Contents

What is Azure Active Directory?

11/14/2018 • 9 minutes to read • Edit Online

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. Azure AD 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.

You can 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, Azure AD gives you 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 leveraging 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. Therefore, 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 Basic, 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 workforce.

NOTE

For the pricing options of these licenses, see Azure Active Directory Pricing.

Azure Active Directory Premium P1, Premium P2, and Azure Active Directory Basic are not currently supported in China. For more information about Azure AD pricing, you can contact the Azure Active Directory Forum.

- **Azure Active Directory Free.** Provides user and group management, on-premises directory synchronization, basic reports, and single sign-on across Azure, Office 365, and many popular SaaS apps.
- **Azure Active Directory Basic.** In addition to the Free features, Basic also provides cloud-centric app access, group-based access management, self-service password reset for cloud apps, and Azure AD Application Proxy, which lets you publish on-premises web apps using Azure AD.
- **Azure Active Directory Premium P1.** In addition to the Free and Basic 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, Basic, 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 How to: 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.

Terminology

To better understand Azure AD and its documentation, you should review the following terms.

TERM OR CONCEPT	DESCRIPTION
Azure subscription	Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
Azure tenant	A dedicated and trusted instance of Azure AD 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.

TERM OR CONCEPT	DESCRIPTION
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.
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.
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.
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 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 perform 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** This administrator role is called Global administrator in the Azure portal, but it's called **Company administrator** in Microsoft Graph API, Azure AD Graph API, and Azure AD PowerShell. For more information about the various administrator roles, see Administrator role permissions in Azure Active Directory.

TERM OR CONCEPT	DESCRIPTION
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.

What features work in Azure AD?

After you choose your Azure AD license, you will 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.
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.
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).
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.

CATEGORY	DESCRIPTION
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, Azure resources, 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.

Next steps

- Sign up for Azure Active Directory Premium
- Associate an Azure subscription to your Azure Active Directory
- Access Azure Active Directory and create a new tenant
- Azure Active Directory Premium P2 feature deployment checklist

What's new in Azure Active Directory?

11/15/2018 • 33 minutes to read • Edit Online

Get notified about when to revisit this page for updates by adding this URL to 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 6 months, you can find them in the Archive for What's new in Azure Active Directory.

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 or Company Writer
- Intune Service Administrator
- User Account 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

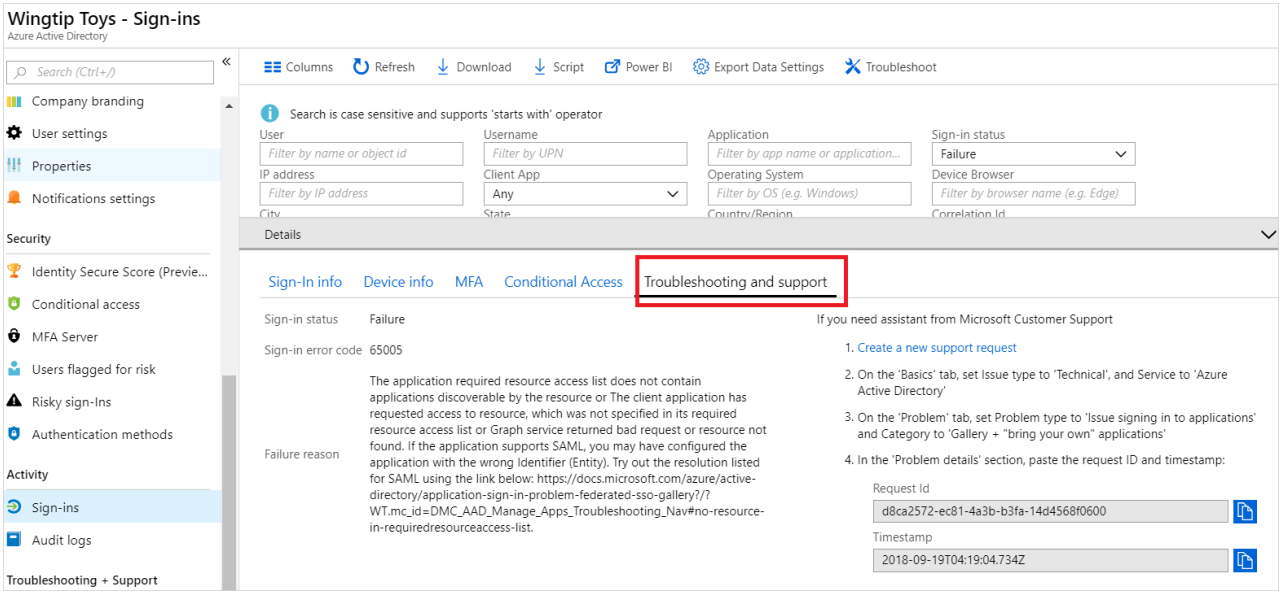
Check out the new deployment plan that's available for the My Apps Access panel (http://aka.ms/deploymentplans). The My Apps Access panel provides users with a single place to find and access their apps. This portal also provides users with self-service opportunities, such as requesting access to apps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

For more information about our native support for Tableau, see Azure AD Application Proxy now with native Tableau support.

