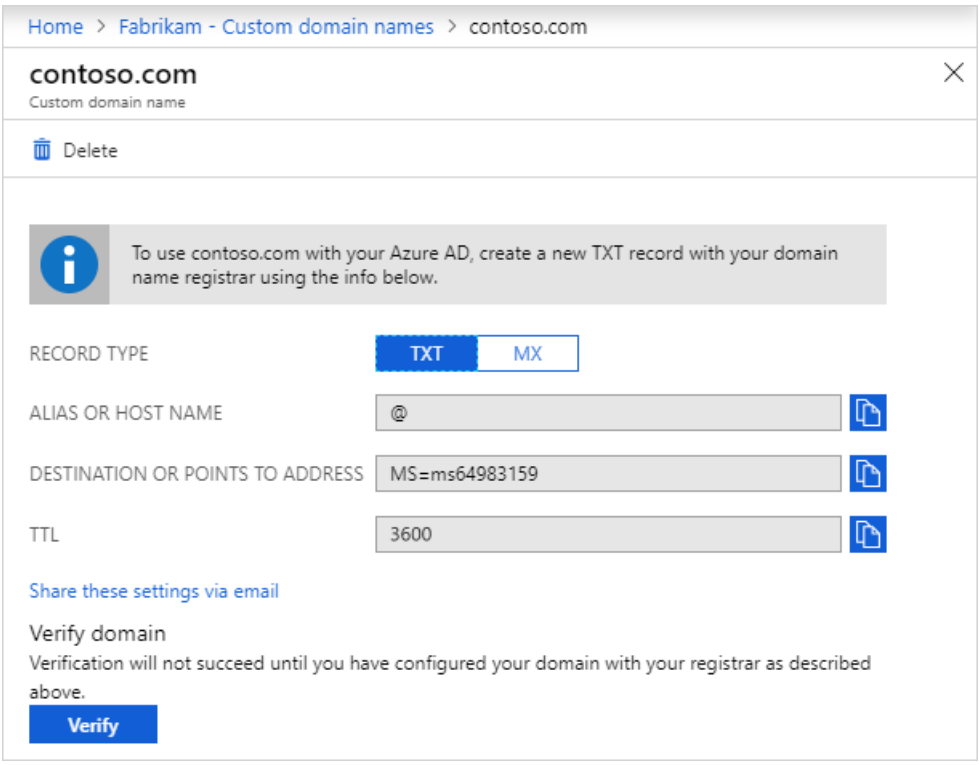


3. In **Custom domain name**, enter your organization's new name, in this example, *contoso.com*. Select **Add domain**.



> **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.



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.

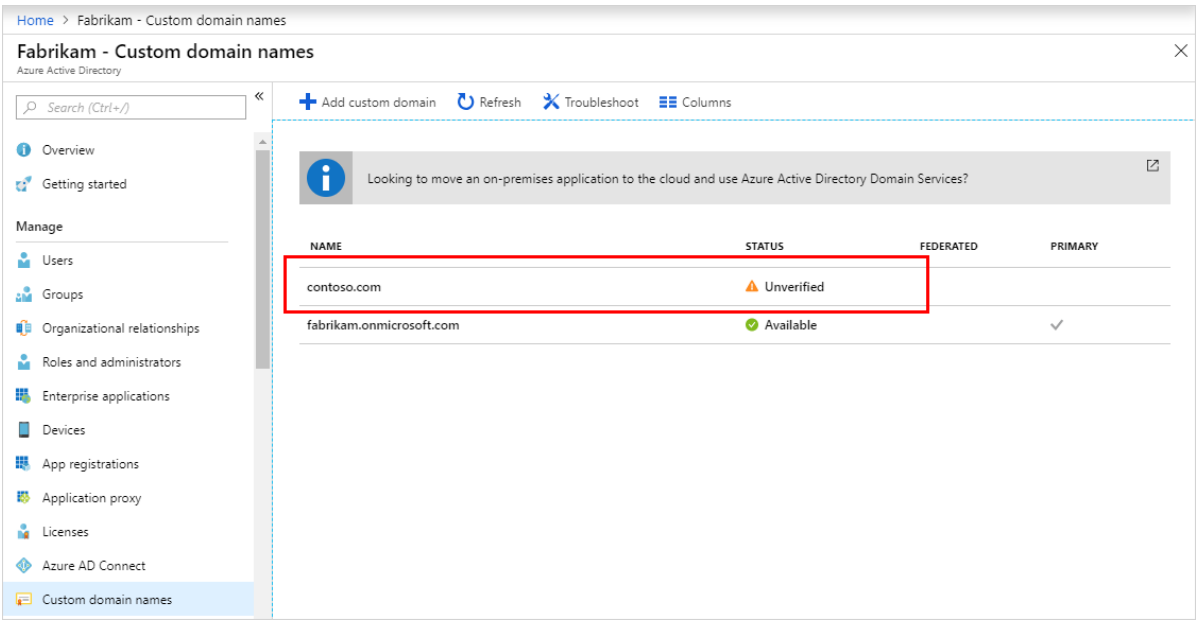
> **IMPORTANT**
> You can register as many domain names as you want. However, each domain gets its own TXT record from Azure AD. Be careful when you enter the TXT file information at the domain registrar. If you enter the wrong or duplicate information by mistake, you'll have to wait until the TTL times out (60 minutes) before you can try again.

Verify your custom domain name

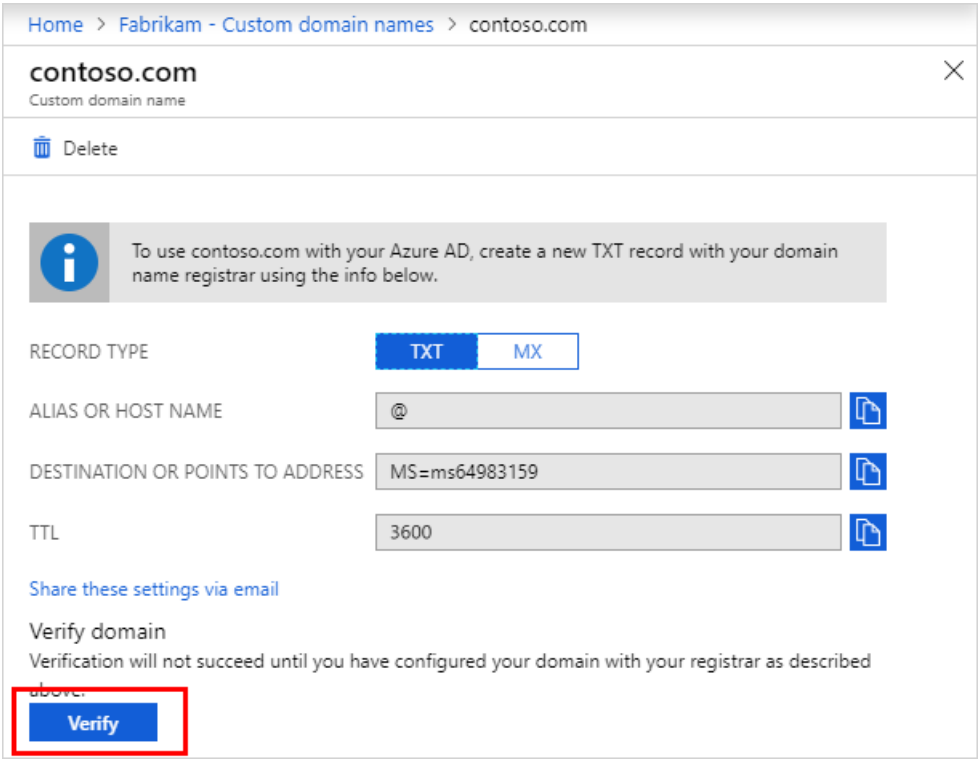
After you register your custom domain name, make sure it's valid in Azure AD. The propagation from your domain registrar to Azure AD can be instantaneous or it can take a few days, depending on your domain registrar.

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**.



4. On the **contoso.com** page, select **Verify** to make sure your custom domain is properly registered and is valid for Azure AD.



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.
- **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

7/20/2020 • 6 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 Office 365, which uses Azure AD as your identity provider.

> **NOTE**
>
> Adding custom branding requires you to use Azure Active Directory Premium 1, Premium 2, or Basic editions, or to have an Office 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 Active Directory. 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 Active Directory Forum.

Customize your Azure AD sign-in page

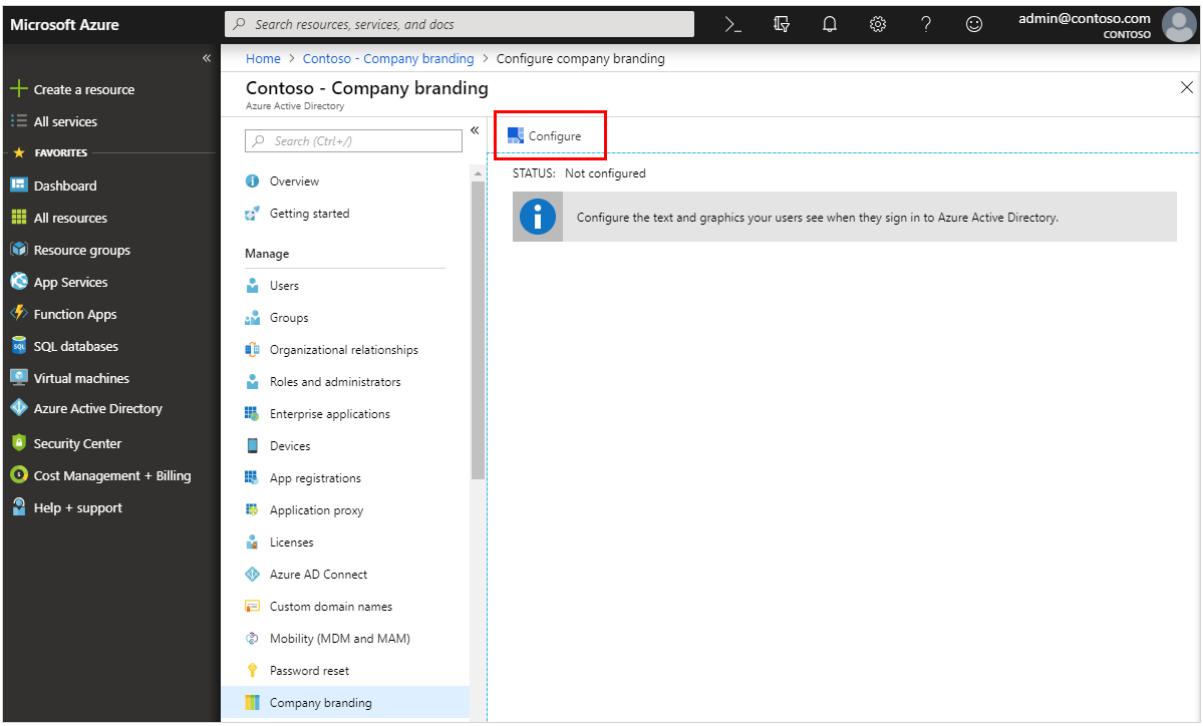
You can customize your Azure AD sign-in pages, which appear when users sign in to your organization's tenant-specific apps, such as `https://outlook.com/contoso.com`, or when passing a domain variable, such as `https://passwordreset.microsoftonline.com/?whr=contoso.com`.

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. 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 (for example, Office 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 customize your branding

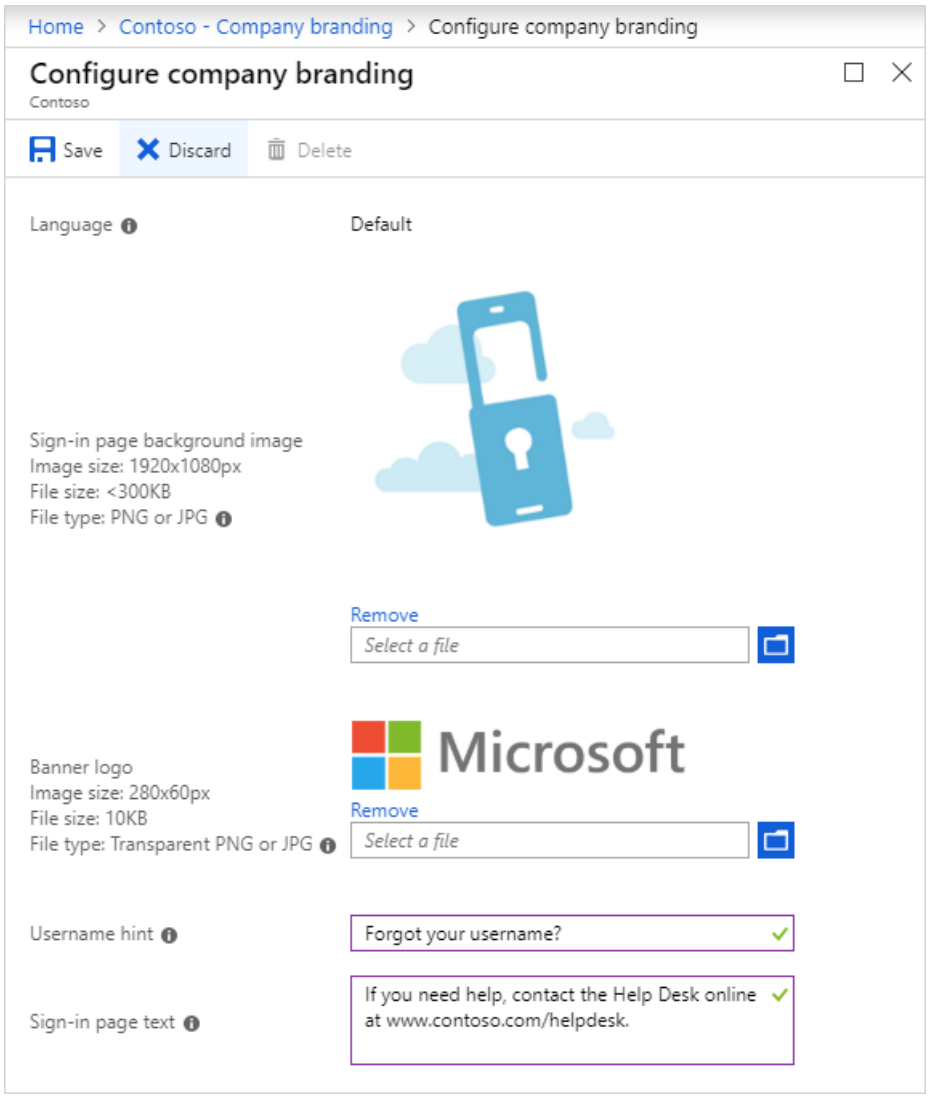
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **Configure**.



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



- **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 KB.

  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. 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:

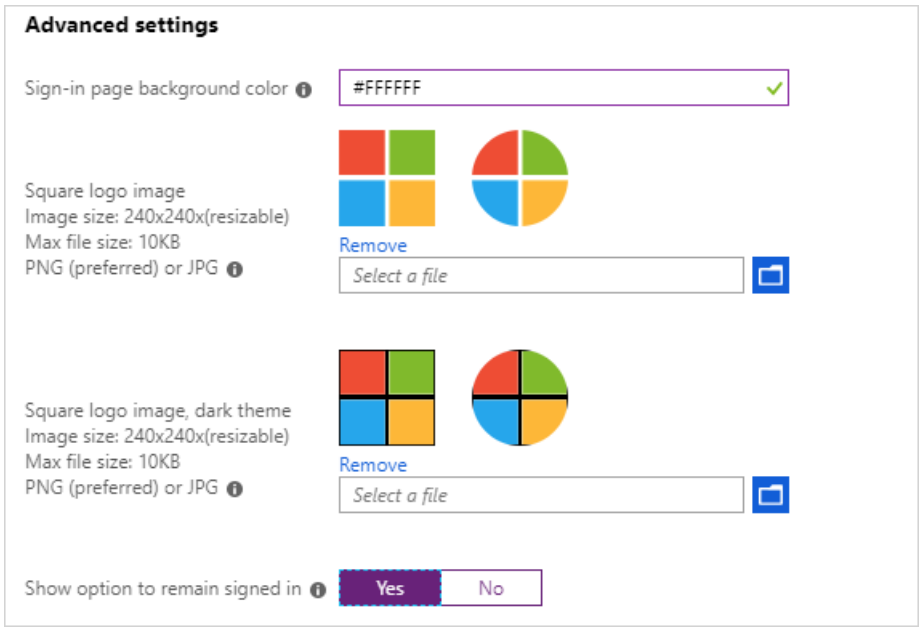
> Hyperlink: `[text](link)`

> Bold: `**text**` or `__text__`

> Italics: `*text*` or `_text_`

> Underline: `++text++`

- Advanced settings



  - **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.

  - **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.

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**.

   If this process creates your first custom branding configuration, it becomes the default for your tenant. If you have additional configurations, you'll be able to choose your default configuration.

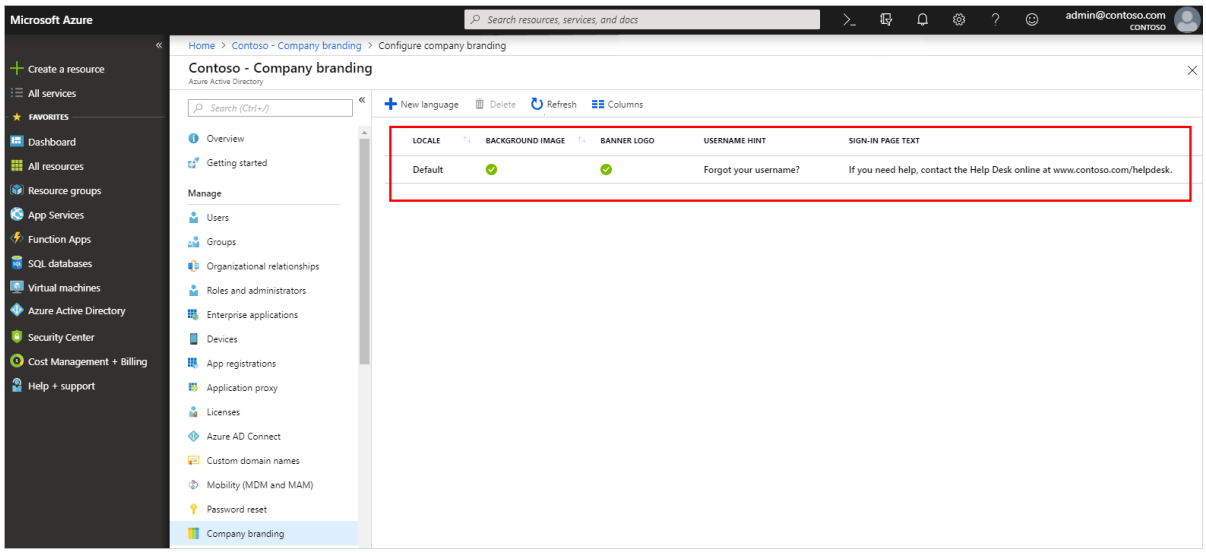
> **IMPORTANT**
> To add more corporate branding configurations to your tenant, you must choose **New language** on the **Contoso - Company branding** page. This opens the **Configure company branding** page, where you can follow the same steps as above.

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**.



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.

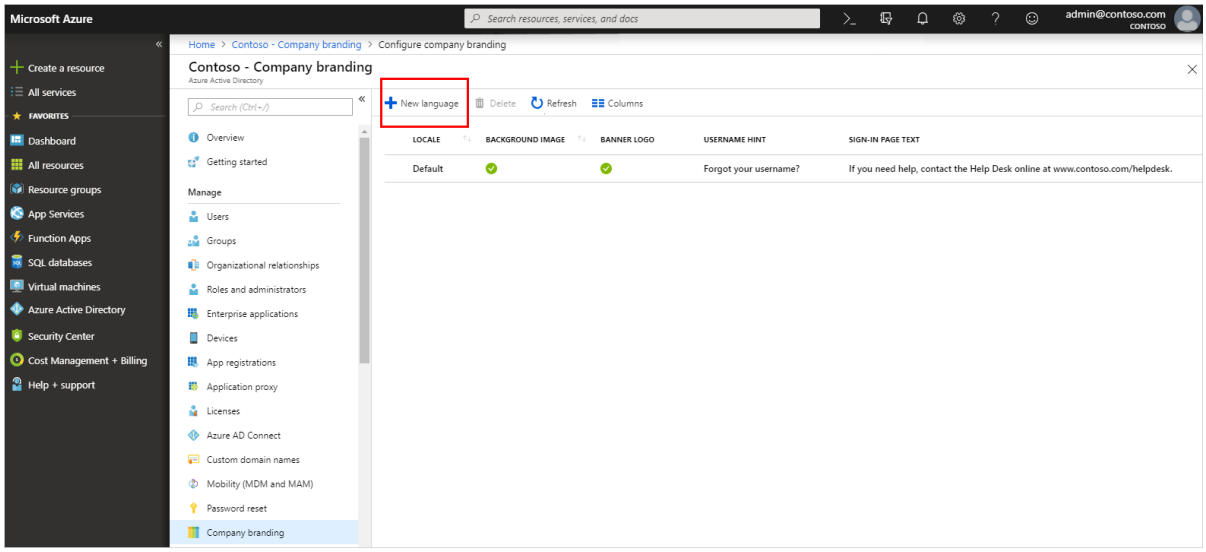
Add language-specific company branding to your directory

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.