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 MS 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 Spark
- 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 (ToU) 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 (ToU) creation

Type: New feature
Service category: Terms of Use
Product capability: Governance

During the creation of your Terms of Use (ToU), 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 (ToU) creation

Type: New feature
Service category: Terms of Use
Product capability: Governance

During the creation of your Terms of Use (ToU), 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 MS Graph. We have exposed two end points through MS Graph 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.

Quickstart: Access Azure Active Directory to create a new tenant

10/24/2018 • 2 minutes to read • Edit Online

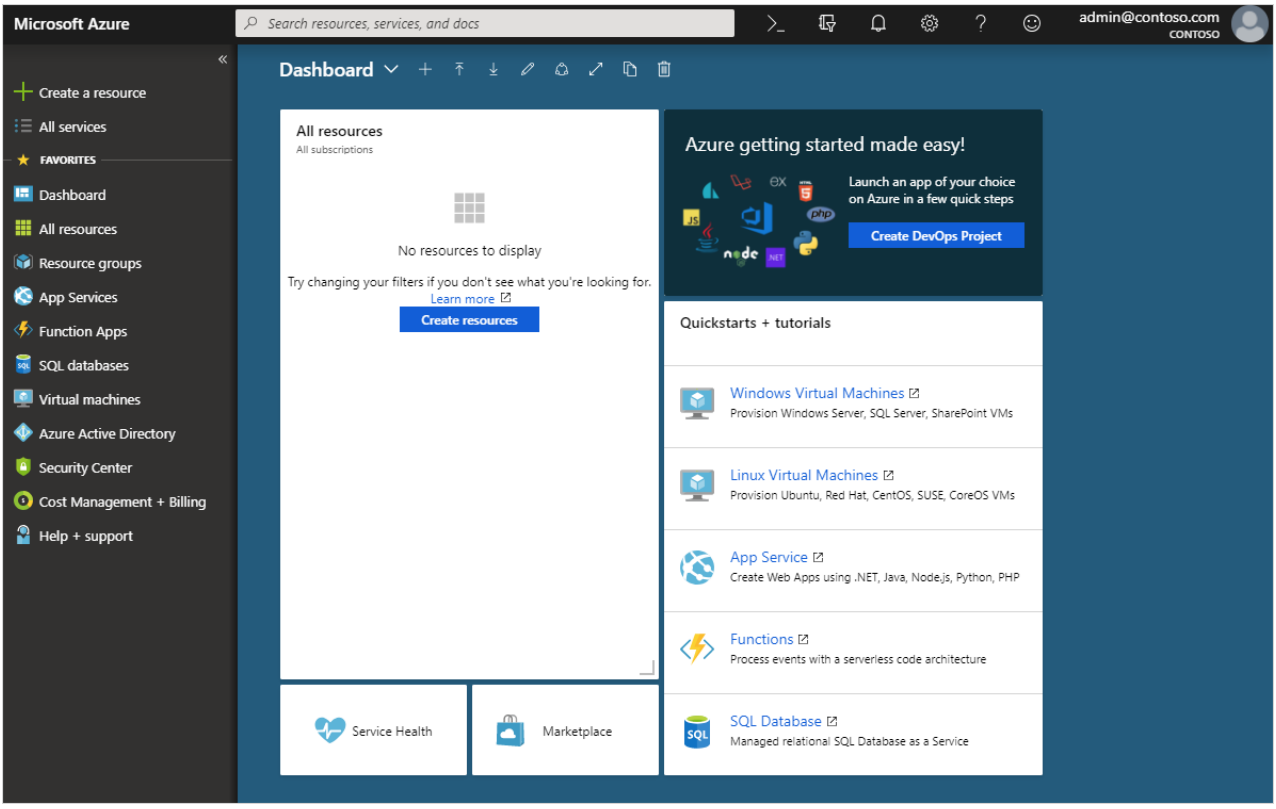
You can do all of your administrative tasks using the Azure Active Directory (Azure AD) portal, including creating a new tenant for your organization.

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.

Sign in to the Azure portal

Sign in to your organization's Azure portal using a Global administrator account.



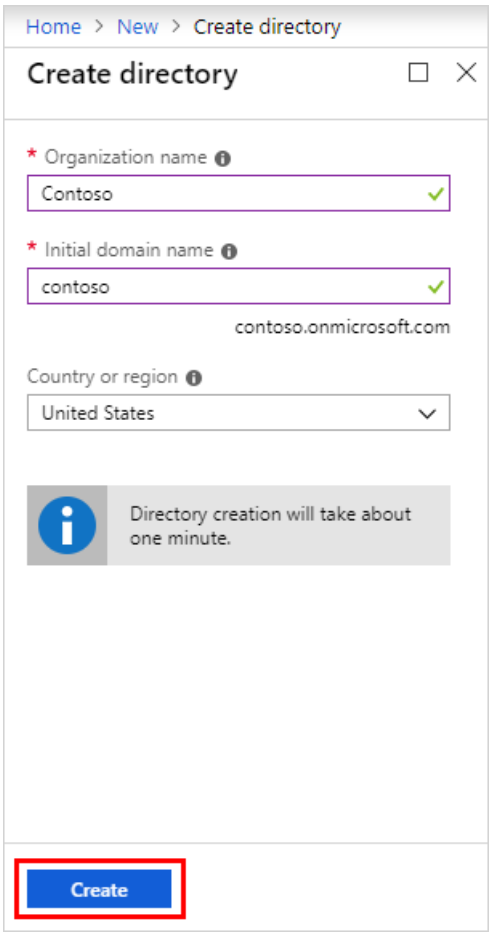
Create a new tenant for your organization

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. Select **Azure Active Directory**, select **Create resources**, select **Identity**, and then select **Azure Active Directory**.

   The **Create directory** page appears.



2. 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.
3. Select **Create**.

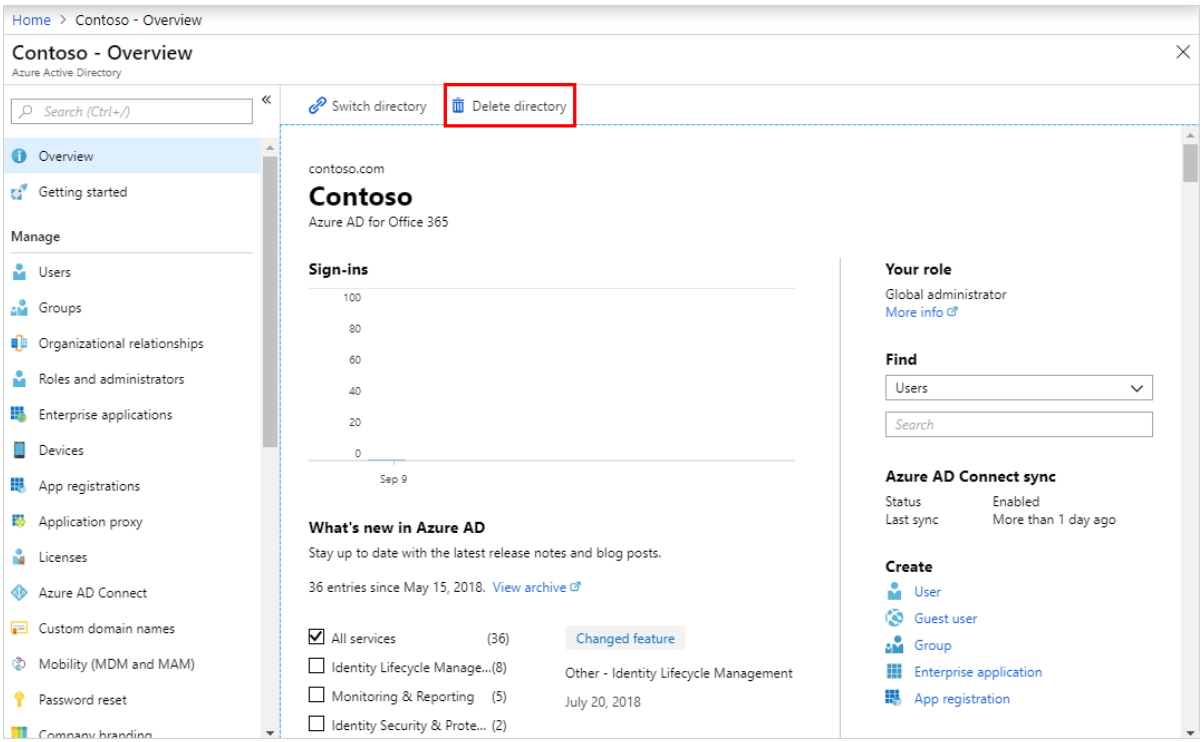
Your new tenant is created with the domain contoso.onmicrosoft.com.

Clean up resources

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

- 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

9/24/2018 • 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. 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.

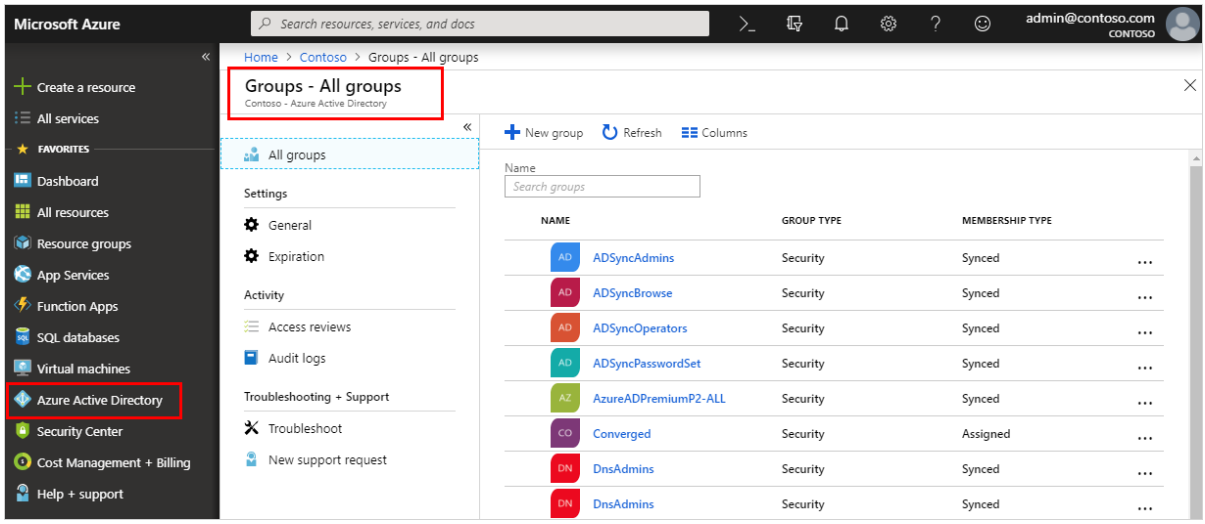
1. Select **Azure Active Directory** > **Groups**.
2. From the **Groups - All groups** page, search for and select the **MDM policy - West** group.
3. From the **MDM policy - West Overview** page, select **Members** from the **Manage** area.
4. Select **Add members**, and then search and select **Alain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