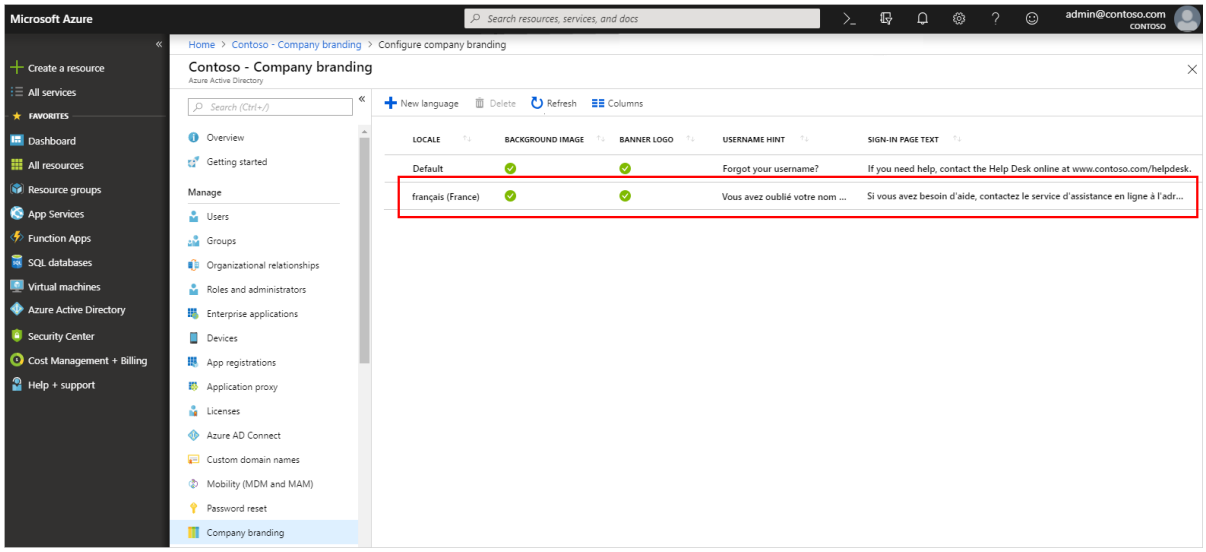
To add a language-specific branding configuration

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**.



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.



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 modification works on several pages, including the Multi-Factor Authentication (MFA) setup page, the Self-service Password Reset (SSPR) setup page, and the sign in 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

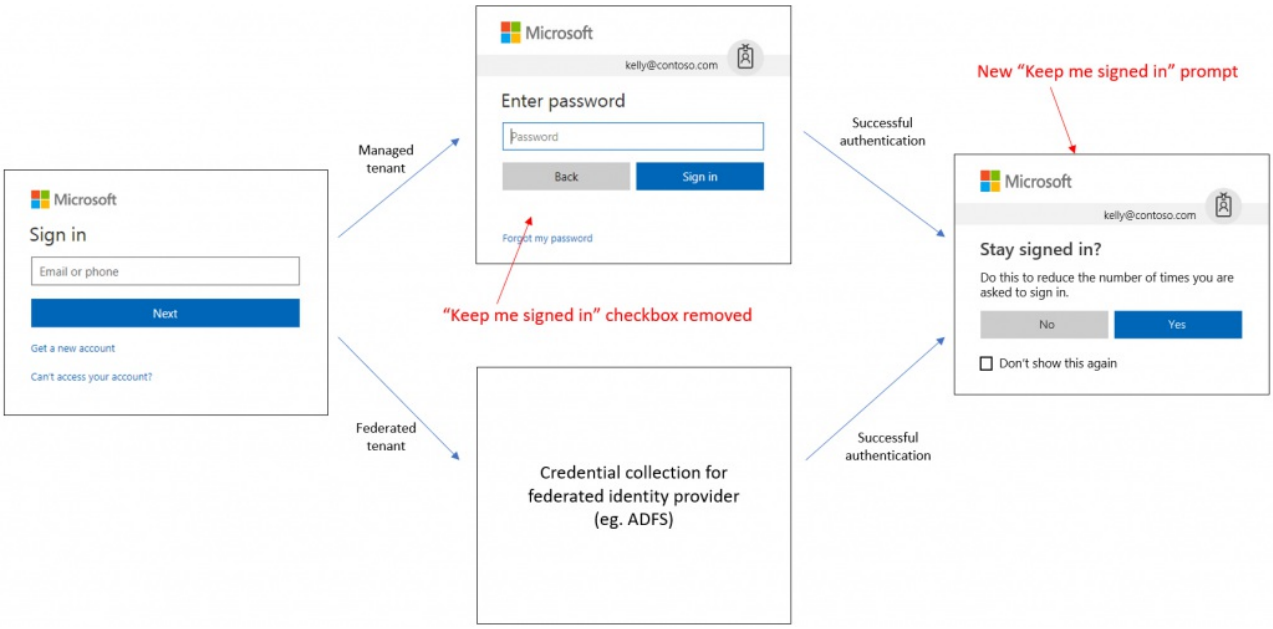
Custom URL: `https://passwordreset.microsoftonline.com/?whr=contoso.com`

Configure the 'Stay signed in?' prompt for Azure AD accounts

7/20/2020 • 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.

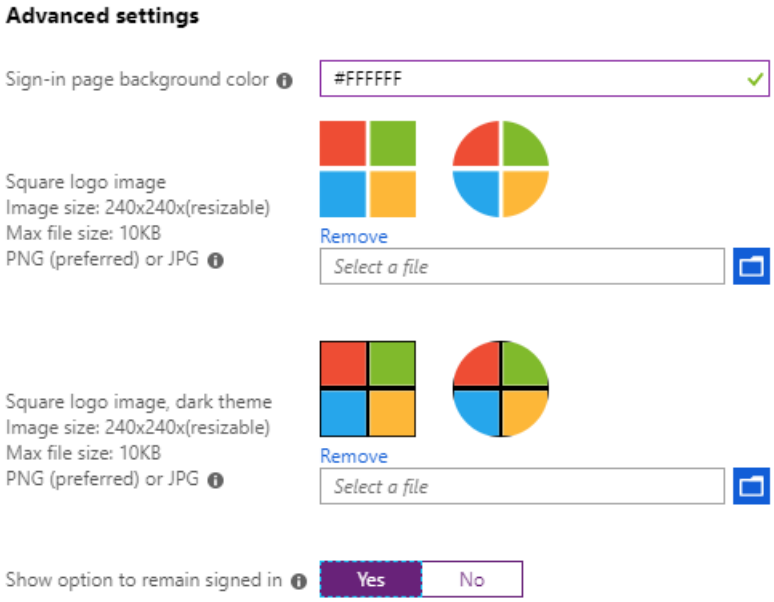
Configure KMSI

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.

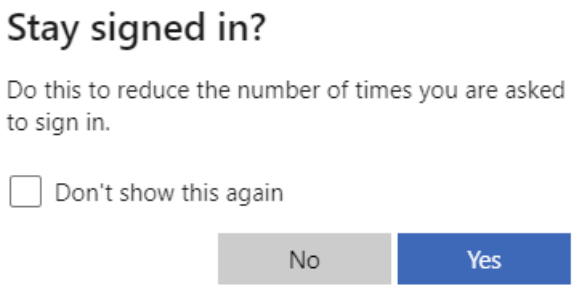
   - If you choose **No**, the **Stay signed in?** option is hidden after the user successfully signs in and the user must sign in each time the browser is closed and reopened.

- If you choose **Yes**, the **Stay signed in?** option is shown to the user.



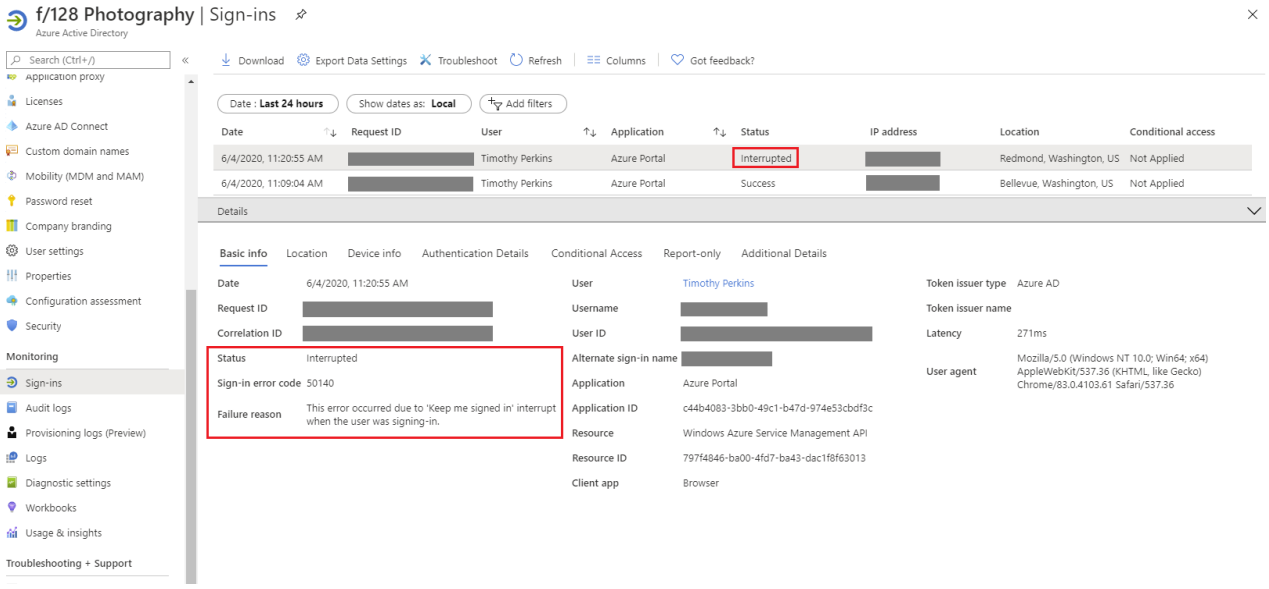
Troubleshoot sign-in issues

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.



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.



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

7/20/2020 • 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.

If your subscription expires, you lose access to all the other resources associated with the subscription. However, the Azure AD directory remains in Azure. You can associate and manage the directory using a different Azure subscription.

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 to a different directory, users that have roles assigned using role-based access control (RBAC) lose their access. Classic subscription administrators, including Service Administrator and Co-Administrators, also lose access.
>
> Policy Assignments are also removed from a subscription when the subscription is associated with a different directory.
>
> 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:

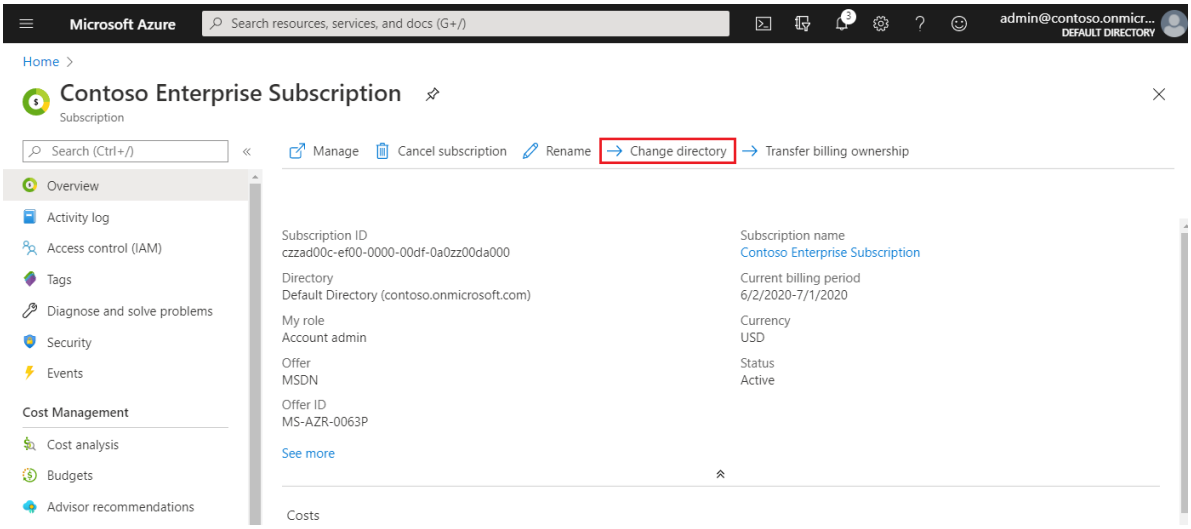
- Review the following list of changes that will occur after you associate or add your subscription, and how you might be affected:
  - Users that have been assigned roles using RBAC will lose their access
  - Service Administrator and Co-Administrators will lose access
  - If you have any key vaults, 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
- Sign in using an account that:
  - Has an Owner role assignment for the subscription. For information about how to assign the Owner role, see Manage access to Azure resources using RBAC and 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 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 Imagine

subscription (MS-AZR-0144P).

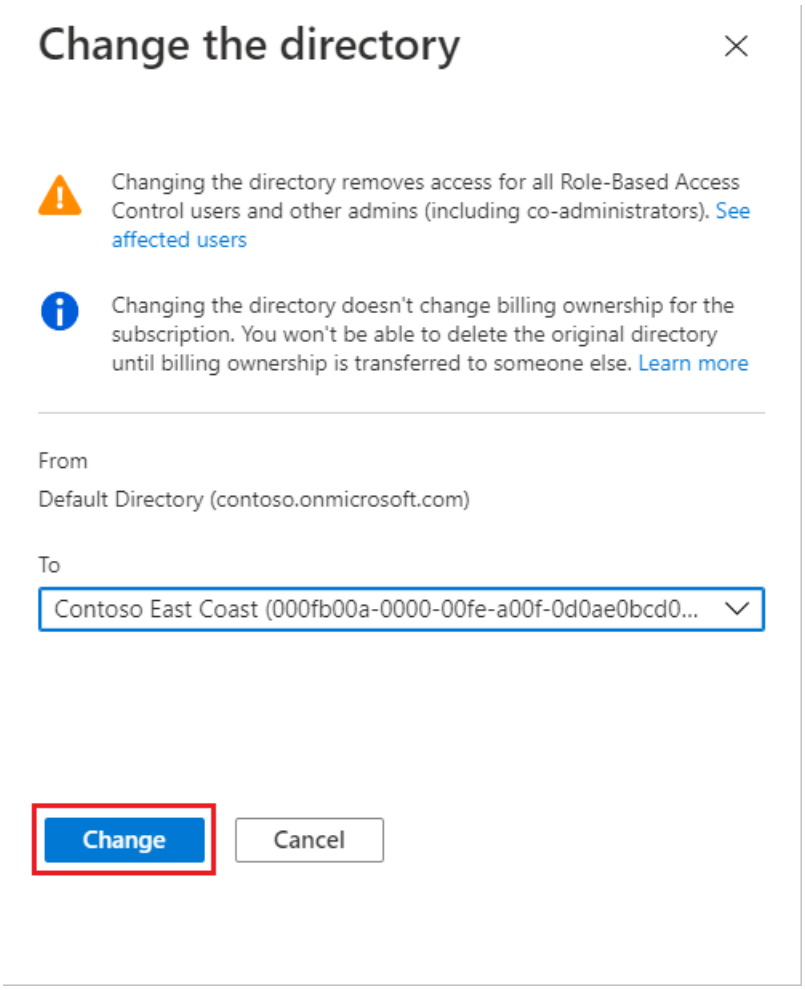
Associate a subscription to a directory

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**.

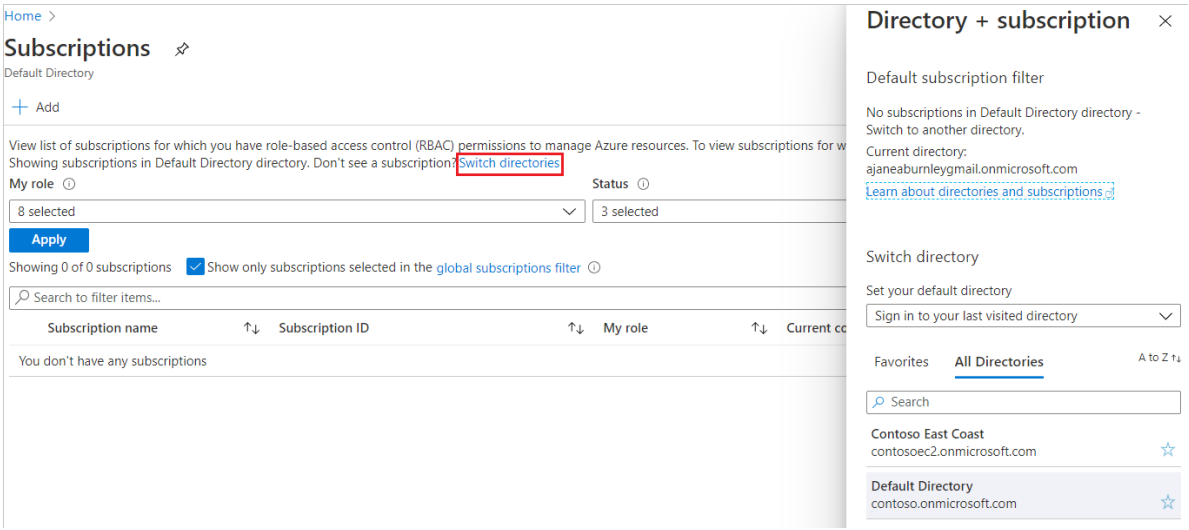


3. Review any warnings that appear, and then select **Change**.



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.



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. The Account Admin can still change the Service Admin from the Account Center. 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 is 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 with Azure.

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 RBAC 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 your organization's privacy info using Azure Active Directory

7/20/2020 • 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 Service Trust portal.

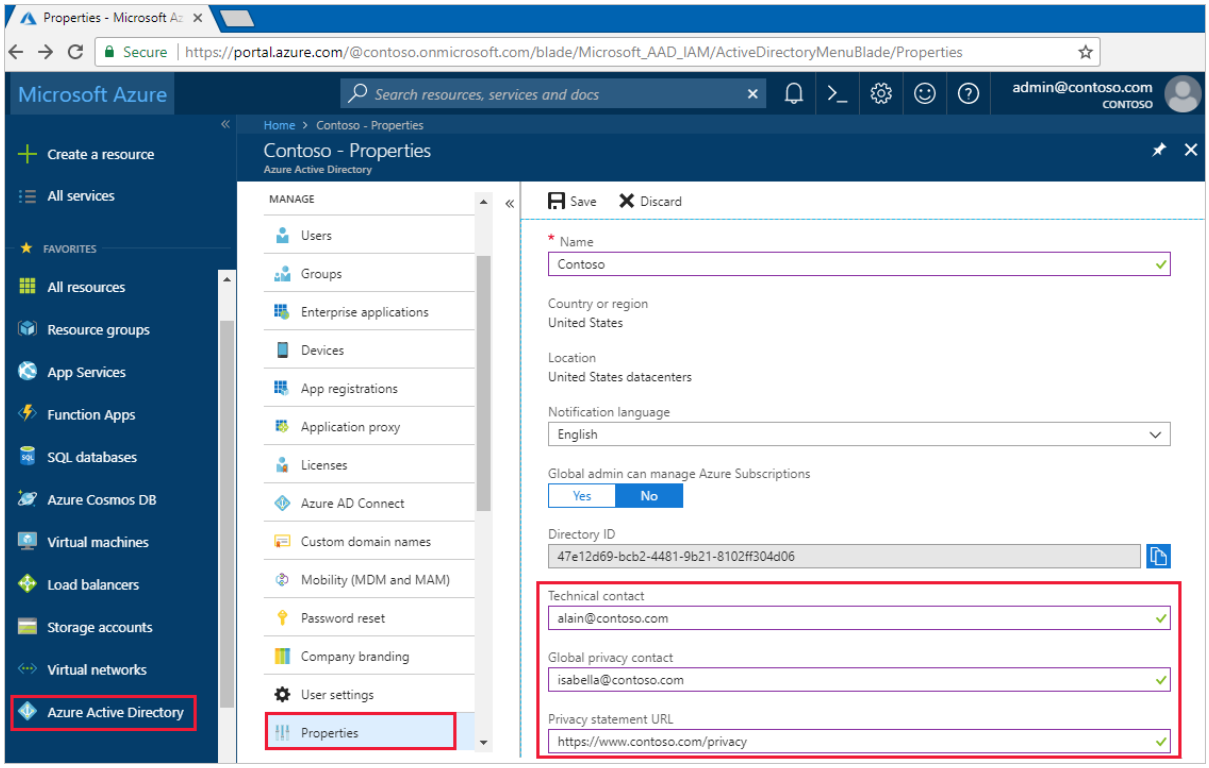
Add your privacy info on Azure AD

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.



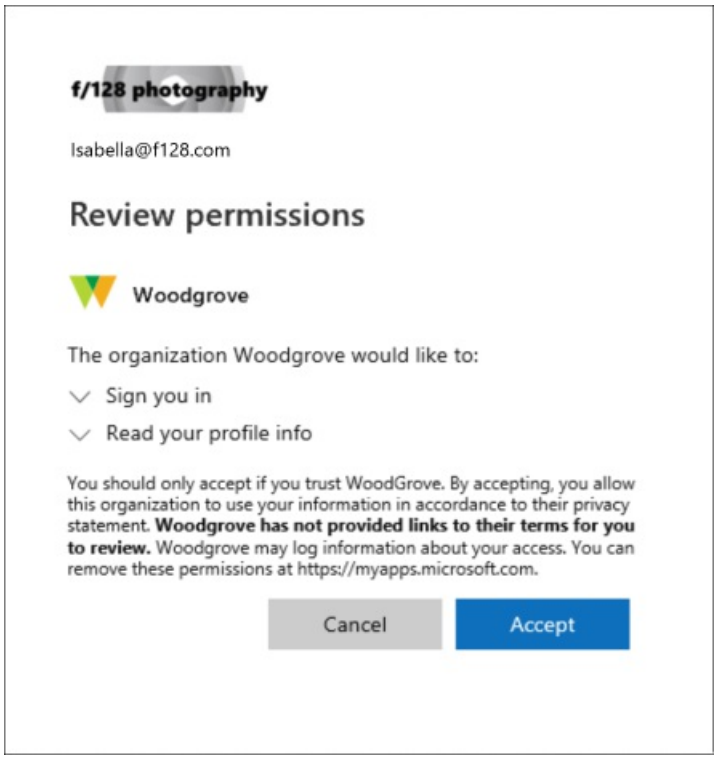
3. Add your privacy info for your employees:

   - **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. If there's no person listed here, Microsoft contacts your global administrators.
- **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

Create a basic group and add members using Azure Active Directory

7/20/2020 • 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.
- **Office 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. An Office 365 group can have only users as its members. Both users and service principals can be owners of an Office 365 group. For more info about Office 365 Groups, see Learn about Office 365 Groups.