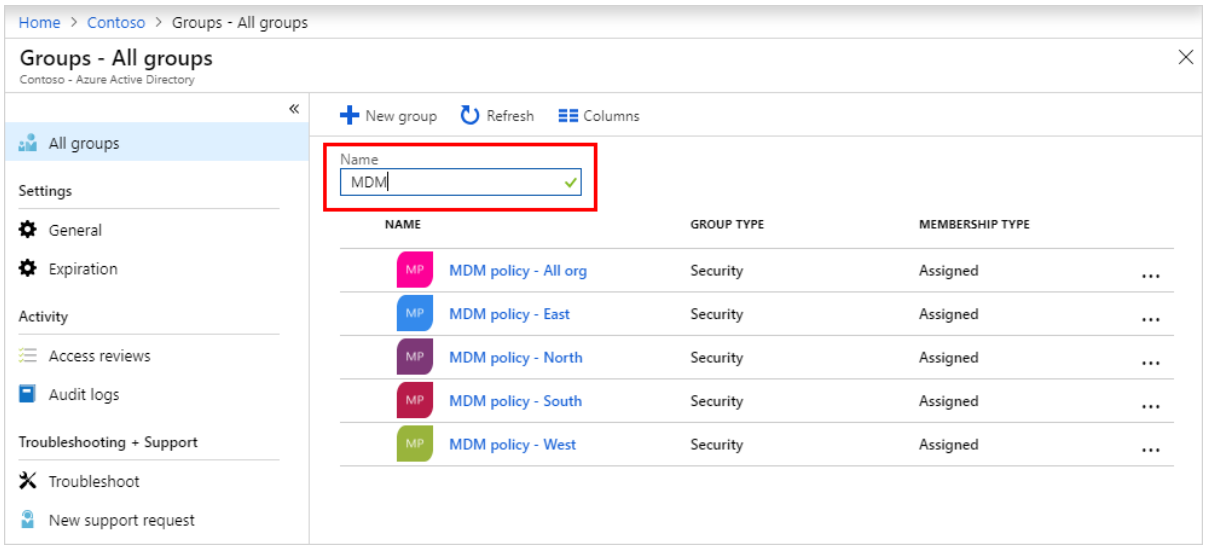


Search for the group

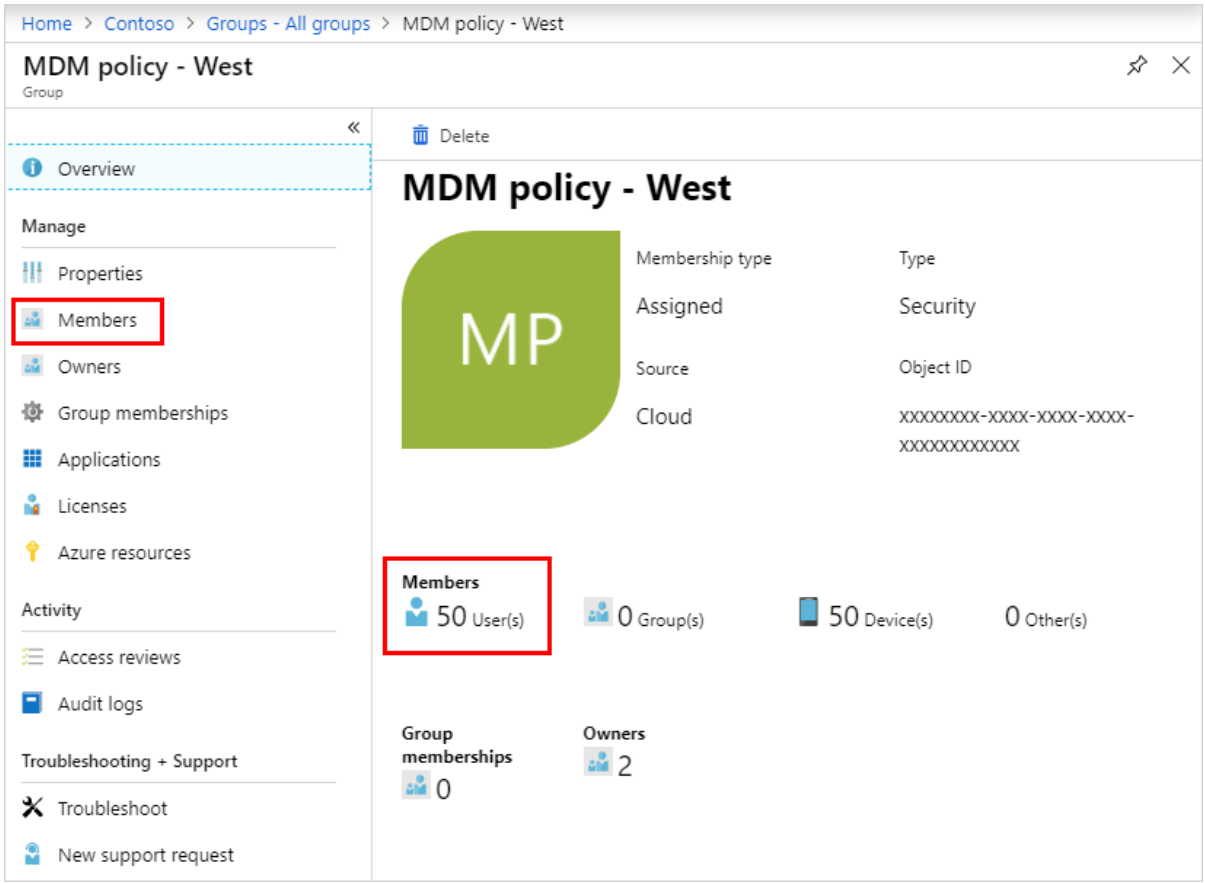
Search the **Groups – All groups** page to find the **MDM policy – West** group.

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.



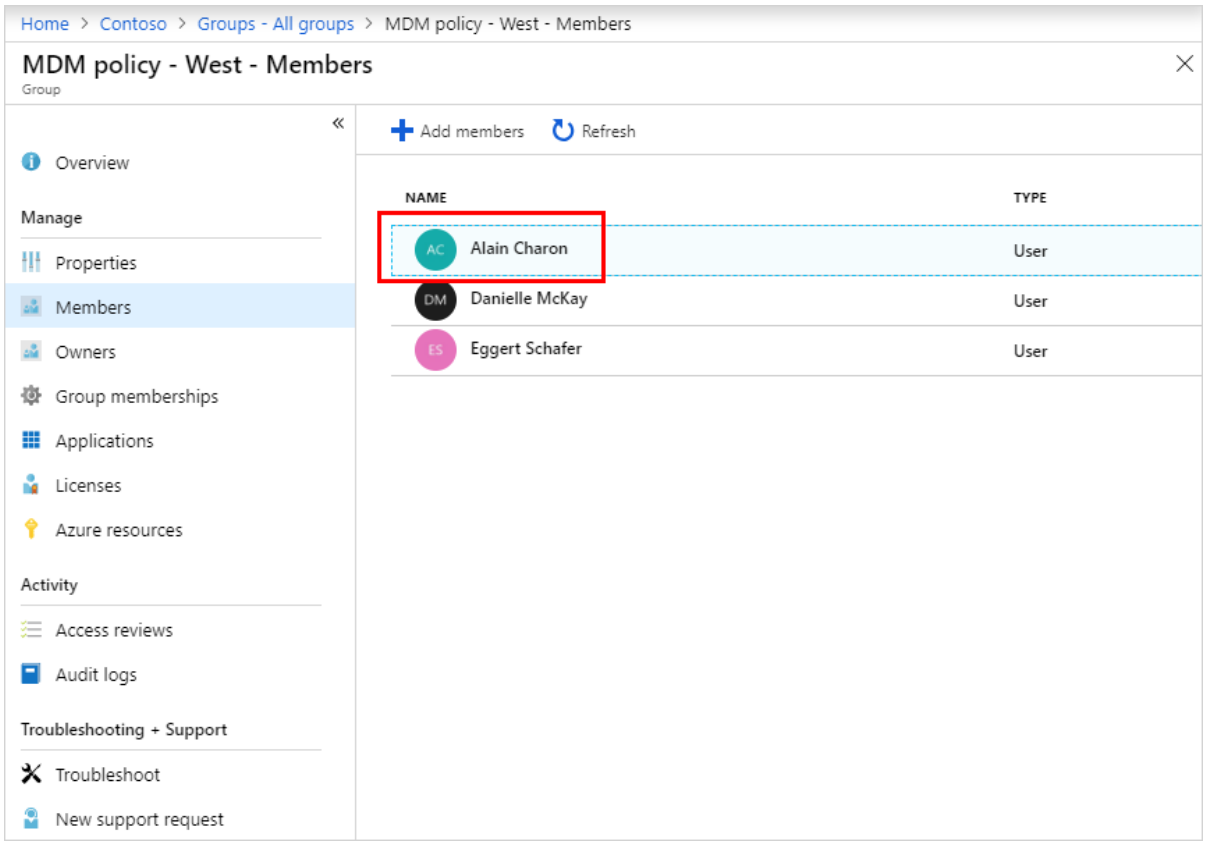
2. Select the group **MDM policy – West**.
3. View the group info on the **MDM policy - West Overview** page, including the number of members of that group.



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*.