Membership types:

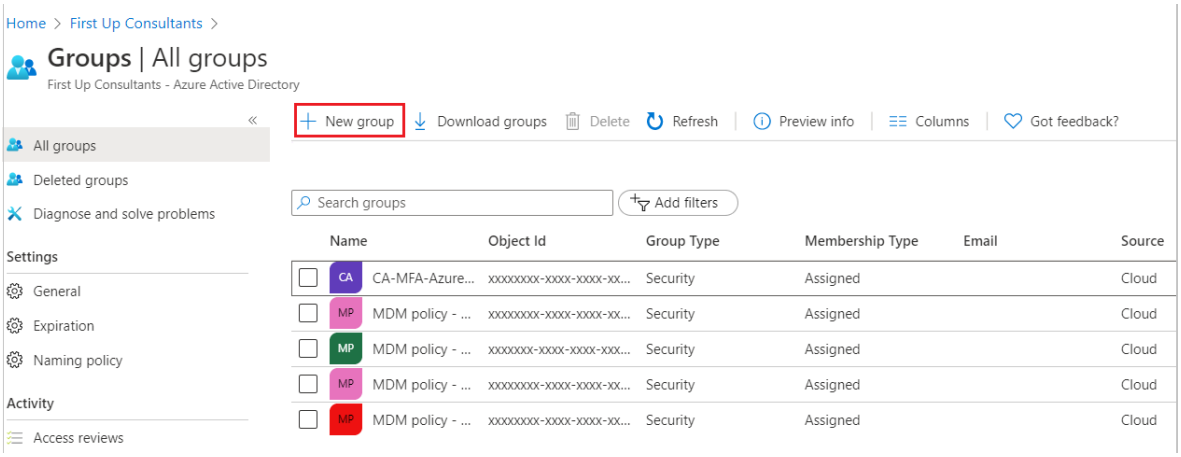
- **Assigned.** Lets you add specific users to be members of this group and to have unique permissions. For the purposes of this article, we're using this option.
- **Dynamic user.** Lets you use dynamic membership rules to automatically add and remove members. If a member's attributes change, the system 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

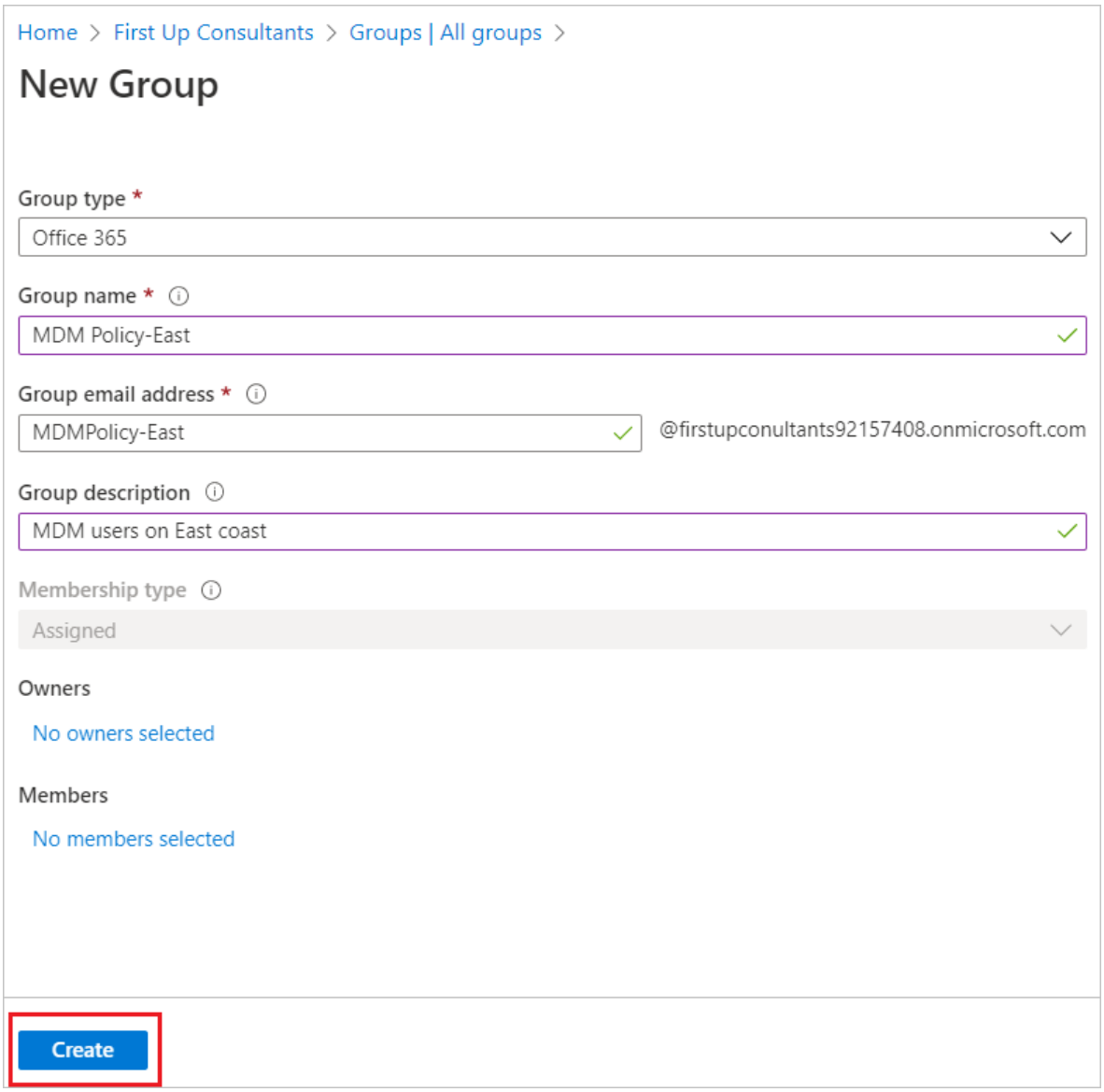
Create a basic group and add members

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**.



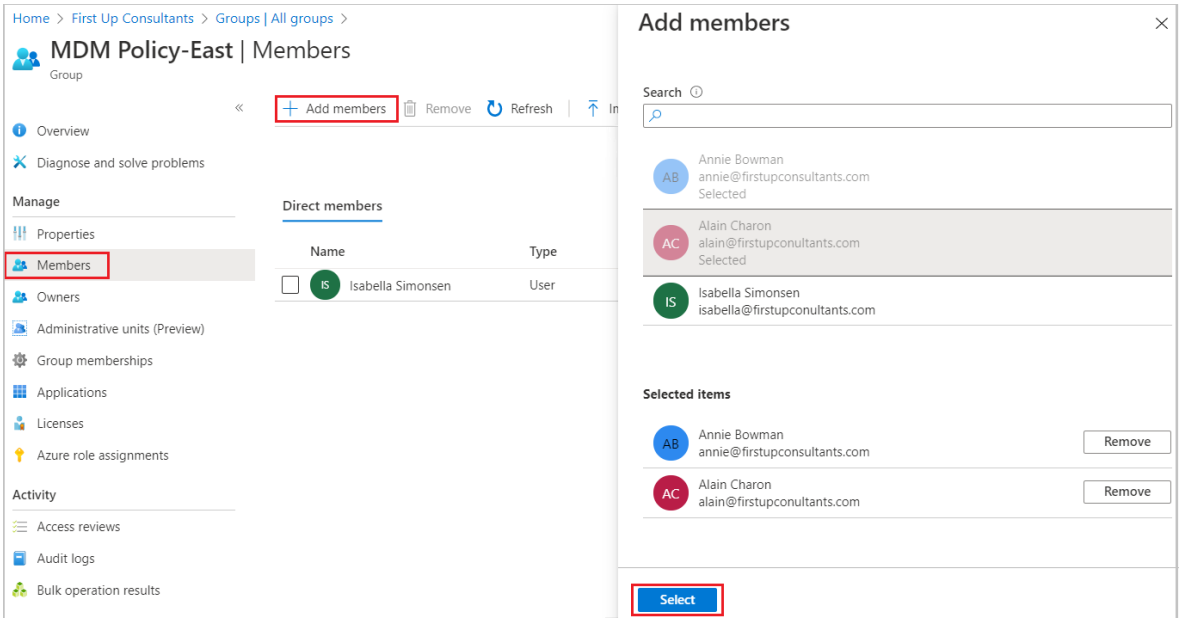
4. The **New Group** pane will appear and you must fill out the required information.



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.

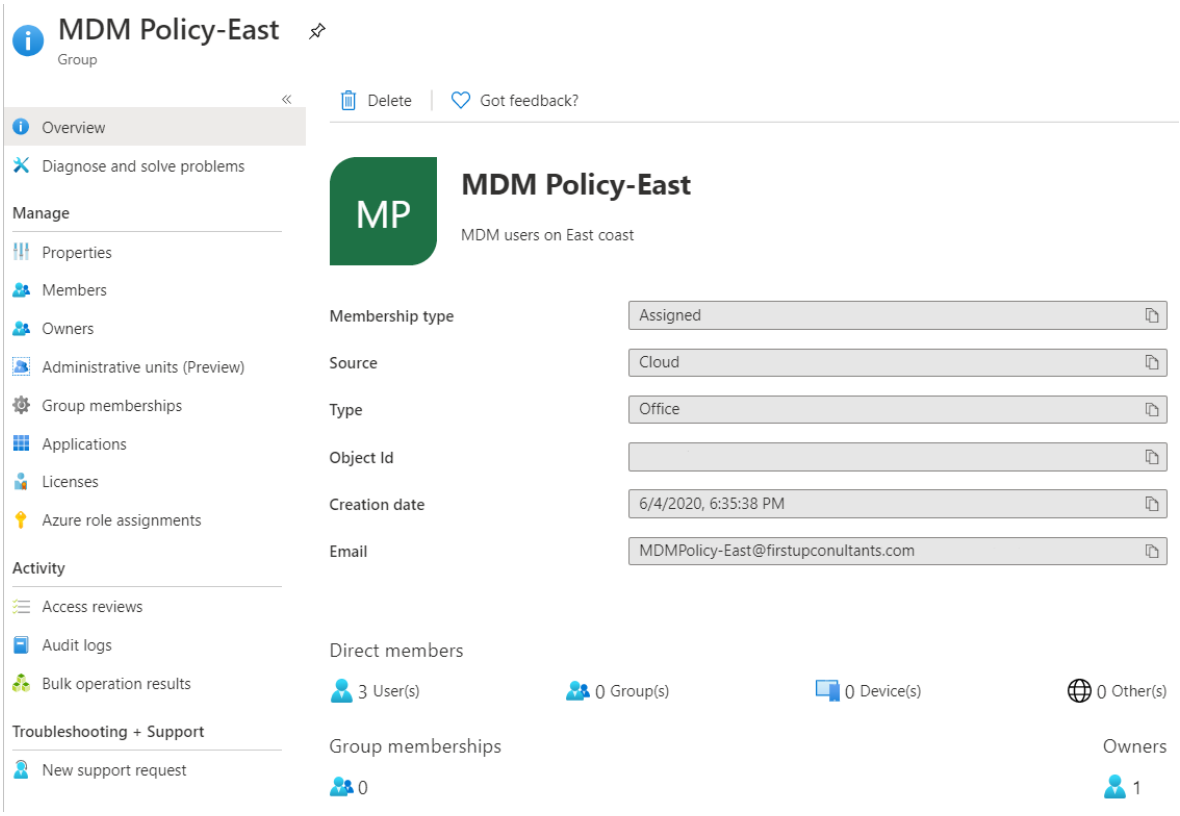
A check will be performed to determine if the name is already in use by another group. If the name is already in use, to avoid duplicate naming, you'll be asked to change the name of your group.

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.



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.



Turn on or off group welcome email

When any new Office 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

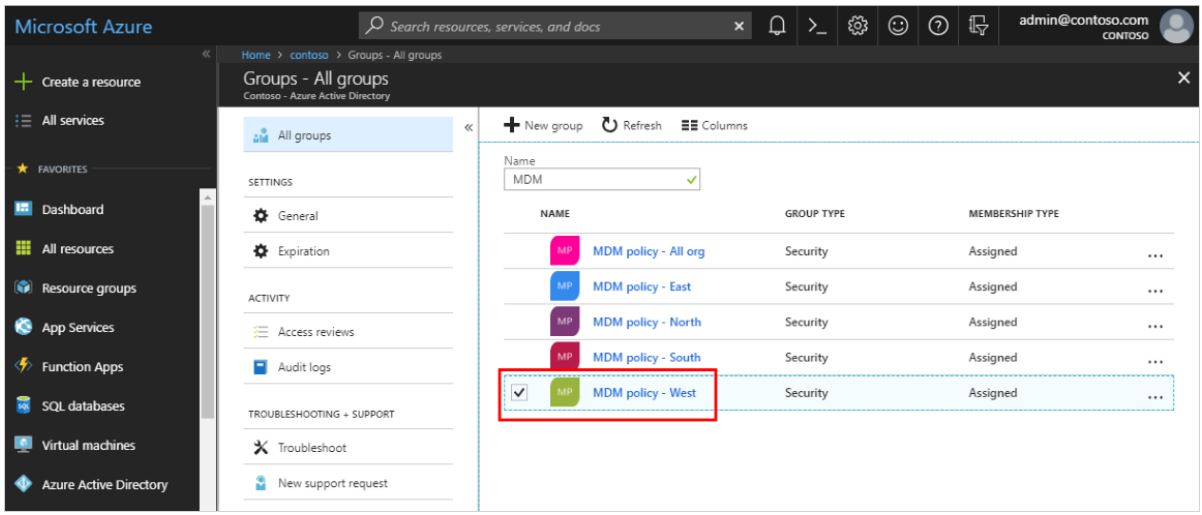
Add or remove group members using Azure Active Directory

7/20/2020 • 2 minutes to read • Edit Online

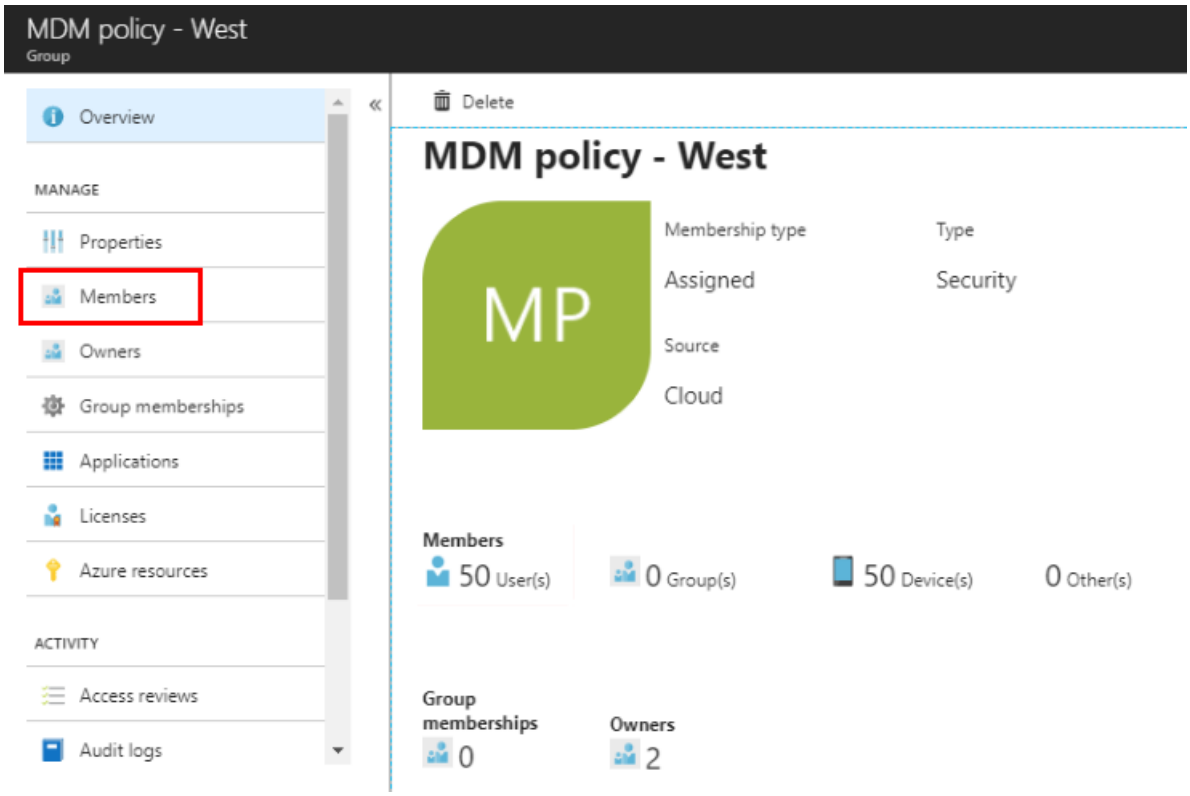
Using Azure Active Directory, you can continue to add and remove group members.

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**.

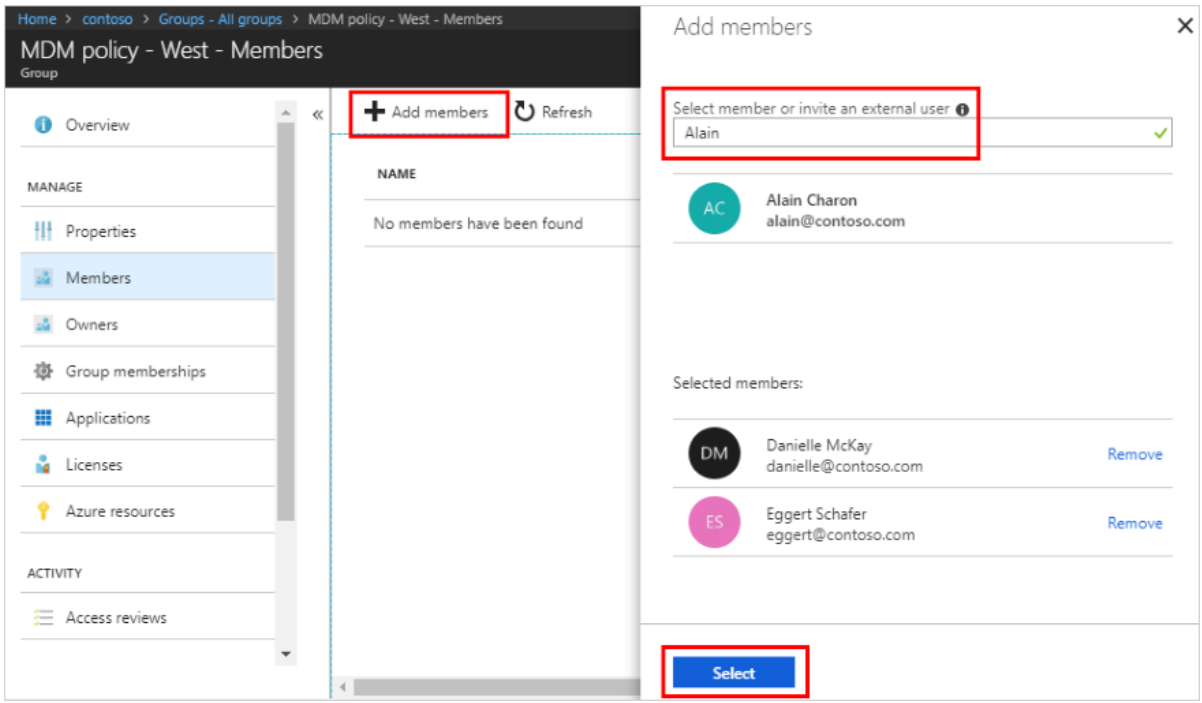


4. From the **MDM policy - West Overview** page, select **Members** from the **Manage** area.



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.

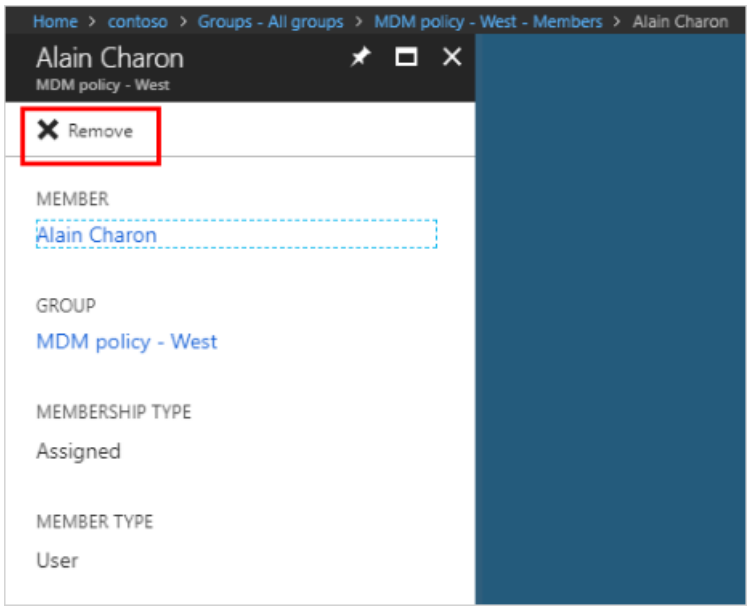


6. Refresh the screen to see all of the member names added to the group.

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**.