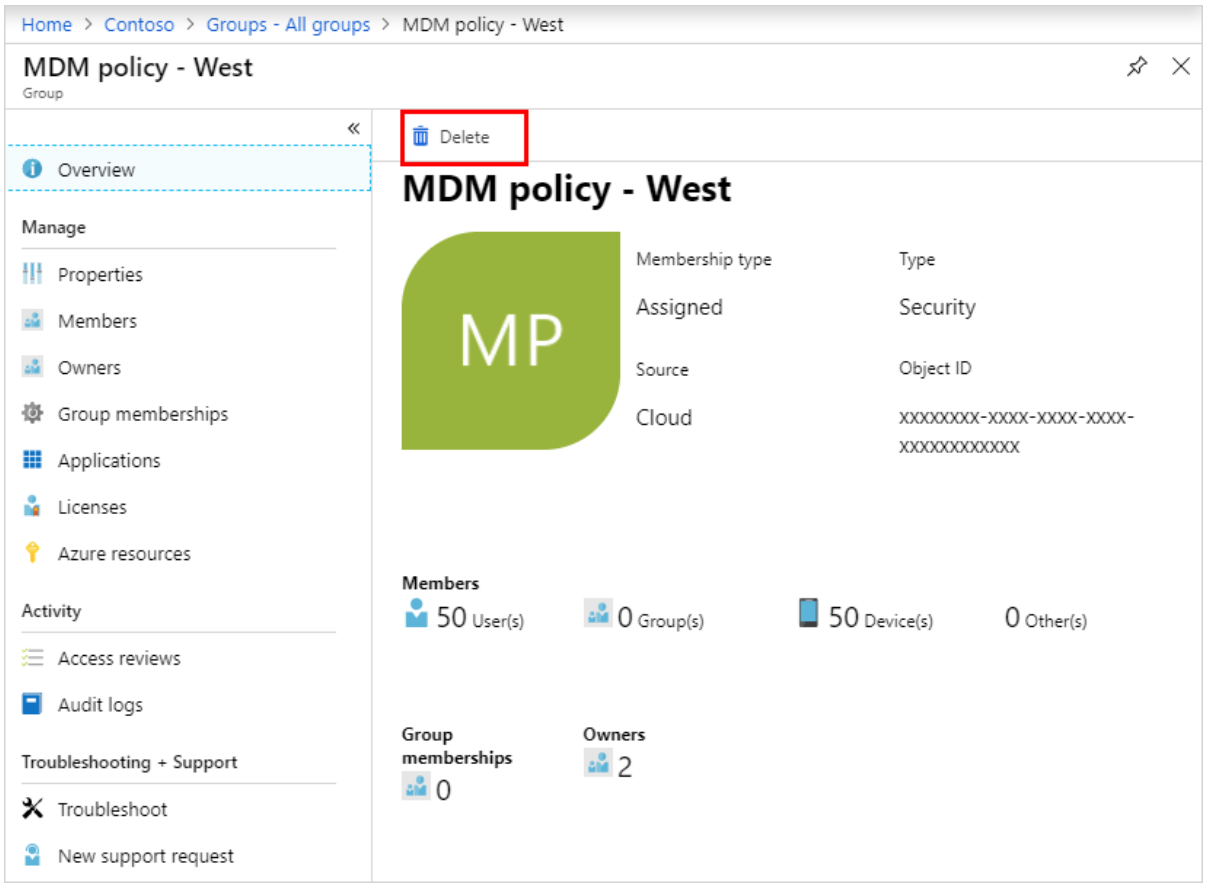
Clean up resources

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

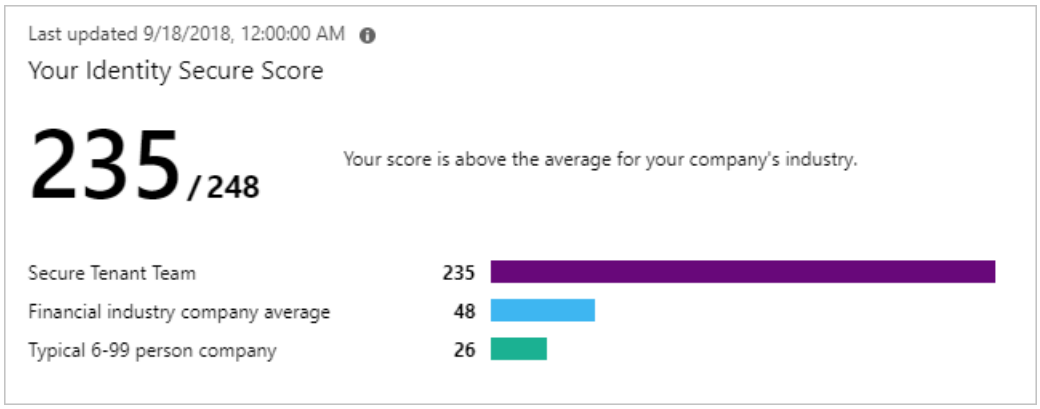
What is the identity secure score in Azure AD? - preview

9/26/2018 • 3 minutes to read • Edit Online

How secure is your Azure AD tenant? If you don't know how to answer this question, read this article to learn 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 248 that functions as indicator for how aligned you are with Microsoft's best practices recommendations for security.

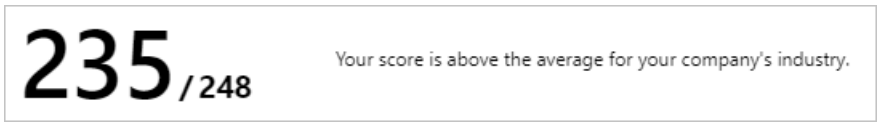


The score helps you to:

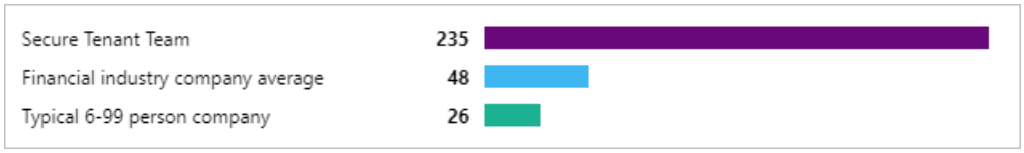
- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

You can access the score and related information on the identity secure score dashboard. On this dashboard, you find:

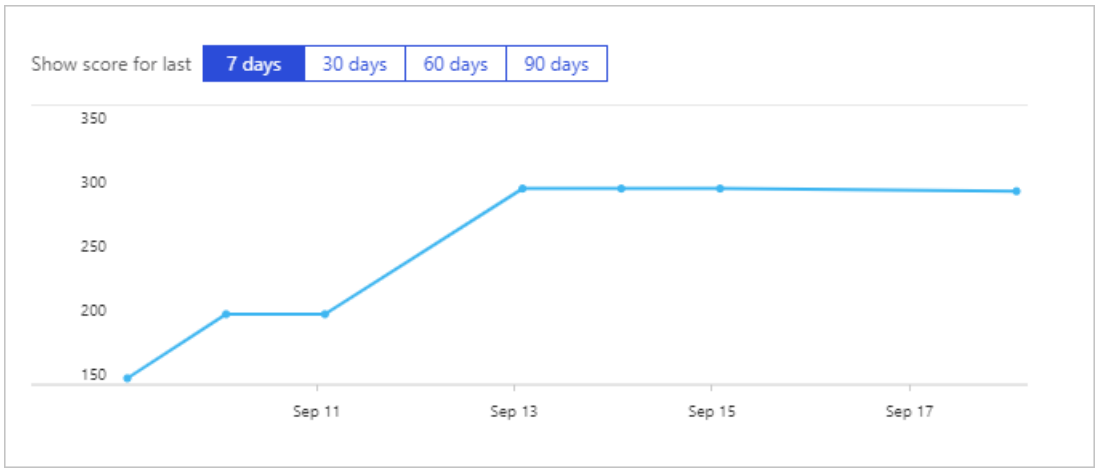
- Your score



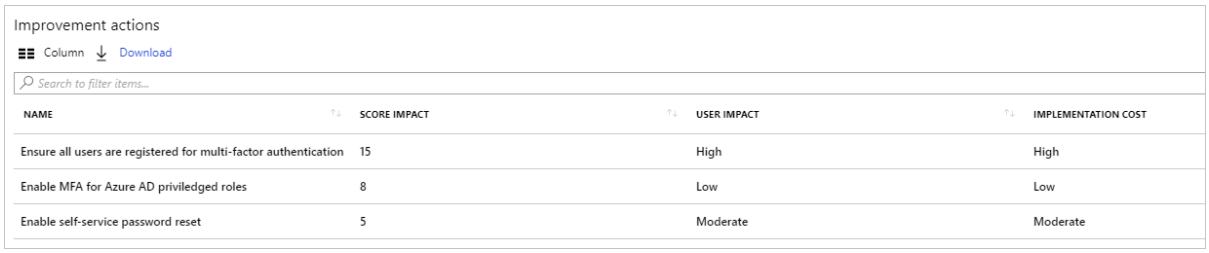
- A comparison graph



- A trend graph



- A list of identity security best practices.



By following the improvement actions, you can:

- Improve your security posture and your score.
- Take advantage of Microsoft's Identity features.

How do I get my secure score?

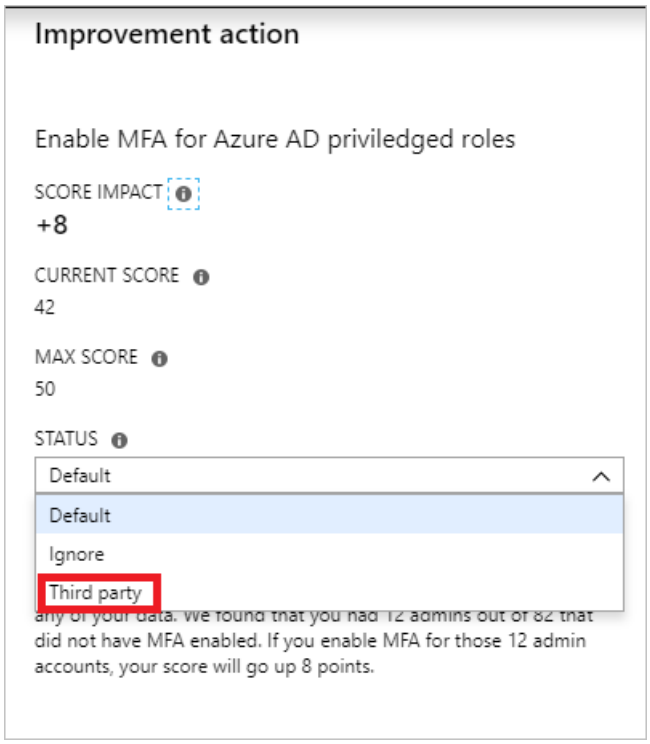
The Identity Secure Score is available in all editions of Azure AD.

To access your score, go to the Azure AD Overview dashboard.