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

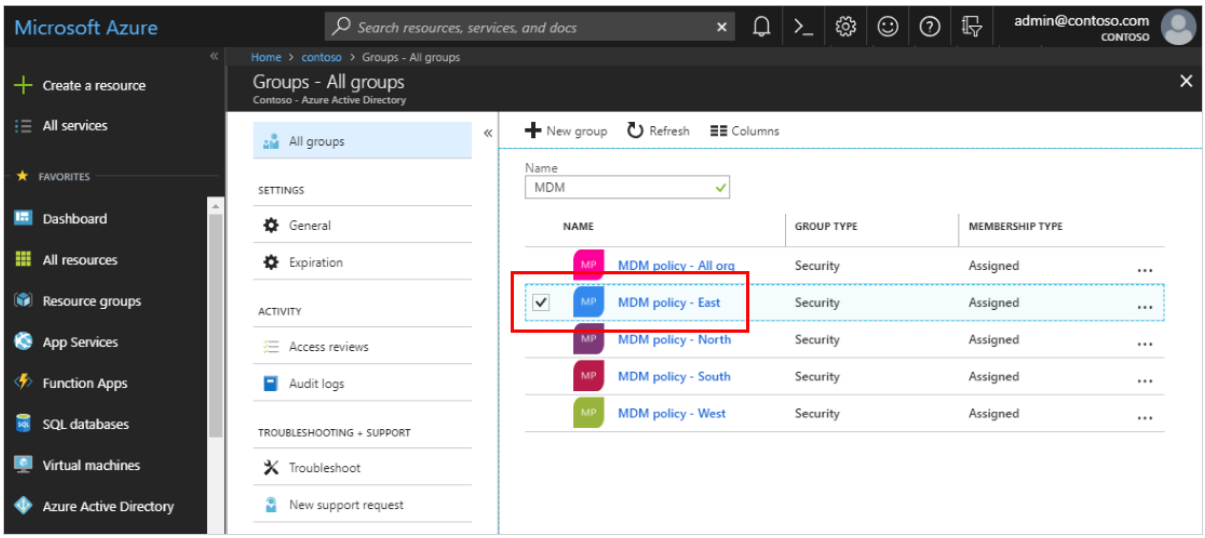
7/20/2020 • 2 minutes to read • Edit Online

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.

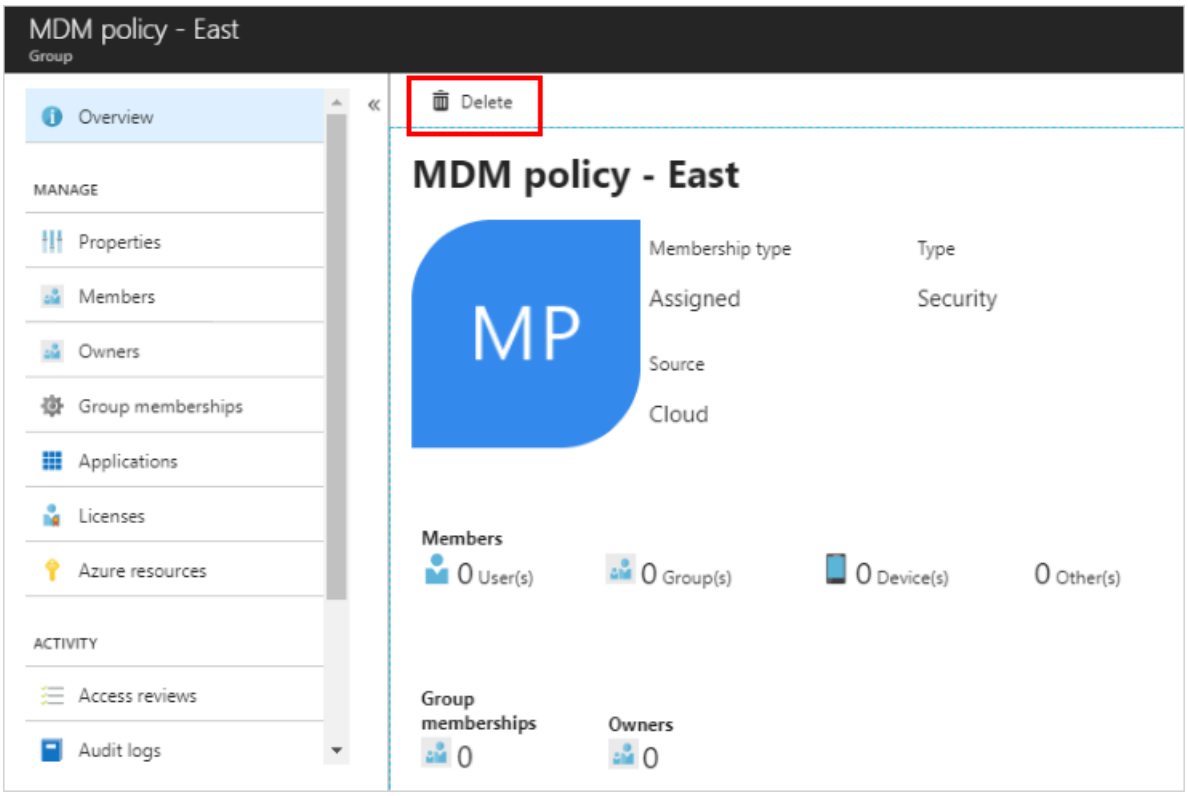
To delete a group

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**.



4. On the **MDM policy - East Overview** page, and then select **Delete**.

   The group is deleted from your Azure Active Directory tenant.



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 an Office 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

7/20/2020 • 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

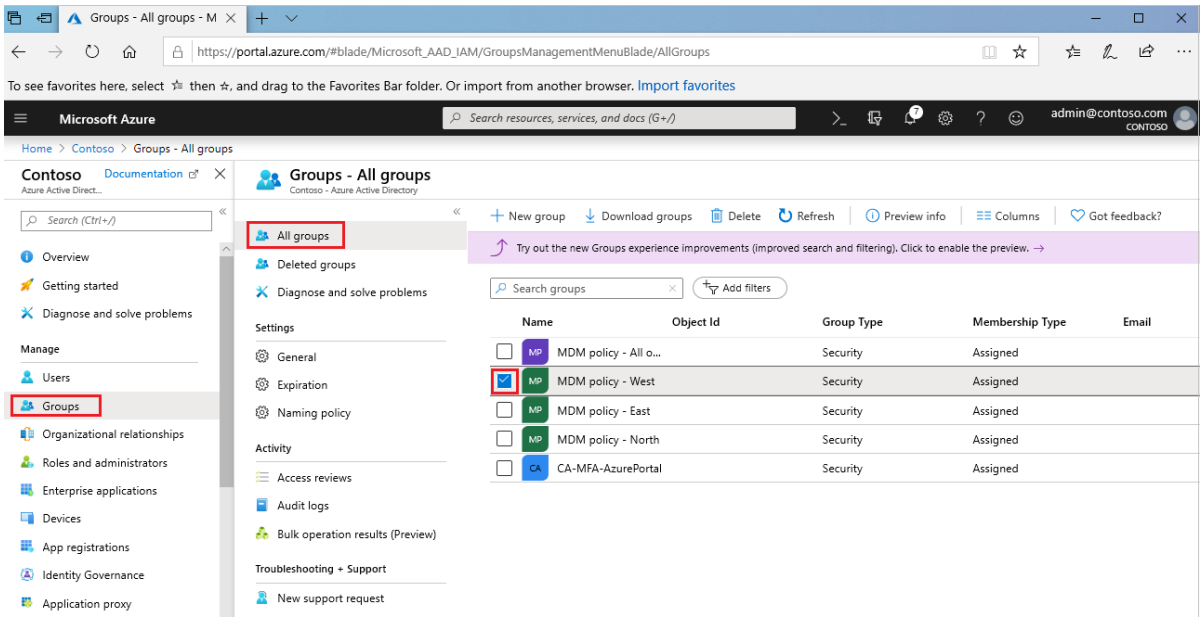
You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

> **IMPORTANT**
>
> We don't currently support:
>
> - Adding groups to a group synced with on-premises Active Directory.
> - Adding Security groups to Office 365 groups.
> - Adding Office 365 groups to Security groups or other Office 365 groups.
> - Assigning apps to nested groups.
> - Applying licenses to nested groups.
> - Adding distribution groups in nesting scenarios.

To add a group as a member of another group

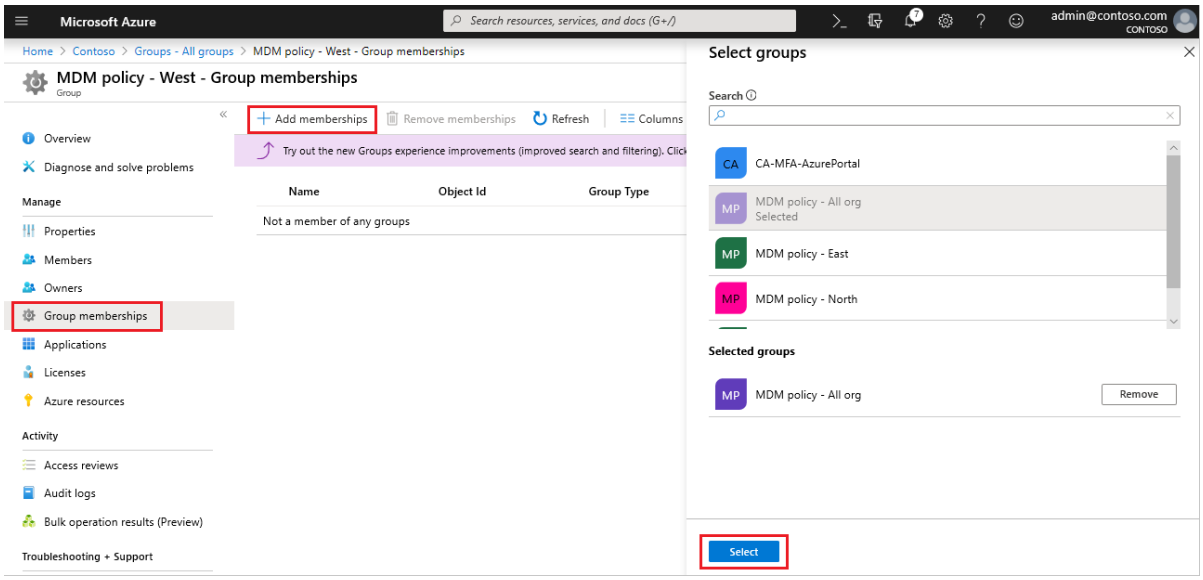
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.
3. On the **Groups - All groups** page, search for and select the group that's to become a member of another group. For this exercise, we're using the **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.



4. 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.



5. Review the **MDM policy - West - Group memberships** page to see the group and member relationship.

6. 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

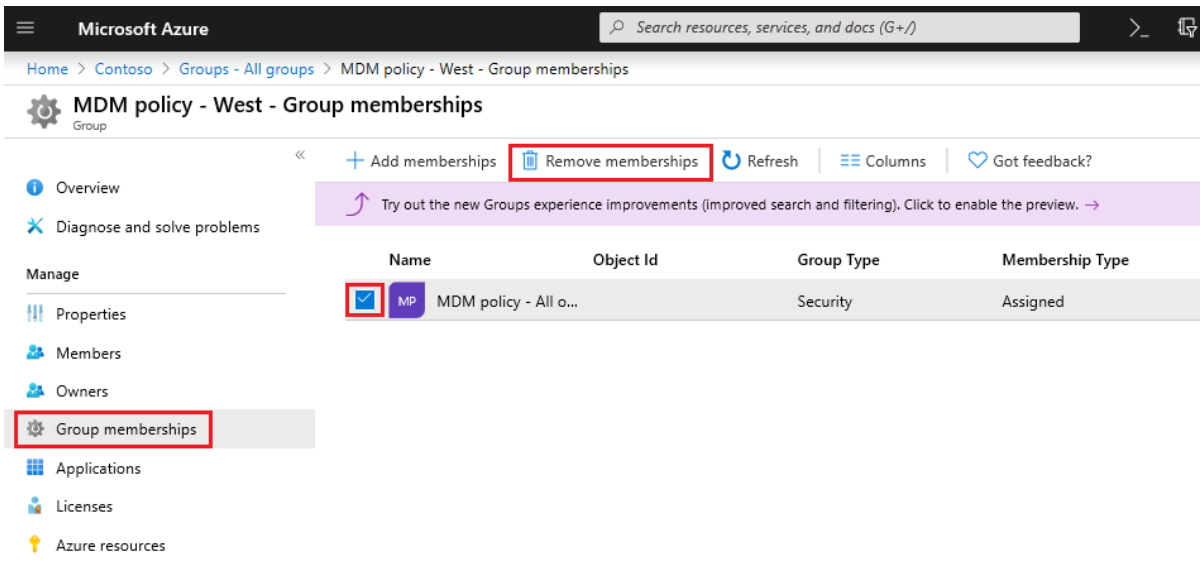
You can remove an existing Security group from another Security group. However, removing the group also removes any inherited attributes and properties for its members.

To remove a member group from another group

1. 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.

2. 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.



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

7/20/2020 • 2 minutes to read • Edit Online

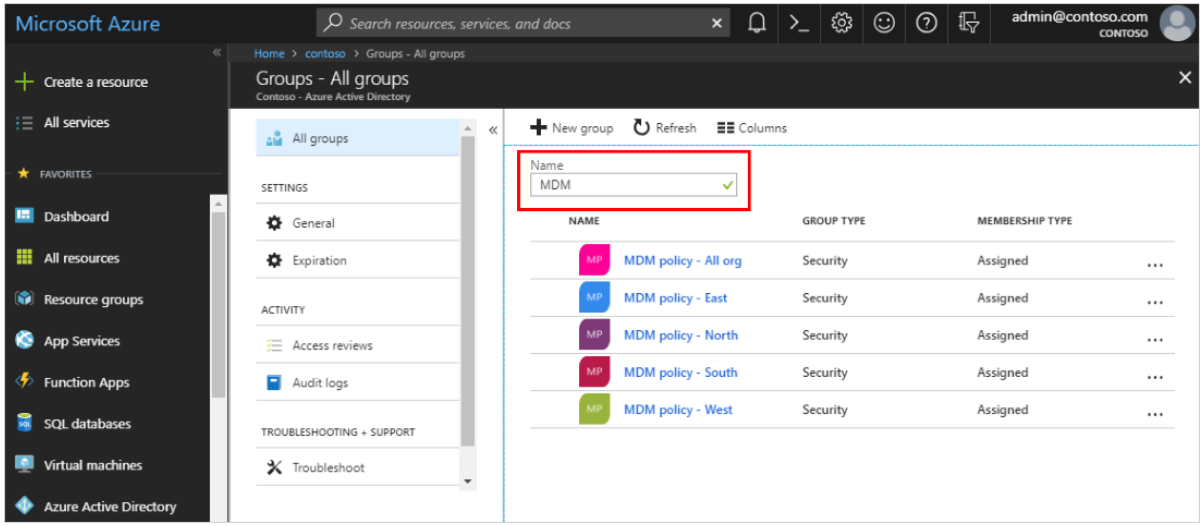
Using Azure Active Directory (Azure AD), you can edit a group's settings, including updating its name, description, or membership type.

To edit your group settings

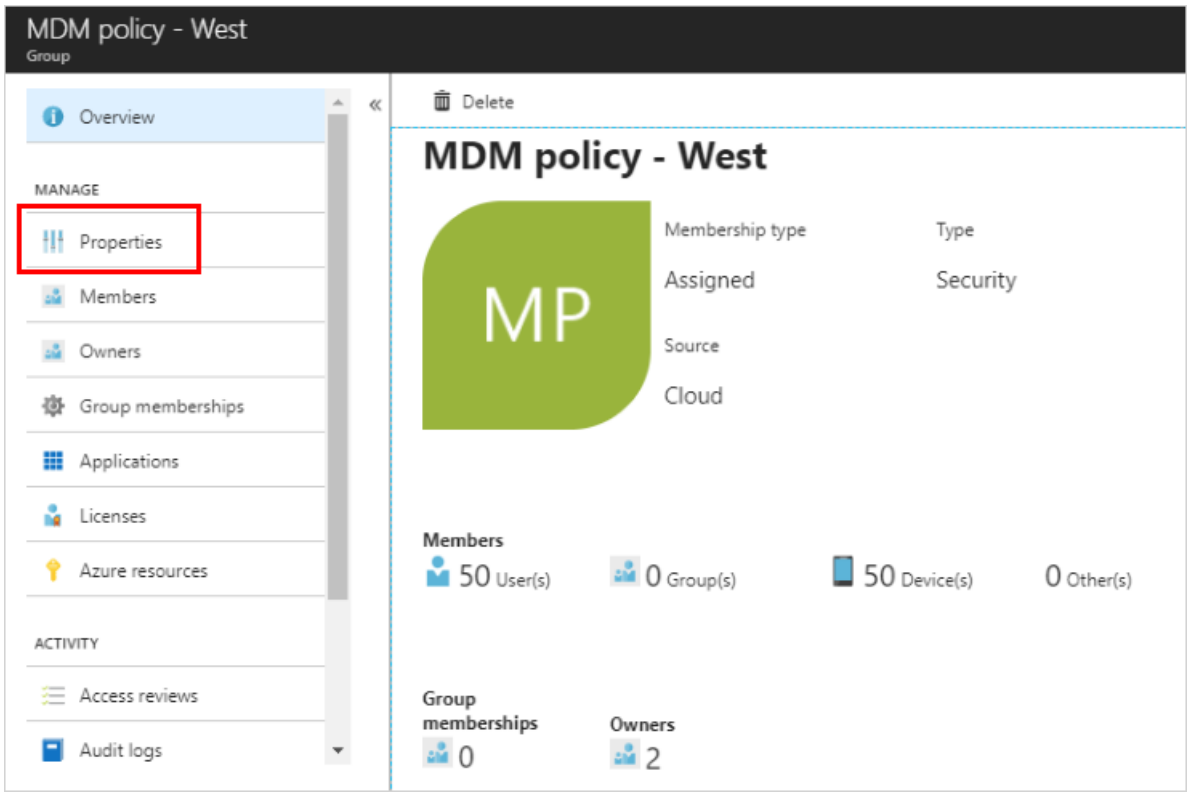
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.

   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.

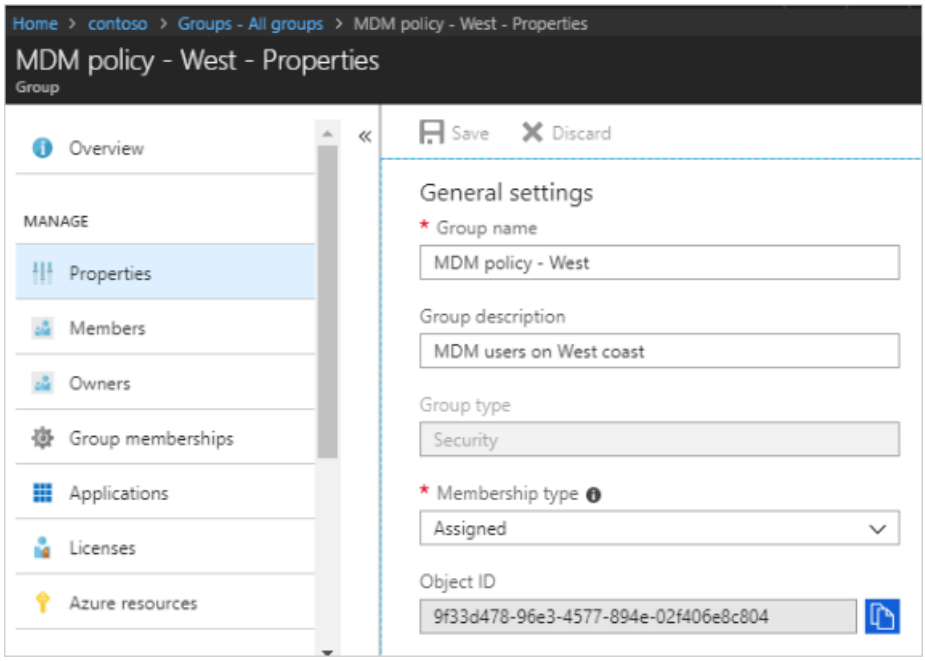
   The search results appear under the **Search** box, updating as you type more characters.



4. Select the group **MDM policy - West**, and then select **Properties** from the **Manage** area.



5. Update the **General settings** information as needed, including:



- **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

7/20/2020 • 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.

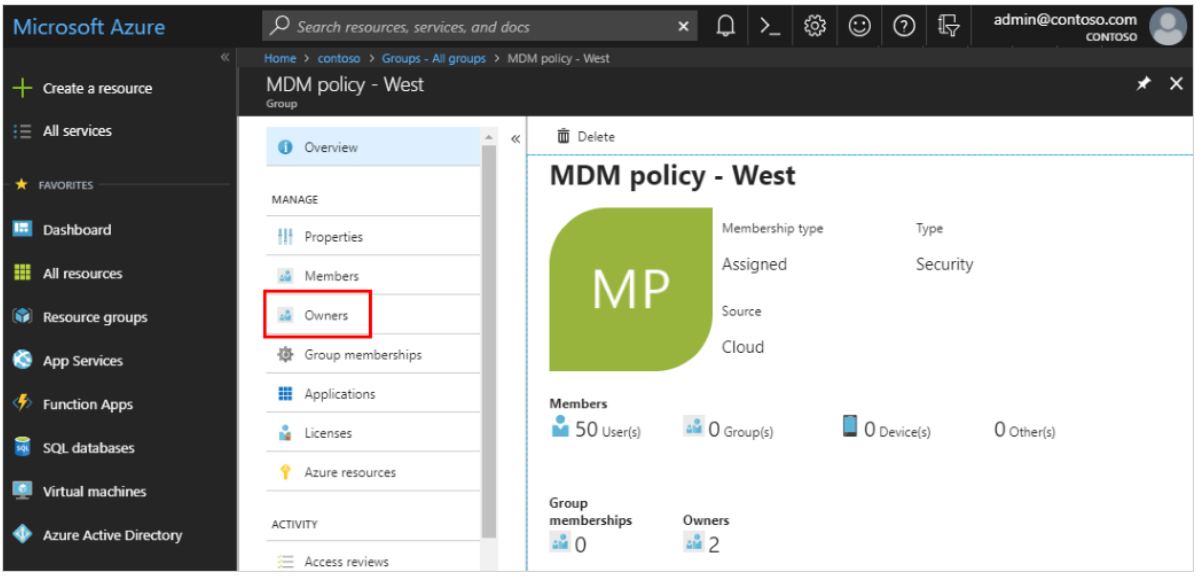
When a group has no owner, group-managing administrators are still able to manage the group. It is recommended for every group to have at least one owner. Once owners are assgined to a group, the last owner of the group cannot be removed. Please make sure to select another owner before removing the last owner from the group.

Add an owner to a group

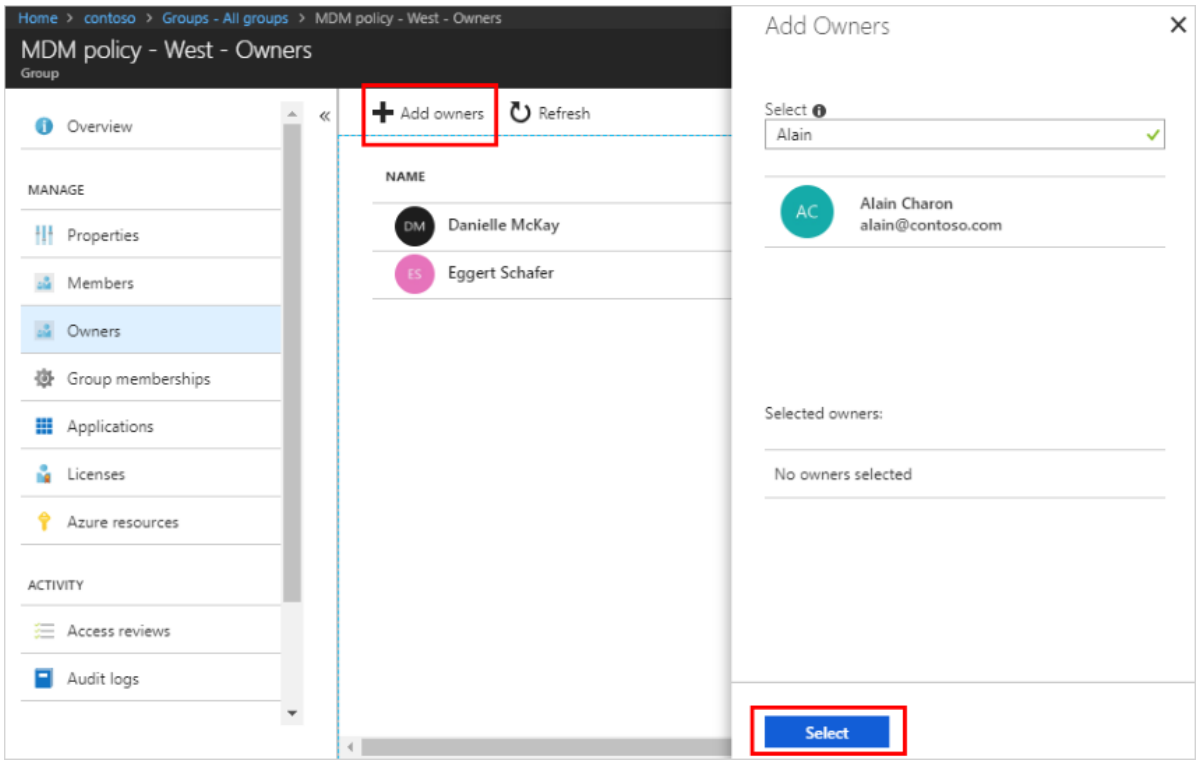
Below are instructions for adding a user as an owner to a group using the Azure AD portal. To add a service principal as an owner of a group, follow the instructions to do so using PowerShell.

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**.



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**.



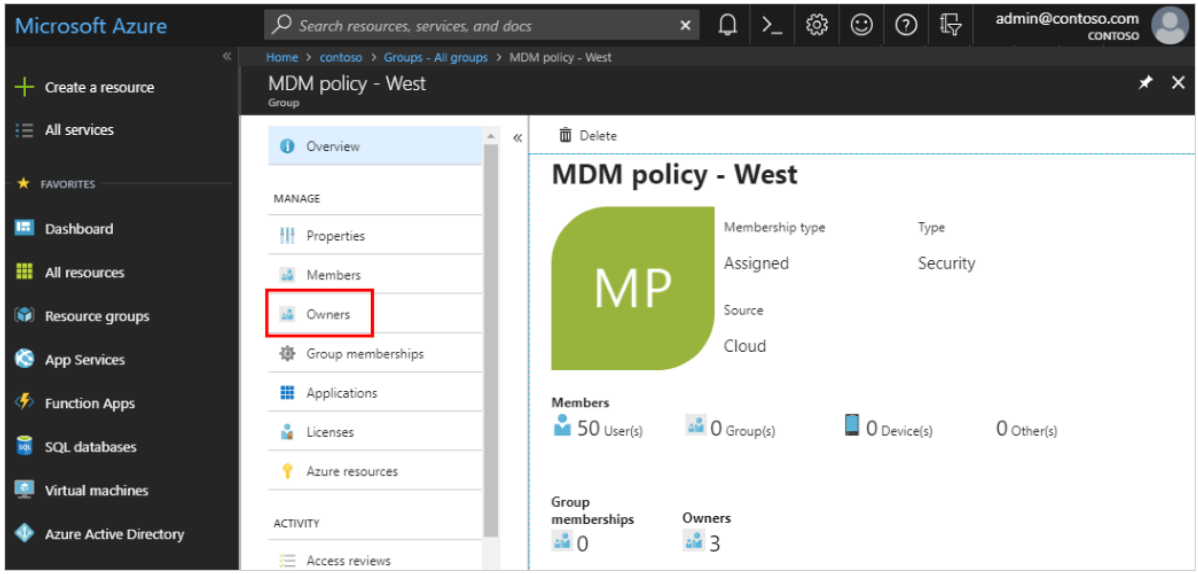
After you select the new owner, you can refresh the **Owners** page and see the name added to the list of owners.

Remove an owner from a group

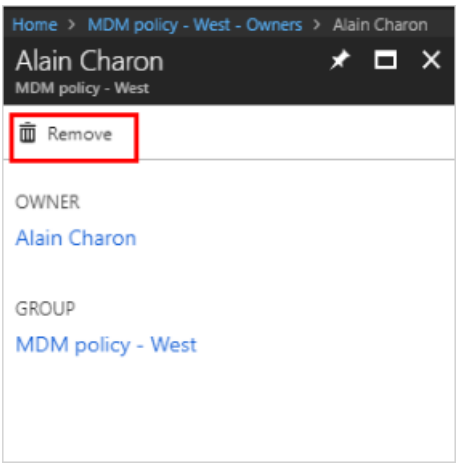
Remove an owner from a group using Azure AD.

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**.



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

4/8/2020 • 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.

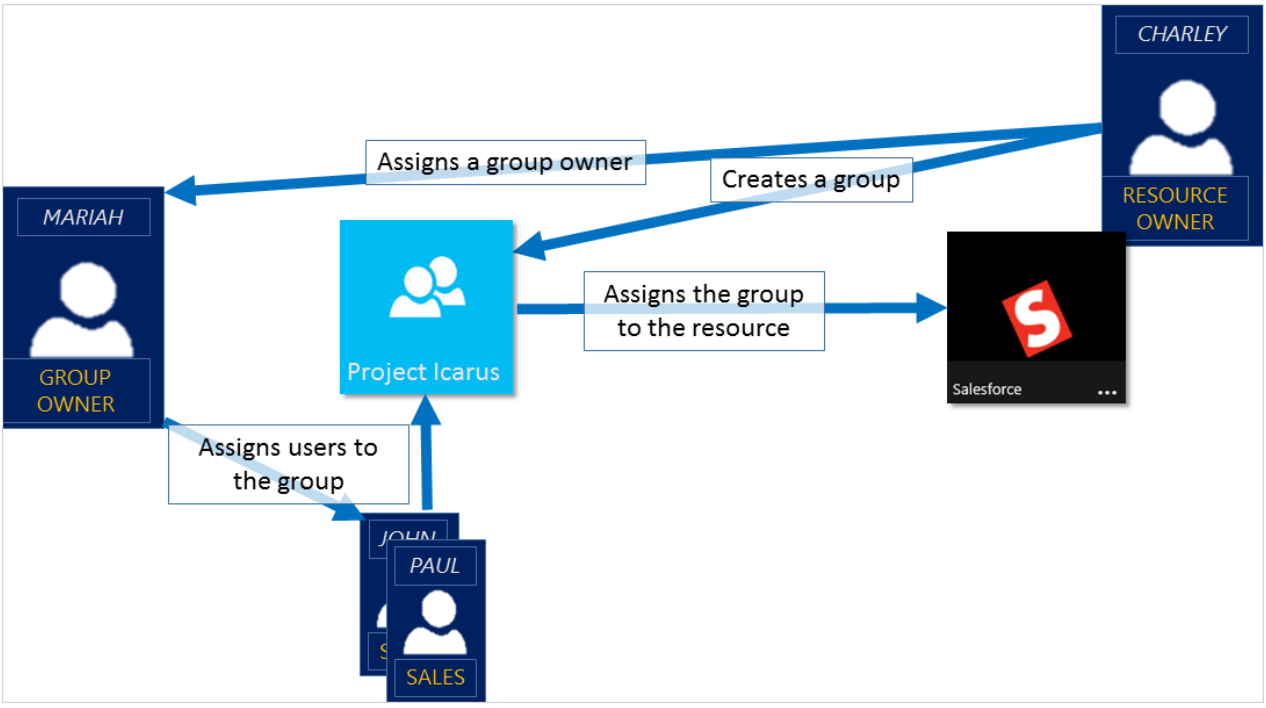
NOTE

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



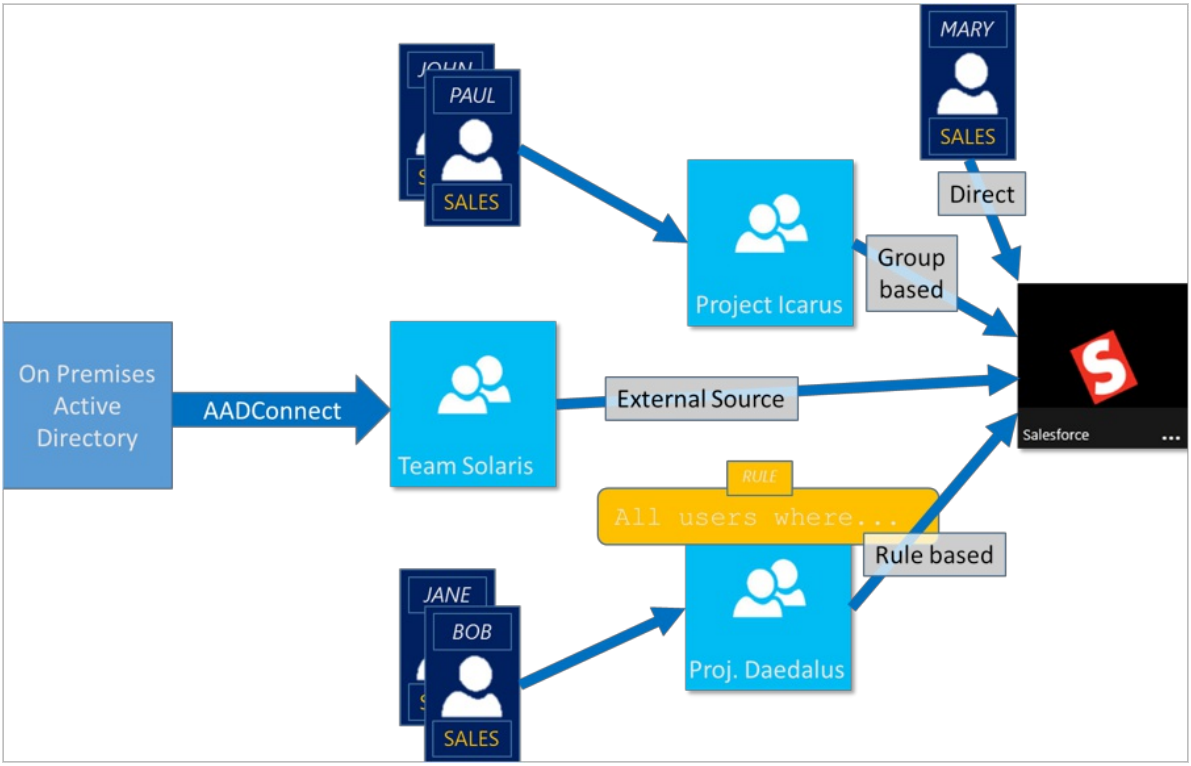
Ways to assign access rights

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 the resource. For more information, see Create a dynamic group and check status.

  You can also Watch this short video for a quick explanation about creating and using dynamic groups:

- **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 delete users using Azure Active Directory

7/20/2020 • 3 minutes to read • Edit Online

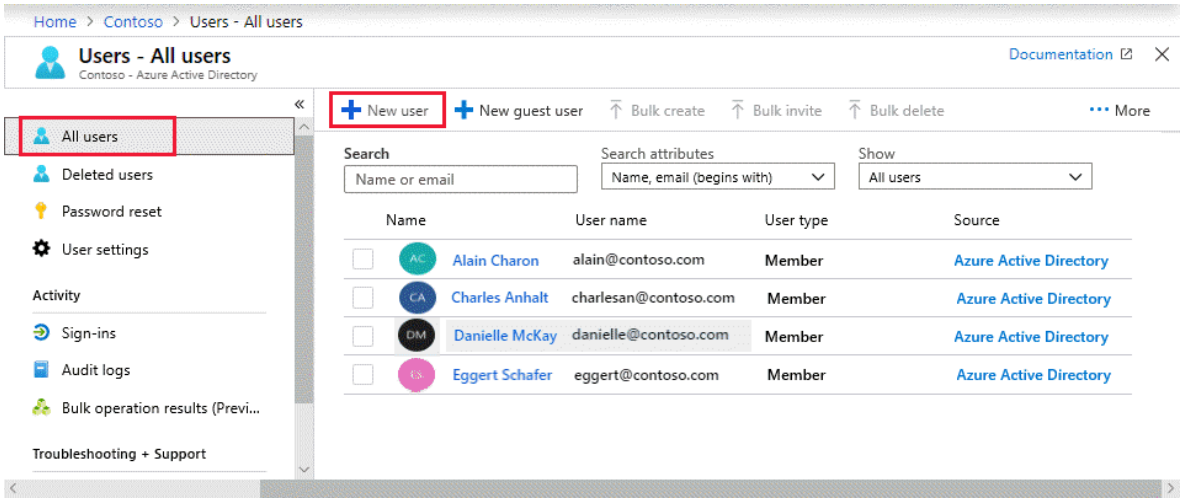
Add new users or delete existing users from your Azure Active Directory (Azure AD) organization. To add or delete users you must be a User administrator or Global administrator.

Add a new user

You can create a new user using the Azure Active Directory portal.

To add a new user, follow these steps:

1. Sign in to the Azure portal as a User administrator for the organization.
2. Search for and select *Azure Active Directory* from any page.
3. Select **Users**, and then select **New user**.



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.

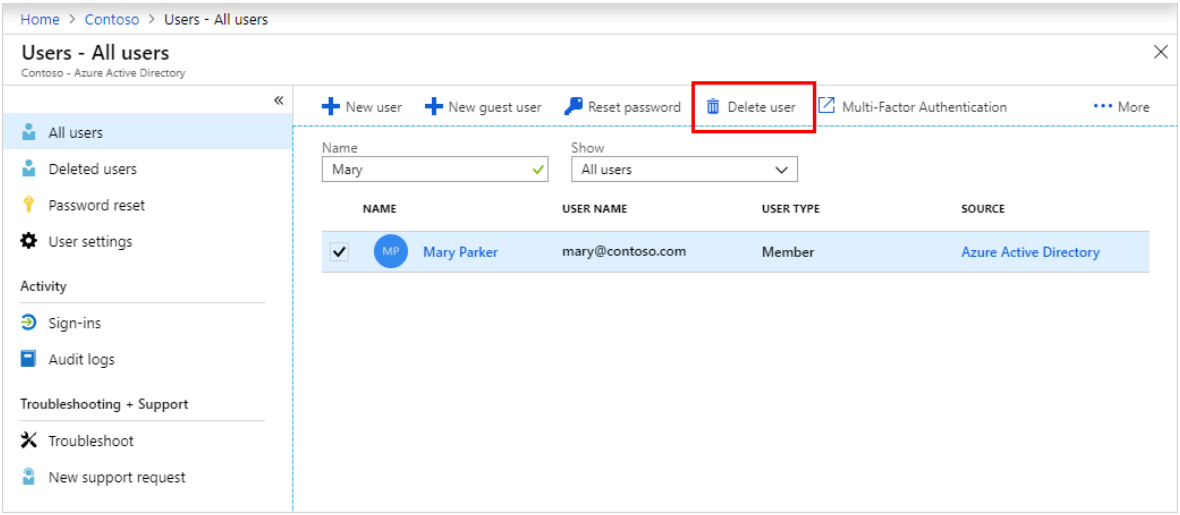
To delete a user, follow these steps:

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 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**
>
> You must use Windows Server Active Directory to update the identity, contact information, or job information 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 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

7/20/2020 • 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.

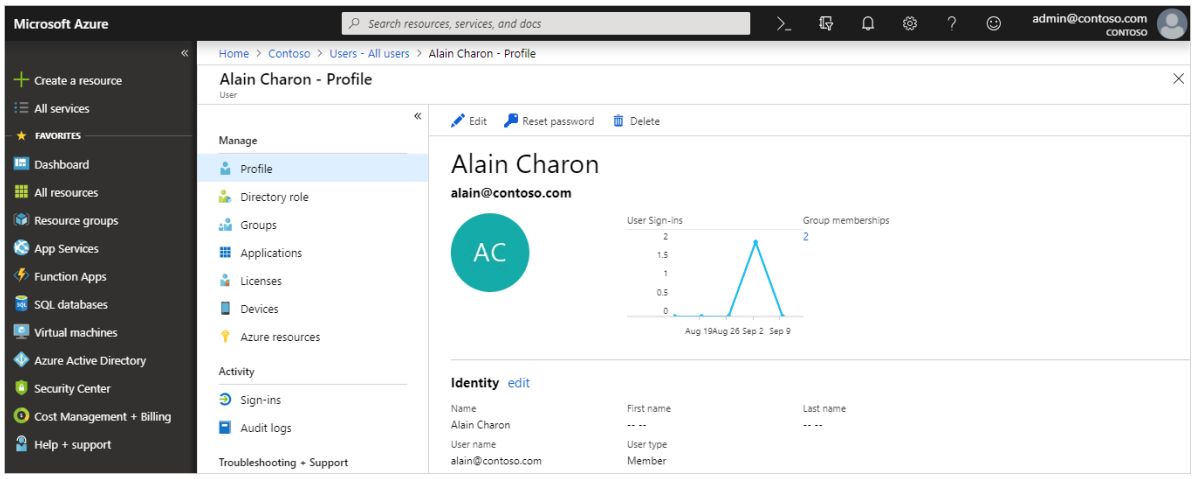
Add or change profile information

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.

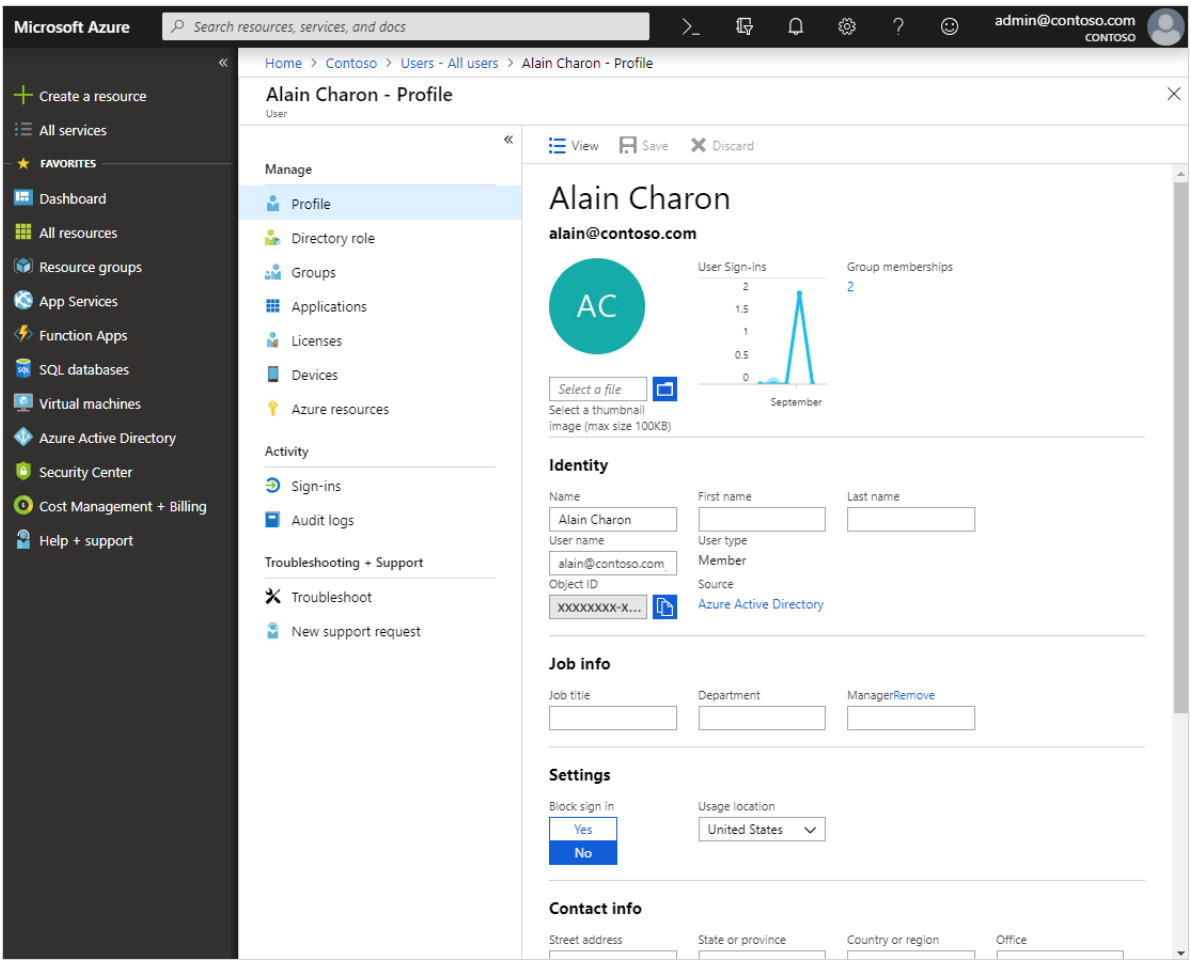
To add or change profile information

1. Sign in to the Azure portal as a User administrator 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.



3. Select **Edit** to optionally add or update the information included in each of the available 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

7/20/2020 • 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.

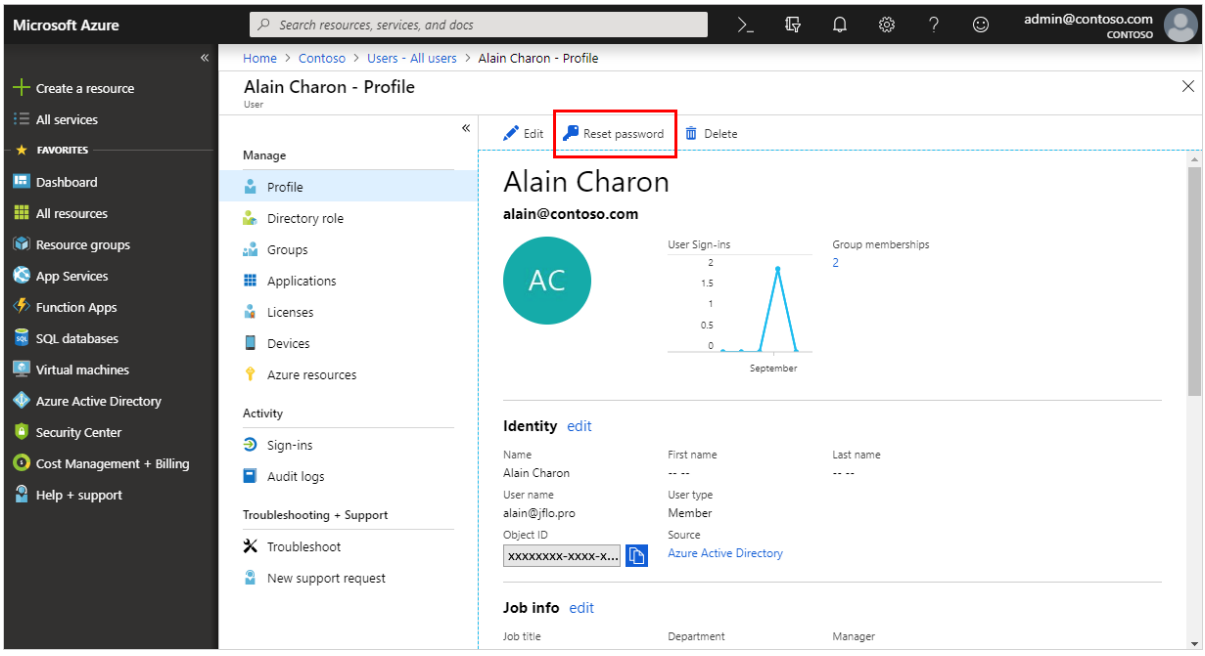
> **NOTE**
>
> Unless your Azure AD tenant is the home directory for a user, you won't be able reset their password. This means that if your user is signing in to your organization using an account from another organization, a Microsoft account, or a Google account, you won't be able to reset their password.
>
> 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 adminsitrator 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 Assigning administrator roles in Azure Active Directory
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.



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.

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

7/20/2020 • 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.

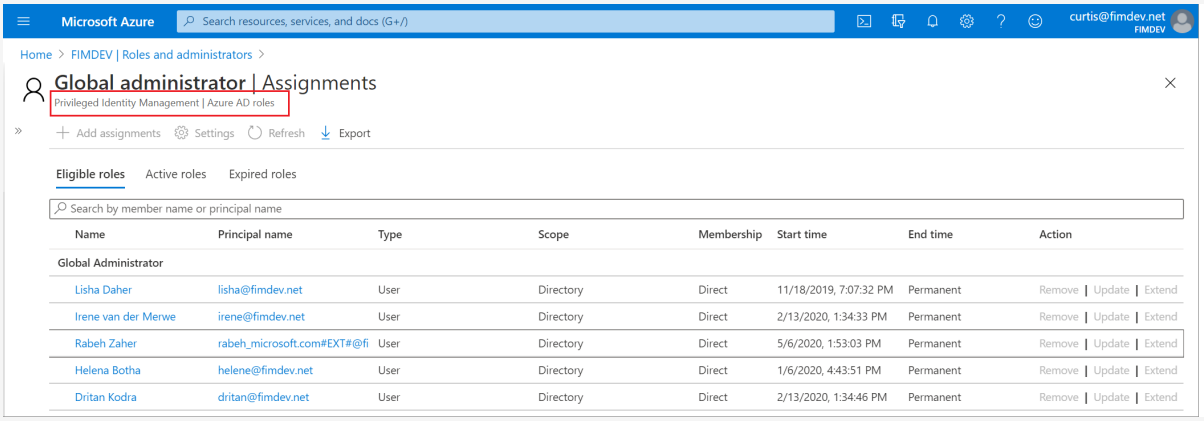
For more information about the available Azure AD roles, see Assigning administrator roles in Azure Active Directory. To add users, see Add new users to Azure Active Directory.

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 the 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.

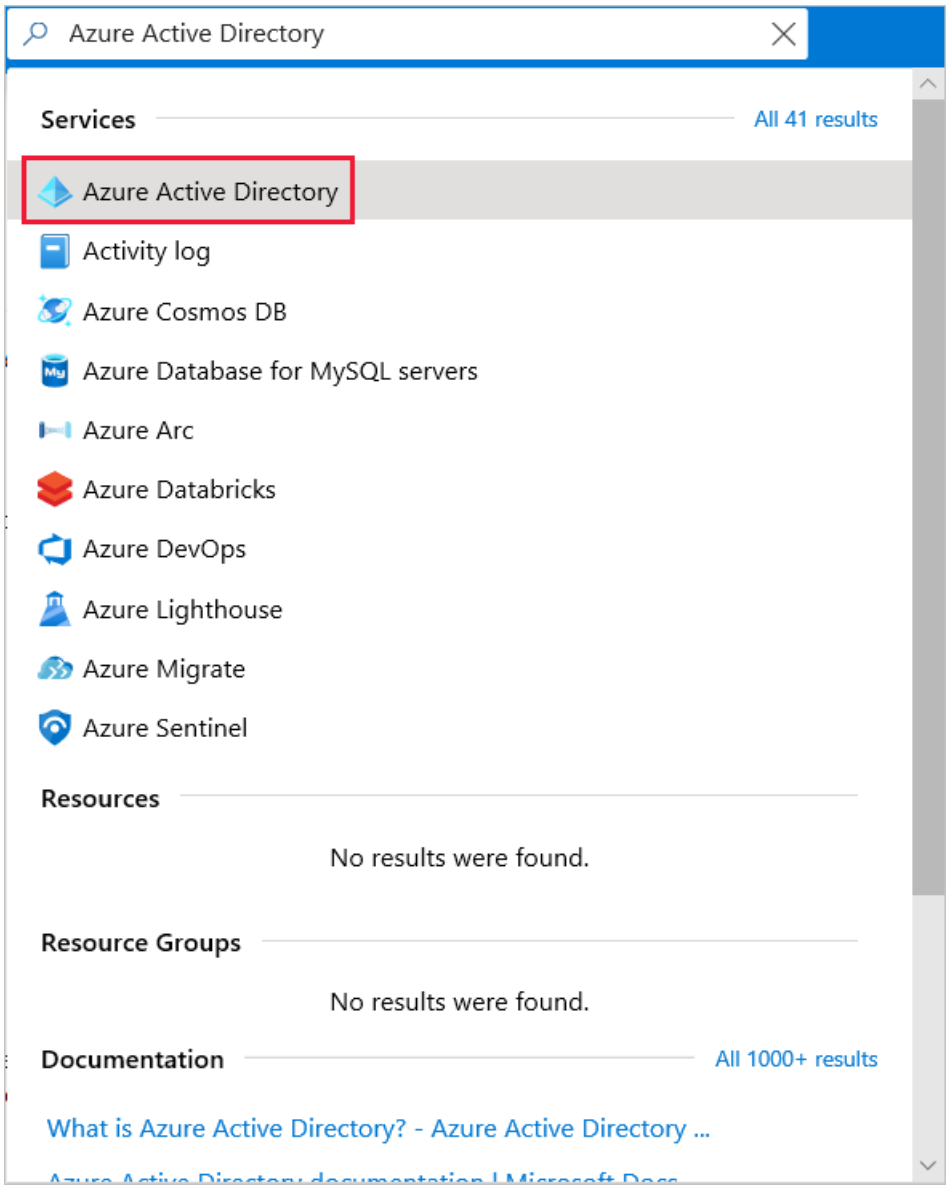
NOTE

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.



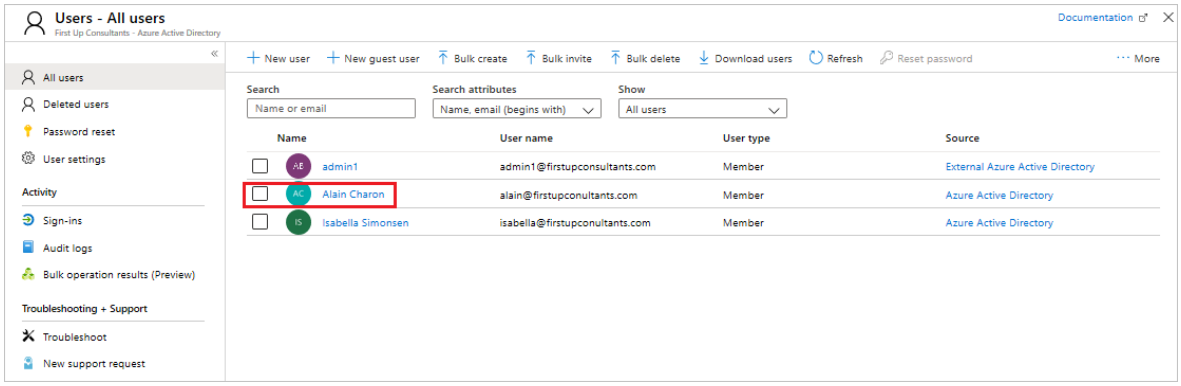
Assign a role to a user

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**.



3. Select **Users**.

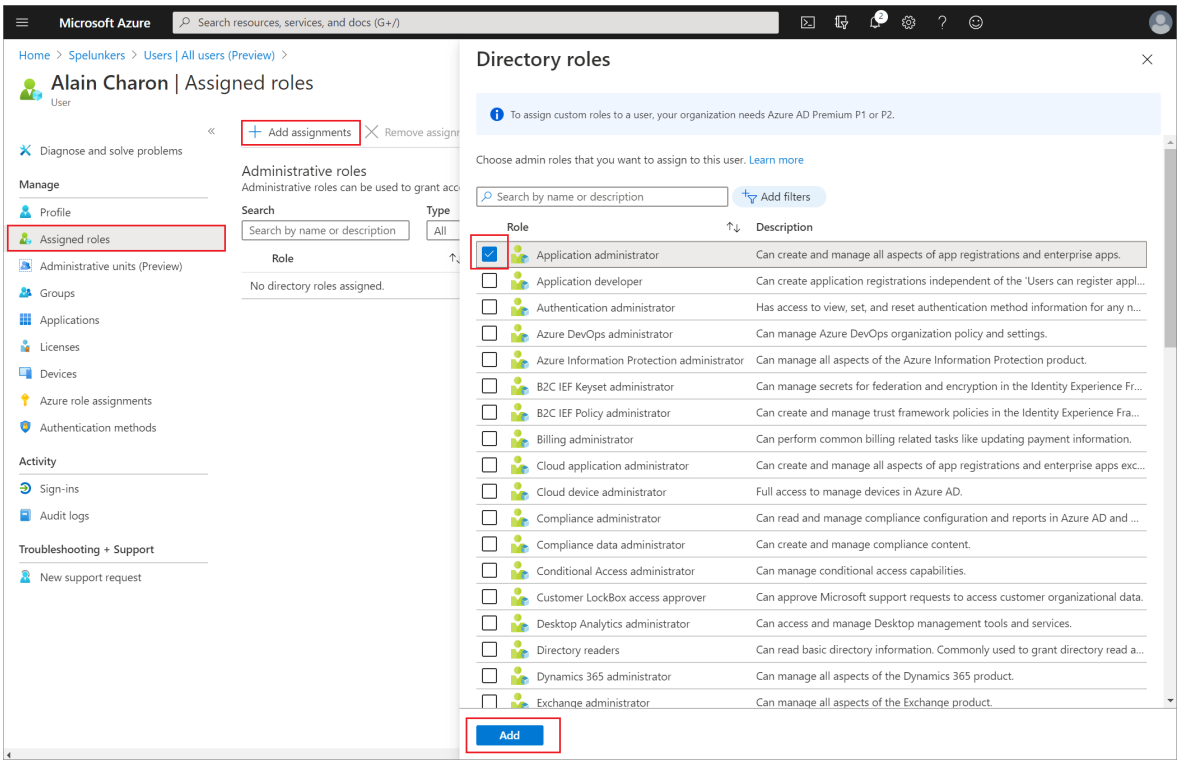
4. Search for and select the user getting the role assignment. For example, *Alain Charon*.



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**.



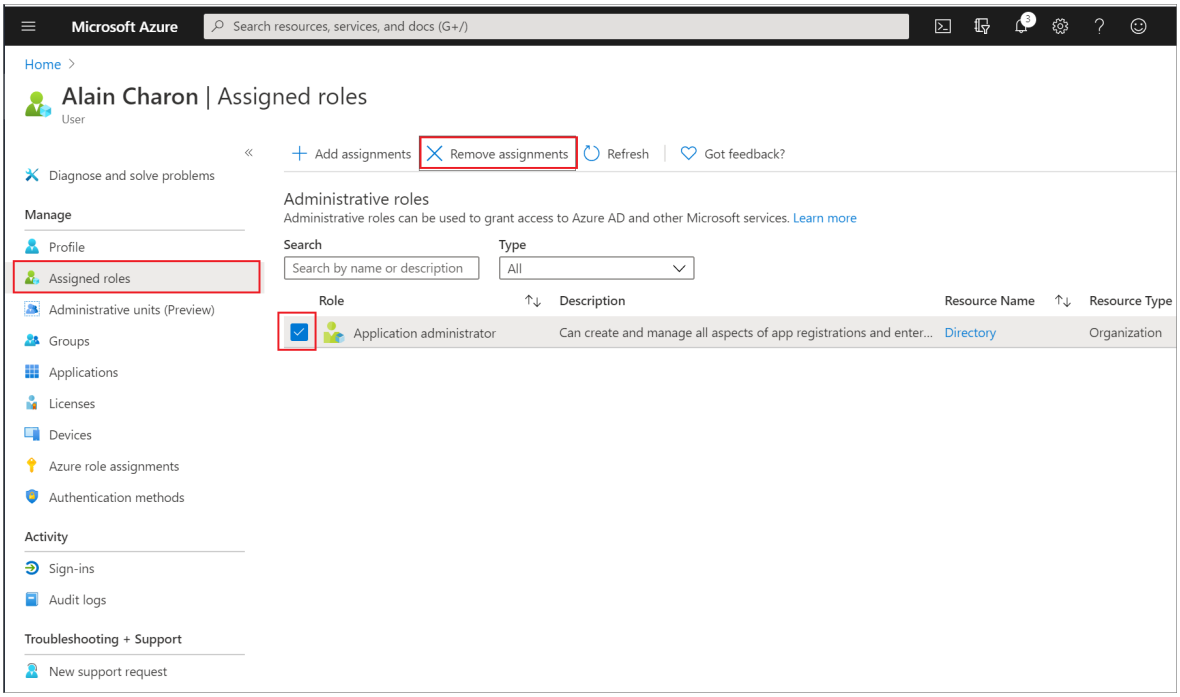
The Application administrator role is assigned to Alain Charon and it appears on the **Alain Charon - Administrative roles** page.

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.

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

7/20/2020 • 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?.

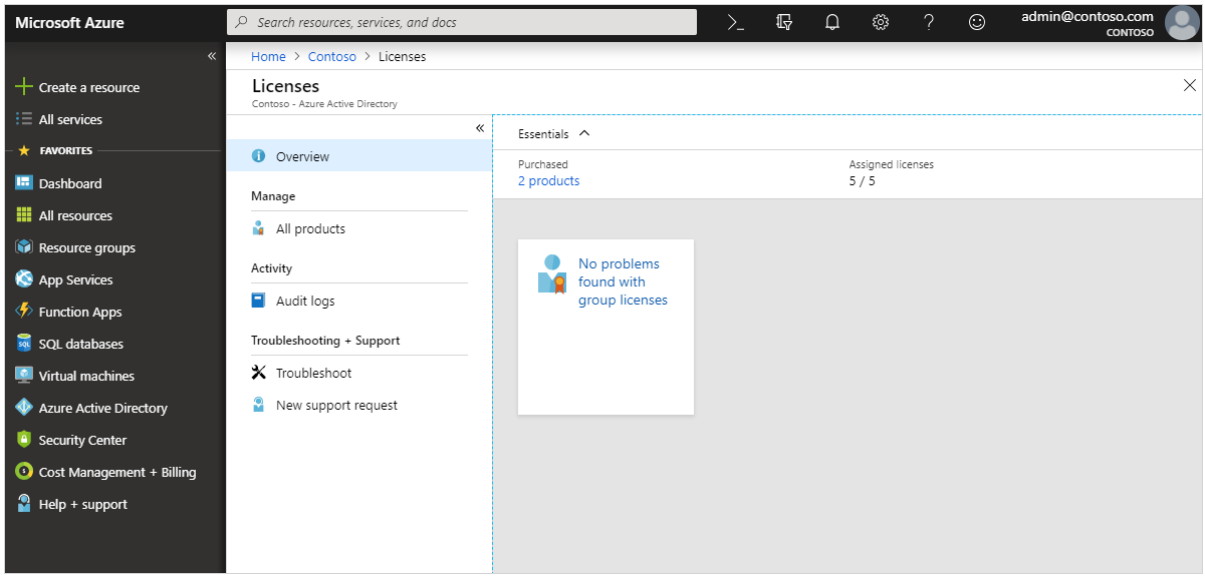
Not all Microsoft services are available in all locations. Before a license can be assigned to a group, you must specify the **Usage location** for all members. You can set this value in the **Azure Active Directory > Users > Profile > Settings** area in Azure AD. Any user whose usage location is not 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.

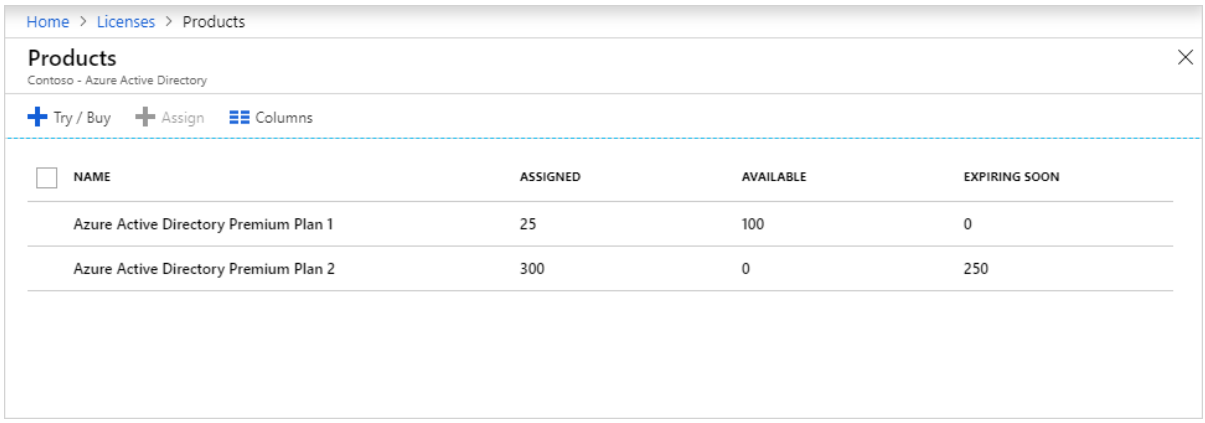
To find your service plan and plan details

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 the **Purchased** link to view the **Products** page and to see the **Assigned**, **Available**, and **Expiring**

soon numbers for your license plans.



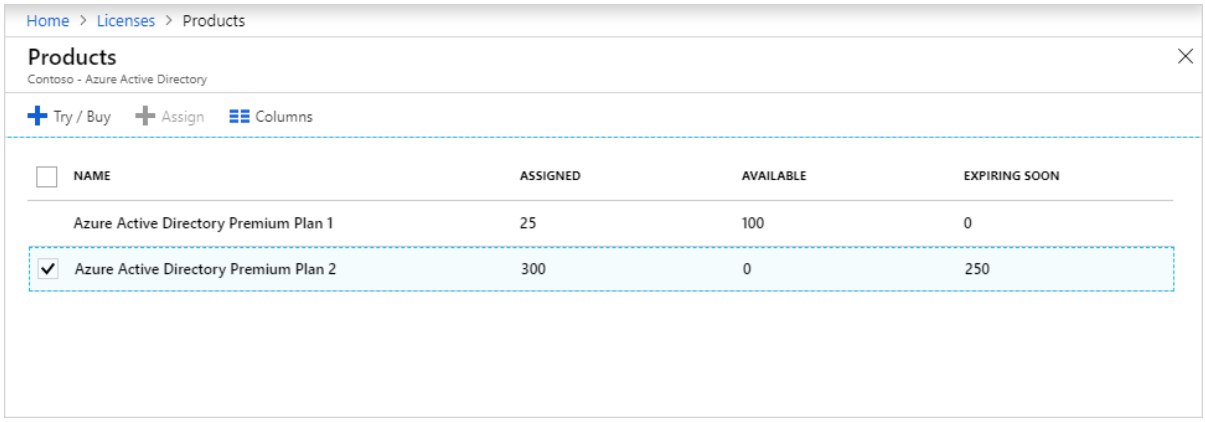
4. Select a plan name to see its licensed users and groups.

Assign licenses to users or groups

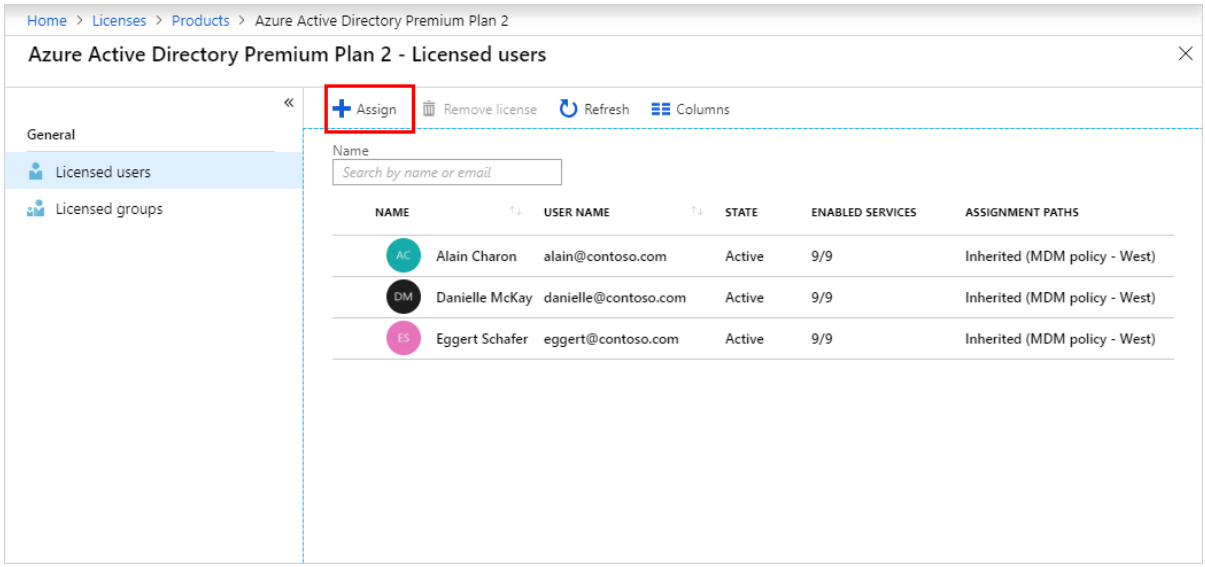
Make sure that anyone needing to use a licensed Azure AD service has the appropriate license. You can add the licensing rights to users or to an entire group.

To assign a license to a user

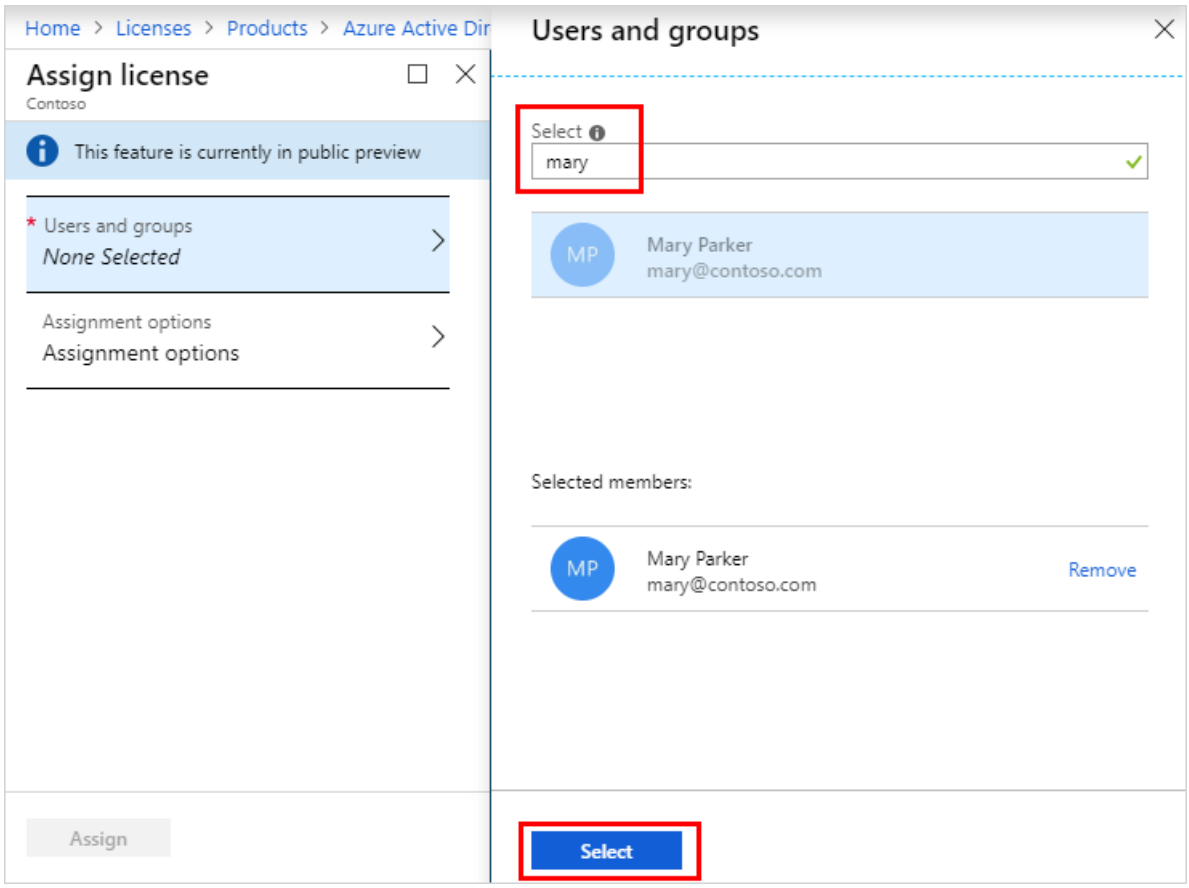
1. On the **Products** page, select the name of the license plan you want to assign to the user.



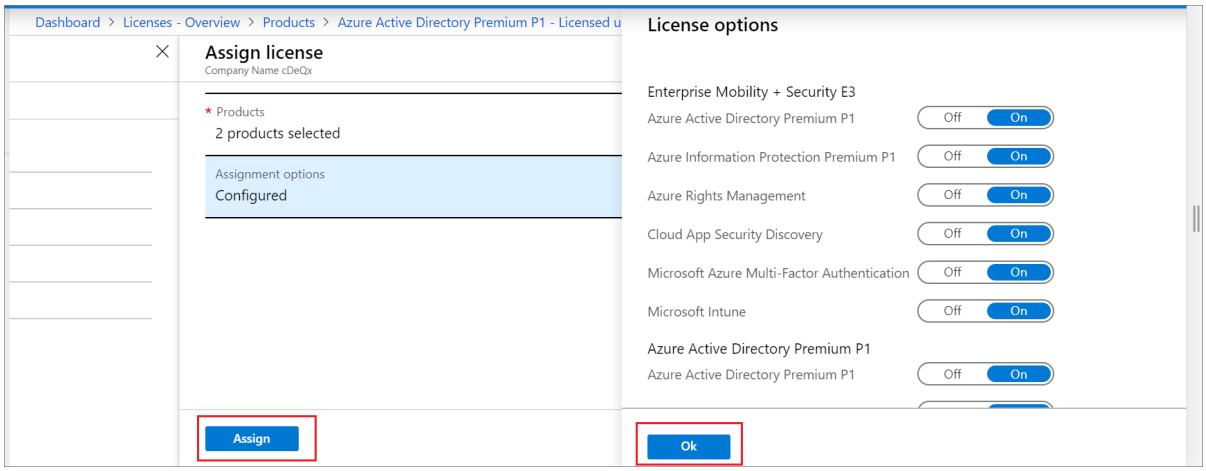
2. On the license plan overview page, select **Assign**.



3. On the **Assign** page, select **Users and groups**, and then search for and select the user you're assigning the license.



4. Select **Assignment options**, make sure you have the appropriate license options turned on, and then select **OK**.



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.

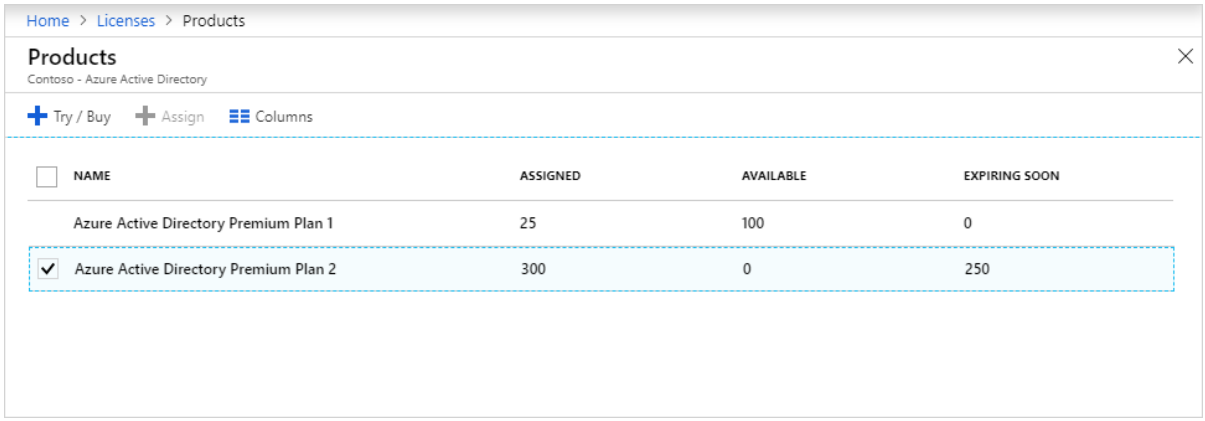
5. Select **Assign**.

The user is added to the list of licensed users and has access to the included Azure AD services.

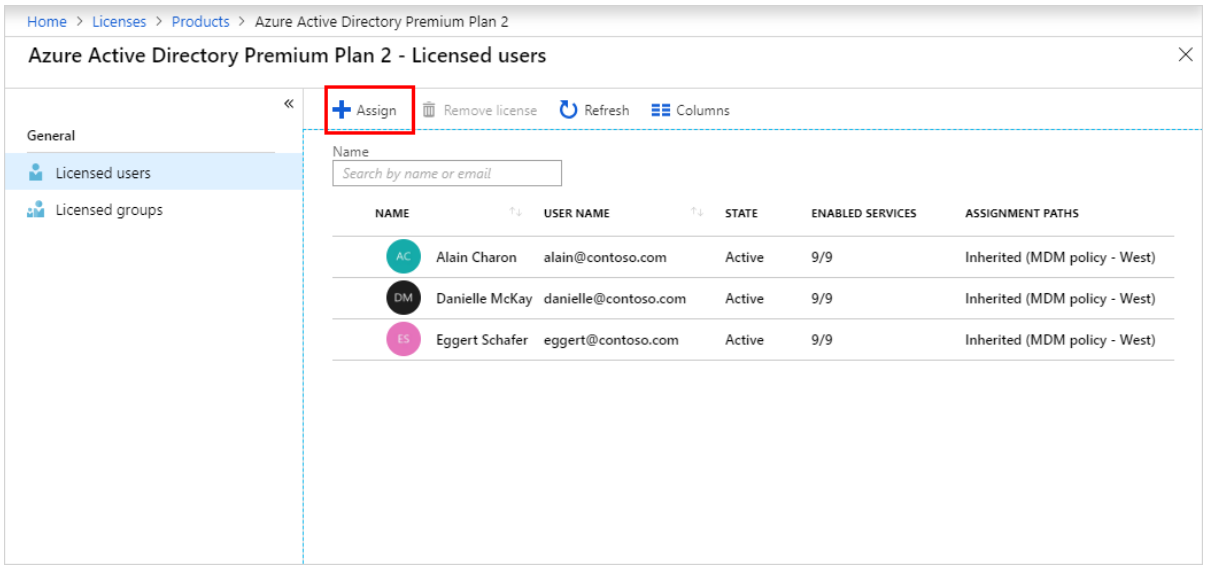
> **NOTE**
>
> Licenses can also be assigned directly to a user from the user's **Licenses** page. If a user has a license assigned through a group membership and you want to assign the same license to the user directly, it can be done only from the **Products** page mentioned in step 1 only.

To assign a license to a group

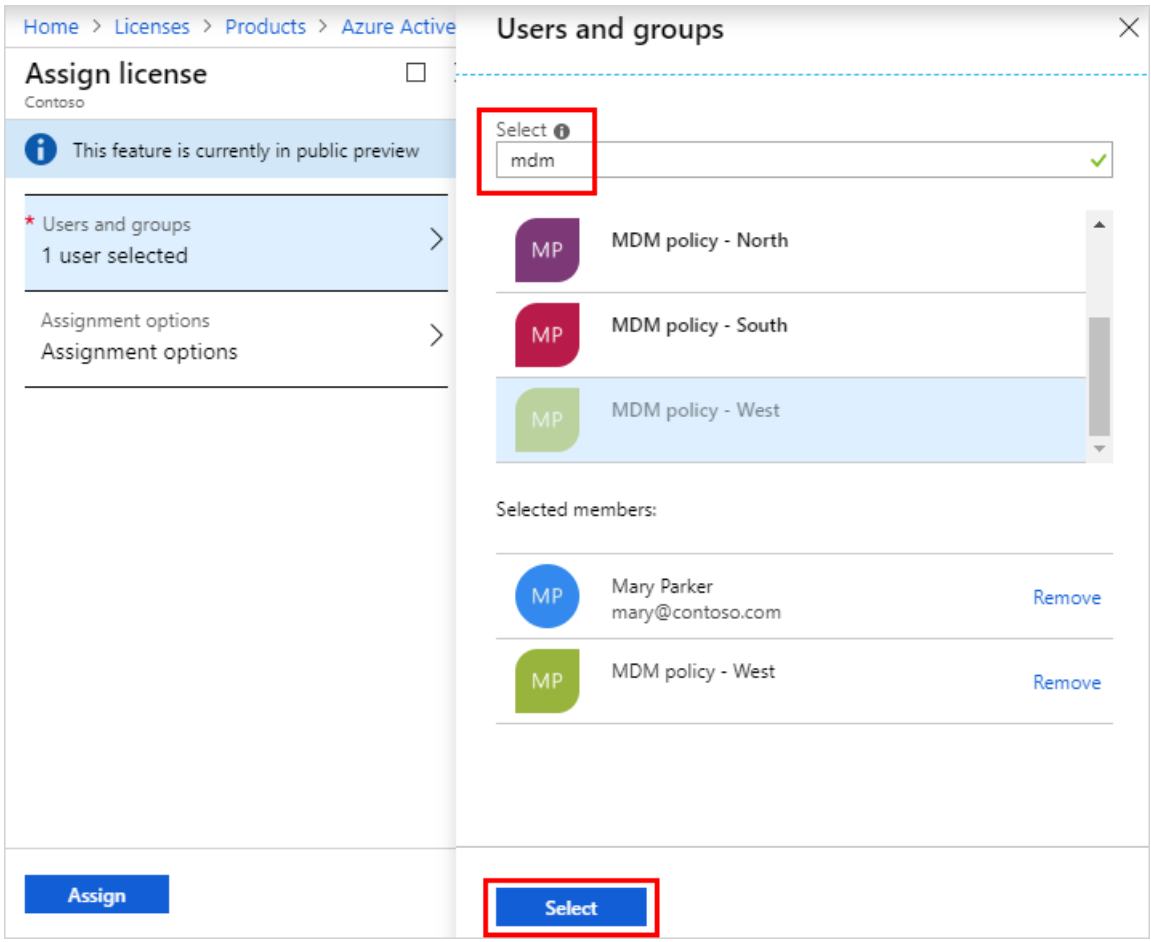
1. On the **Products** page, select the name of the license plan you want to assign to the user.



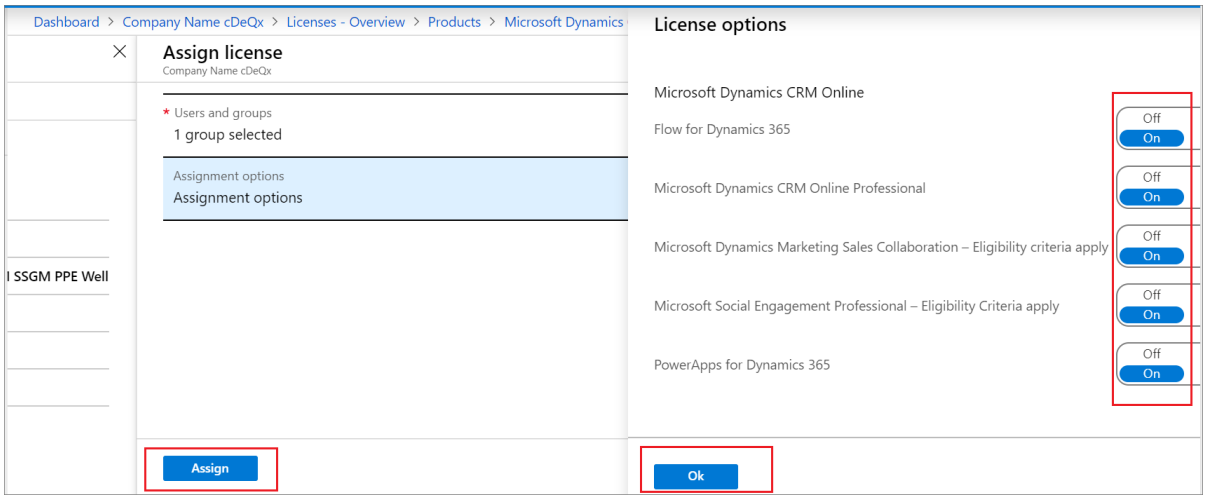
2. On the **Azure Active Directory Premium Plan 2** page, select **Assign**.



3. On the **Assign** page, select **Users and groups**, and then search for and select the group you're assigning the license.



4. Select **Assignment options**, make sure you have the appropriate license options turned on, and then select **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

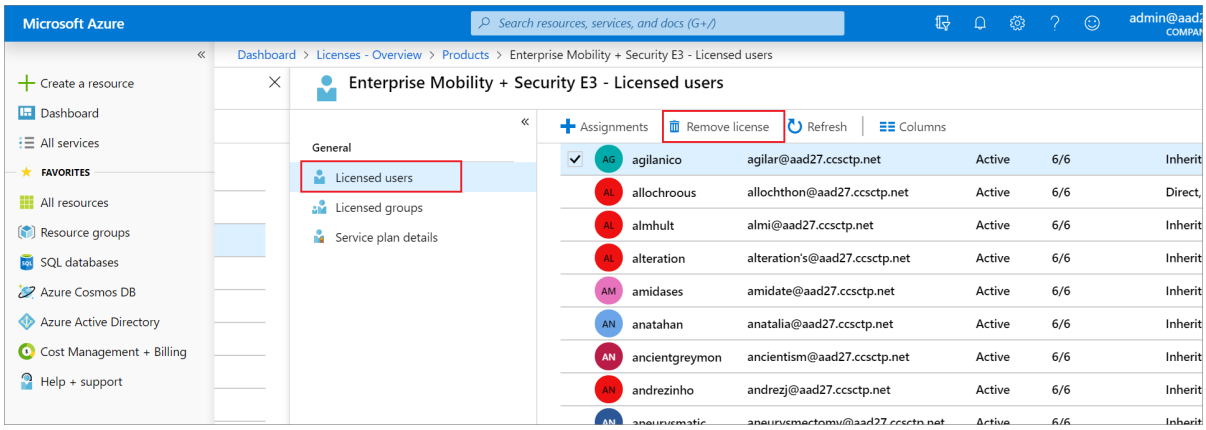
You can remove a license from a user's Azure AD user page, from the group overview page for a group assignment, or starting from the Azure AD **Licenses** page to see the users and groups for a license.

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**.



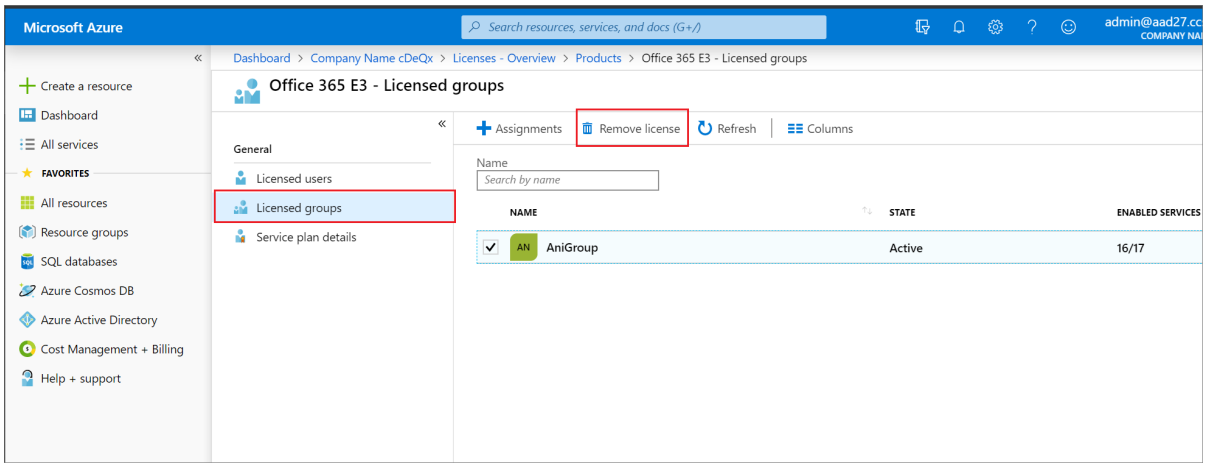
IMPORTANT

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**.



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

7/20/2020 • 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 user is automatically, and permanently, deleted.

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

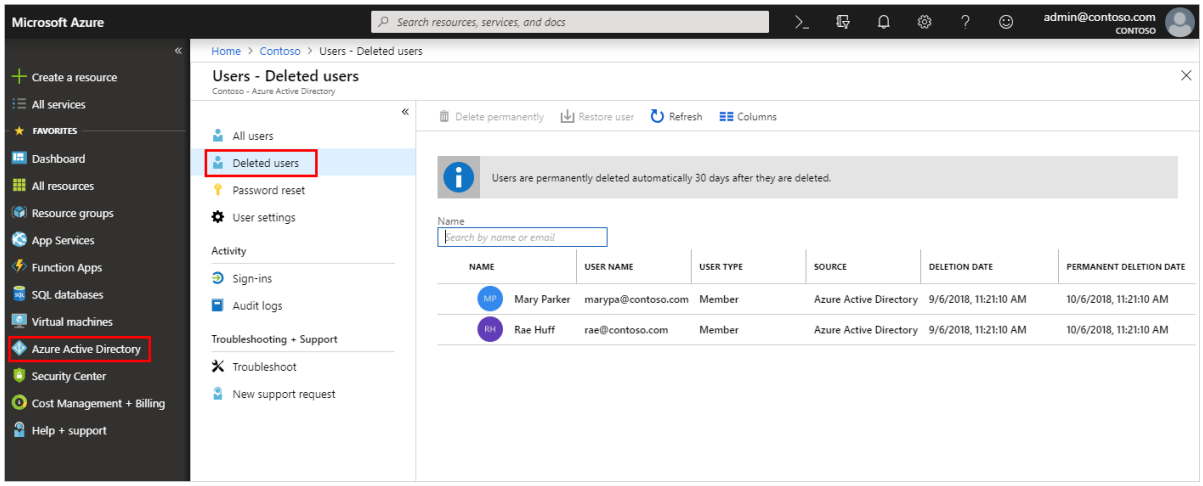
View your restorable users

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.



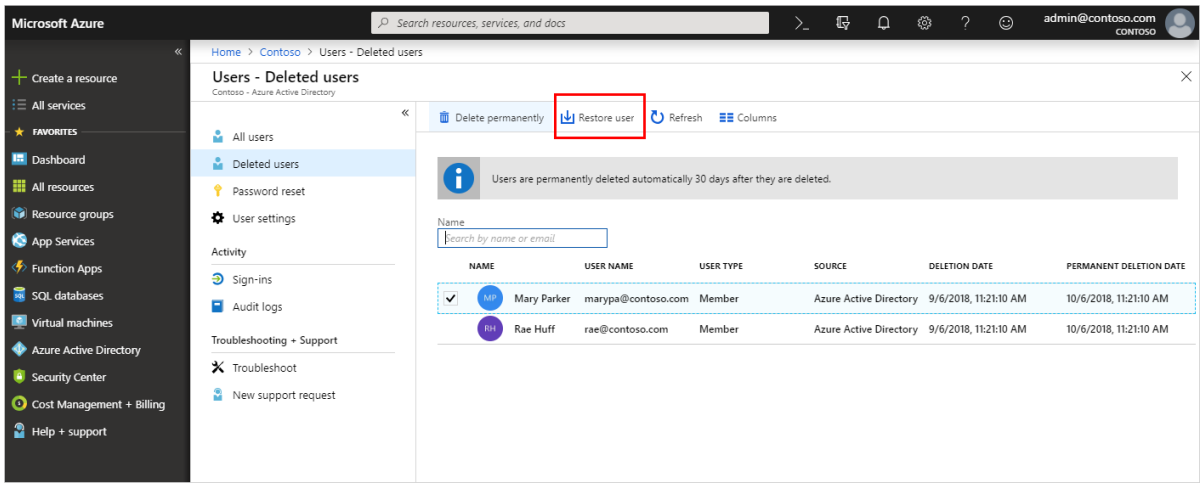
Restore a recently deleted user

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**.



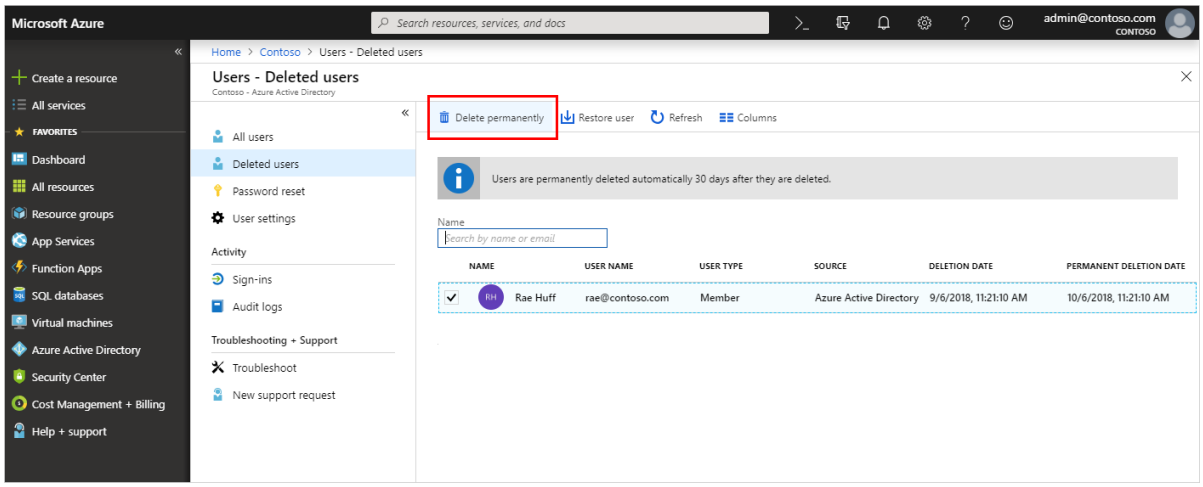
Permanently delete a user

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**.



Next steps

After you've restored or deleted your users, you can perform the following basic processes:

- 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.

Find help and open a support ticket for Azure Active Directory

7/20/2020 • 2 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.

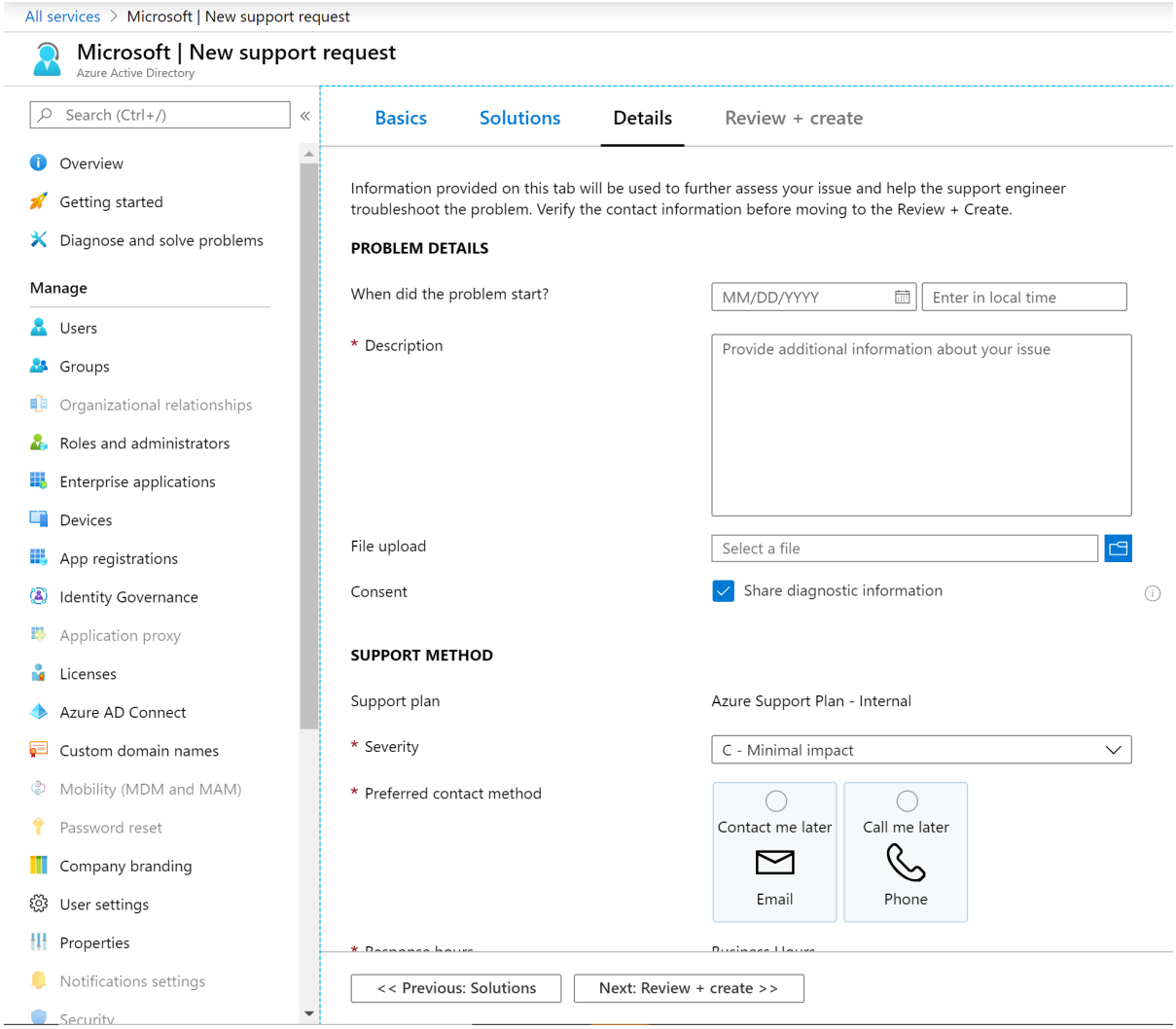
Open a support ticket

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.

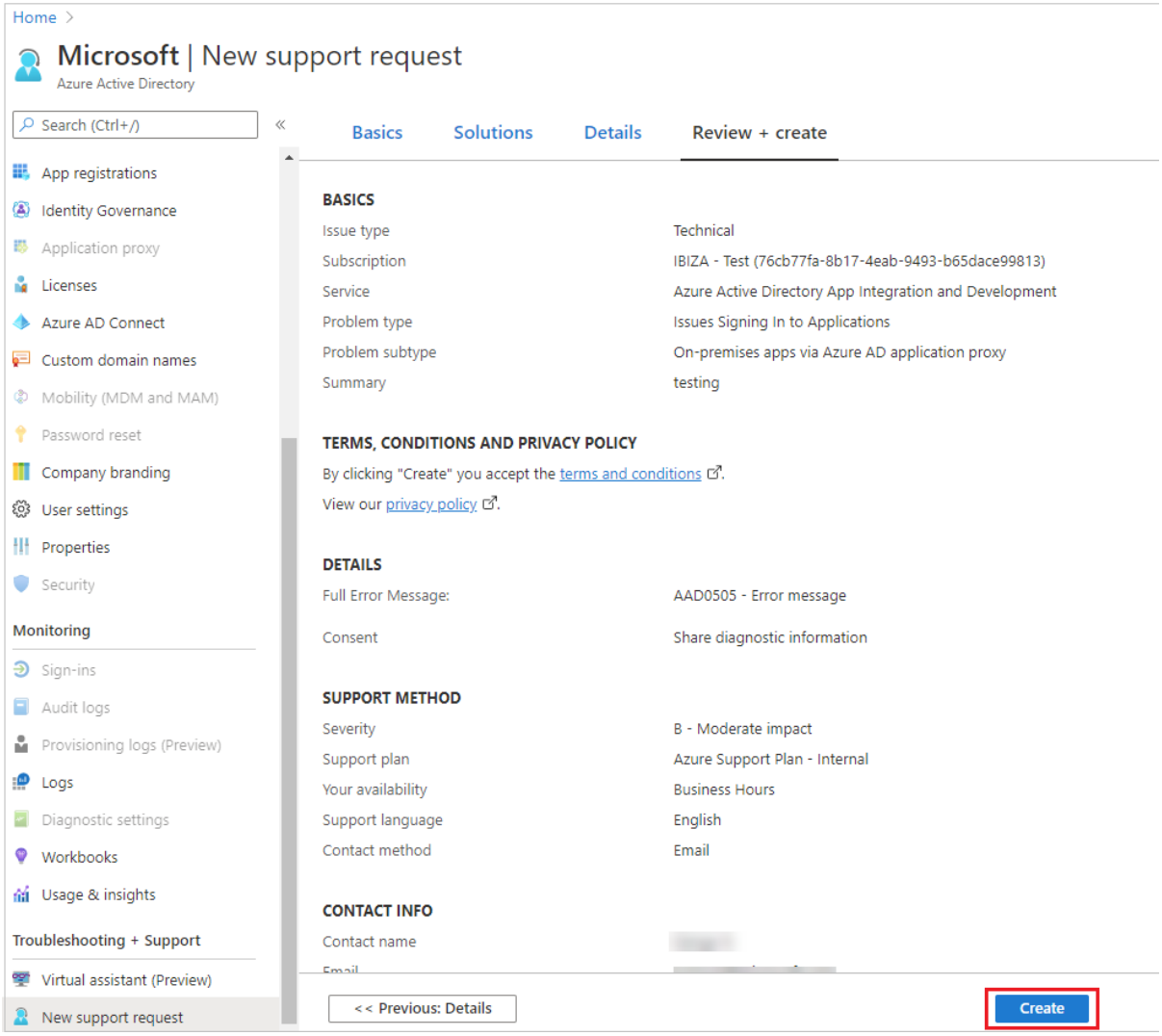
How to open a support ticket for Azure AD in the Azure portal

> **NOTE**
> For billing or subscription issues, you must use the Microsoft 365 admin center.

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**.
9. 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**.
10. On the **Details** blade, fill out the required details and select a Severity.



11. Provide your contact information and select **Next**.
12. Provide your contact information and select **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

Frequently asked questions about Azure Active Directory

7/20/2020 • 9 minutes to read • Edit Online

Azure Active Directory (Azure AD) is a comprehensive identity as a service (IDaaS) solution that spans all aspects of identity, access management, and security.

For more information, see What is Azure Active Directory?.

Access Azure and Azure Active Directory

Q: Why do I get "No subscriptions found" when I try to access Azure AD in the Azure portal?

A: To access the Azure portal, each user needs permissions with an Azure subscription. If you don't have a paid Office 365 or Azure AD subscription, you will need to activate a free Azure account or a paid subscription.

For more information, see:

- How Azure subscriptions are associated with Azure Active Directory

---

Q: What's the relationship between Azure AD, Office 365, and Azure?

A: Azure AD provides you with common identity and access capabilities to all web services. Whether you are using Office 365, Microsoft Azure, Intune, or others, you're already using Azure AD to help turn on sign-on and access management for all these services.

All users who are set up to use web services are defined as user accounts in one or more Azure AD instances. You can set up these accounts for free Azure AD capabilities like cloud application access.

Azure AD paid services like Enterprise Mobility + Security complement other web services like Office 365 and Microsoft Azure with comprehensive enterprise-scale management and security solutions.

Q: What are the differences between Owner and Global Administrator?

A: By default, the person who signs up for an Azure subscription is assigned the Owner role for Azure resources. An Owner can use either a Microsoft account or a work or school account from the directory that the Azure subscription is associated with. This role is authorized to manage services in the Azure portal.

If others need to sign in and access services by using the same subscription, you can assign them the appropriate built-in role. For additional information, see Manage access using RBAC and the Azure portal.

By default, the person who signs up for an Azure subscription is assigned the Global Administrator role for the directory. The Global Administrator has access to all Azure AD directory features. Azure AD has a different set of administrator roles to manage the directory and identity-related features. These administrators will have access to various features in the Azure portal. The administrator's role determines what they can do, like create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, or manage domains. For additional information on Azure AD directory admins and their roles, see Assign a user to administrator roles in Azure Active Directory and Assigning administrator roles in Azure Active Directory.

Additionally, Azure AD paid services like Enterprise Mobility + Security complement other web services, such as Office 365 and Microsoft Azure, with comprehensive enterprise-scale management and security solutions.

Q: Is there a report that shows when my Azure AD user licenses will expire?

A: No. This is not currently available.

Get started with Hybrid Azure AD

Q: How do I leave a tenant when I am added as a collaborator?

A: When you are added to another organization's tenant as a collaborator, you can use the "tenant switcher" in the upper right to switch between tenants. Currently, there is no way to leave the inviting organization, and Microsoft is working on providing this functionality. Until this feature is available, you can ask the inviting organization to remove you from their tenant.

Q: How can I connect my on-premises directory to Azure AD?

A: You can connect your on-premises directory to Azure AD by using Azure AD Connect.

For more information, see Integrating your on-premises identities with Azure Active Directory.

Q: How do I set up SSO between my on-premises directory and my cloud applications?

A: You only need to set up single sign-on (SSO) between your on-premises directory and Azure AD. As long as you access your cloud applications through Azure AD, the service automatically drives your users to correctly authenticate with their on-premises credentials.

Implementing SSO from on-premises can be easily achieved with federation solutions such as Active Directory Federation Services (AD FS), or by configuring password hash sync. You can easily deploy both options by using the Azure AD Connect configuration wizard.

For more information, see Integrating your on-premises identities with Azure Active Directory.

Q: Does Azure AD provide a self-service portal for users in my organization?

A: Yes, Azure AD provides you with the Azure AD Access Panel for user self-service and application access. If you are an Office 365 customer, you can find many of the same capabilities in the Office 365 portal.

For more information, see Introduction to the Access Panel.

Q: Does Azure AD help me manage my on-premises infrastructure?

A: Yes. The Azure AD Premium edition provides you with Azure AD Connect Health. Azure AD Connect Health helps you monitor and gain insight into your on-premises identity infrastructure and the synchronization services.

For more information, see Monitor your on-premises identity infrastructure and synchronization services in the cloud.

Password management

Q: Can I use Azure AD password write-back without password sync? (In this scenario, is it possible to use Azure AD self-service password reset (SSPR) with password write-back and not store passwords in the cloud?)

A: You do not need to synchronize your Active Directory passwords to Azure AD to enable write-back. In a federated environment, Azure AD single sign-on (SSO) relies on the on-premises directory to authenticate the user. This scenario does not require the on-premises password to be tracked in Azure AD.

Q: How long does it take for a password to be written back to Active Directory on-premises?

A: Password write-back operates in real time.

For more information, see Getting started with password management.

Q: Can I use password write-back with passwords that are managed by an admin?

A: Yes, if you have password write-back enabled, the password operations performed by an admin are written back to your on-premises environment.

For more answers to password-related questions, see Password management frequently asked questions.

Q: What can I do if I can't remember my existing Office 365/Azure AD password while trying to change my password?

A: For this type of situation, there are a couple of options. Use self-service password reset (SSPR) if it's available. Whether SSPR works depends on how it's configured. For more information, see How does the password reset portal work.

For Office 365 users, your admin can reset the password by using the steps outlined in Reset user passwords.

For Azure AD accounts, admins can reset passwords by using one of the following:

- Reset accounts in the Azure portal
- Using PowerShell

Security

Q: Are accounts locked after a specific number of failed attempts or is there a more sophisticated strategy used?

We use a more sophisticated strategy to lock accounts. This is based on the IP of the request and the passwords entered. The duration of the lockout also increases based on the likelihood that it is an attack.

Q: Certain (common) passwords get rejected with the messages 'this password has been used to many times', does this refer to passwords used in the current active directory?

This refers to passwords that are globally common, such as any variants of "Password" and "123456".

Q: Will a sign-in request from dubious sources (botnets, tor endpoint) be blocked in a B2C tenant or does this require a Basic or Premium edition tenant?

We do have a gateway that filters requests and provides some protection from botnets, and is applied for all B2C tenants.

Application access

Q: Where can I find a list of applications that are pre-integrated with Azure AD and their capabilities?

A: Azure AD has more than 2,600 pre-integrated applications from Microsoft, application service providers, and partners. All pre-integrated applications support single sign-on (SSO). SSO lets you use your organizational credentials to access your apps. Some of the applications also support automated provisioning and de-provisioning.

For a complete list of the pre-integrated applications, see the Active Directory Marketplace.

Q: What if the application I need is not in the Azure AD marketplace?

A: With Azure AD Premium, you can add and configure any application that you want. Depending on your

application's capabilities and your preferences, you can configure SSO and automated provisioning.

For more information, see:

- Configuring single sign-on to applications that are not in the Azure Active Directory application gallery
- Using SCIM to enable automatic provisioning of users and groups from Azure Active Directory to applications

---

Q: How do users sign in to applications by using Azure AD?

A: Azure AD provides several ways for users to view and access their applications, such as:

- The Azure AD access panel
- The Office 365 application launcher
- Direct sign-in to federated apps
- Deep links to federated, password-based, or existing apps

For more information, see End user experiences for applications.

Q: What are the different ways Azure AD enables authentication and single sign-on to applications?

A: Azure AD supports many standardized protocols for authentication and authorization, such as SAML 2.0, OpenID Connect, OAuth 2.0, and WS-Federation. Azure AD also supports password vaulting and automated sign-in capabilities for apps that only support forms-based authentication.

For more information, see:

- Authentication Scenarios for Azure AD
- Active Directory authentication protocols
- Single sign-on for applications in Azure AD

Q: Can I add applications I'm running on-premises?

A: Azure AD Application Proxy provides you with easy and secure access to on-premises web applications that you choose. You can access these applications in the same way that you access your software as a service (SaaS) apps in Azure AD. There is no need for a VPN or to change your network infrastructure.

For more information, see How to provide secure remote access to on-premises applications.

Q: How do I require multi-factor authentication for users who access a particular application?

A: With Azure AD Conditional Access, you can assign a unique access policy for each application. In your policy, you can require multi-factor authentication always, or when users are not connected to the local network.

For more information, see Securing access to Office 365 and other apps connected to Azure Active Directory.

Q: What is automated user provisioning for SaaS apps?

A: Use Azure AD to automate the creation, maintenance, and removal of user identities in many popular cloud SaaS apps.

For more information, see Automate user provisioning and deprovisioning to SaaS applications with Azure Active Directory.

Q: Can I set up a secure LDAP connection with Azure AD?

A: No. Azure AD does not support the Lightweight Directory Access Protocol (LDAP) protocol or Secure LDAP directly. However, it's possible to enable Azure AD Domain Services (Azure AD DS) instance on your Azure AD tenant with properly configured network security groups through Azure Networking to achieve LDAP connectivity.

For more information, see Configure secure LDAP for an Azure Active Directory Domain Services managed domain