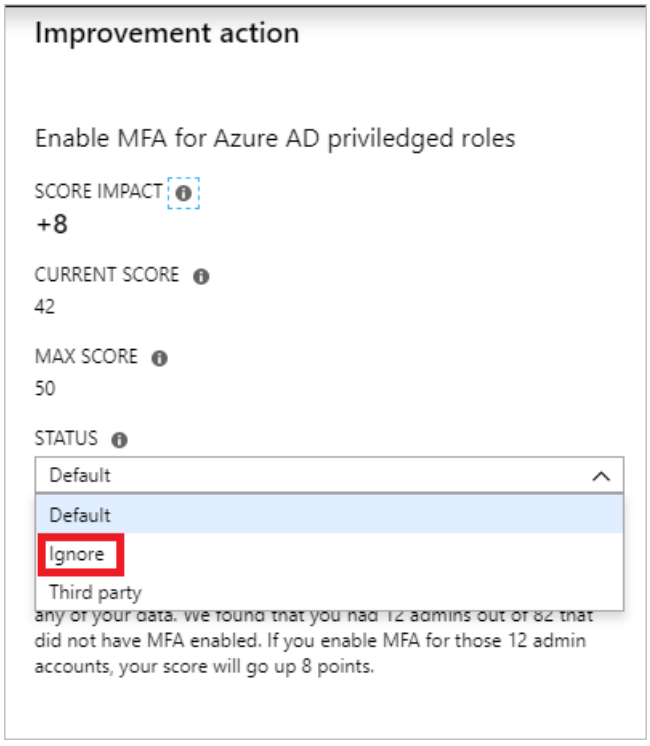
How does it work?

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 tenant. This means that it can take up to 48 hours until a configuration change you have made is reflected in your score.

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 in the settings of an improvement action.



Additionally, 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

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?

On the score analyzer page on the secure score portal, click a data point for a specific day, then scroll down to see the completed and incomplete actions for that day to find out what changed.

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 should always 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, go to the score analyzer page on the secure score portal. 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 Office 365 secure score is about to be migrated into an aggregate of five different scores:

- Identity
- Data
- Devices
- Infrastructure
- Apps

The identity secure score represents the identity part of the Office 365 secure score. This means that your recommendations for the identity secure score and the identity score in Office 365 are the same.

Next steps

If you would like to see a video about the Office 365 secure score, click here.

Learn about access management using Azure Active Directory groups

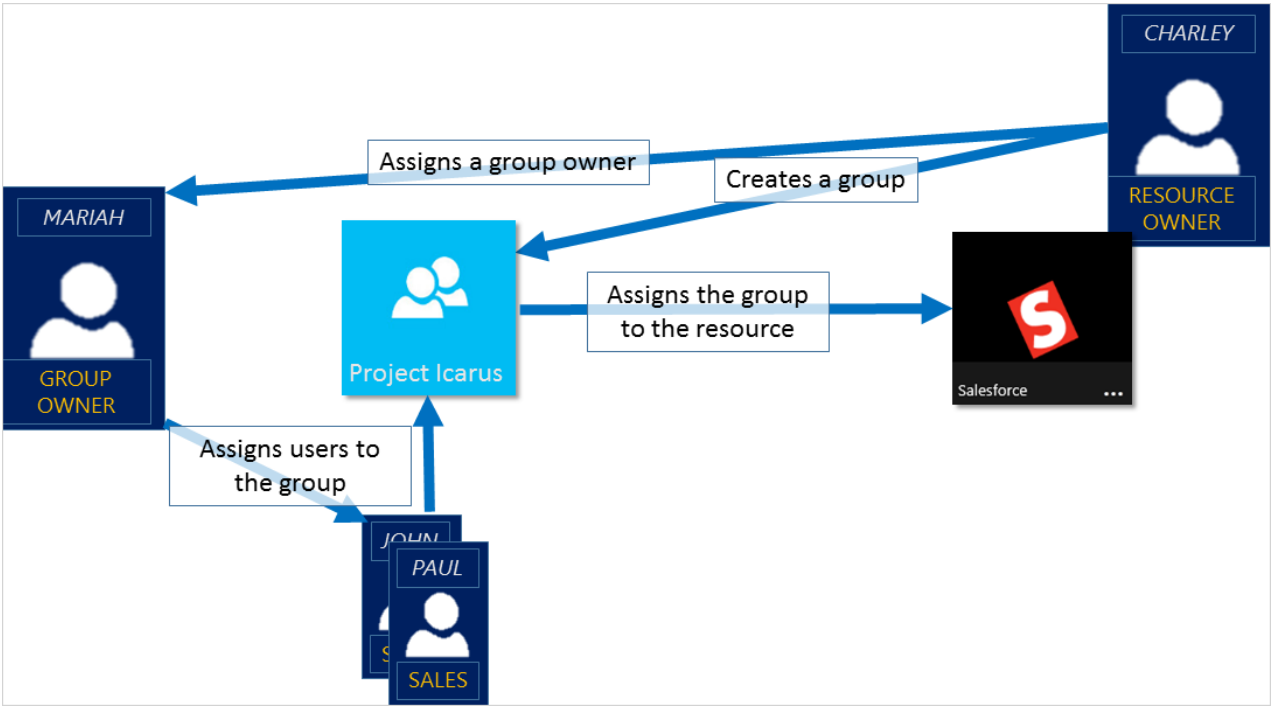
9/26/2018 • 3 minutes to read • Edit Online

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

> **NOTE**
>
> To use Azure Active Directory, you need an Azure account. If you don't have an account, you can sign up for a free Azure account.

How does access management in Azure AD work?

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:

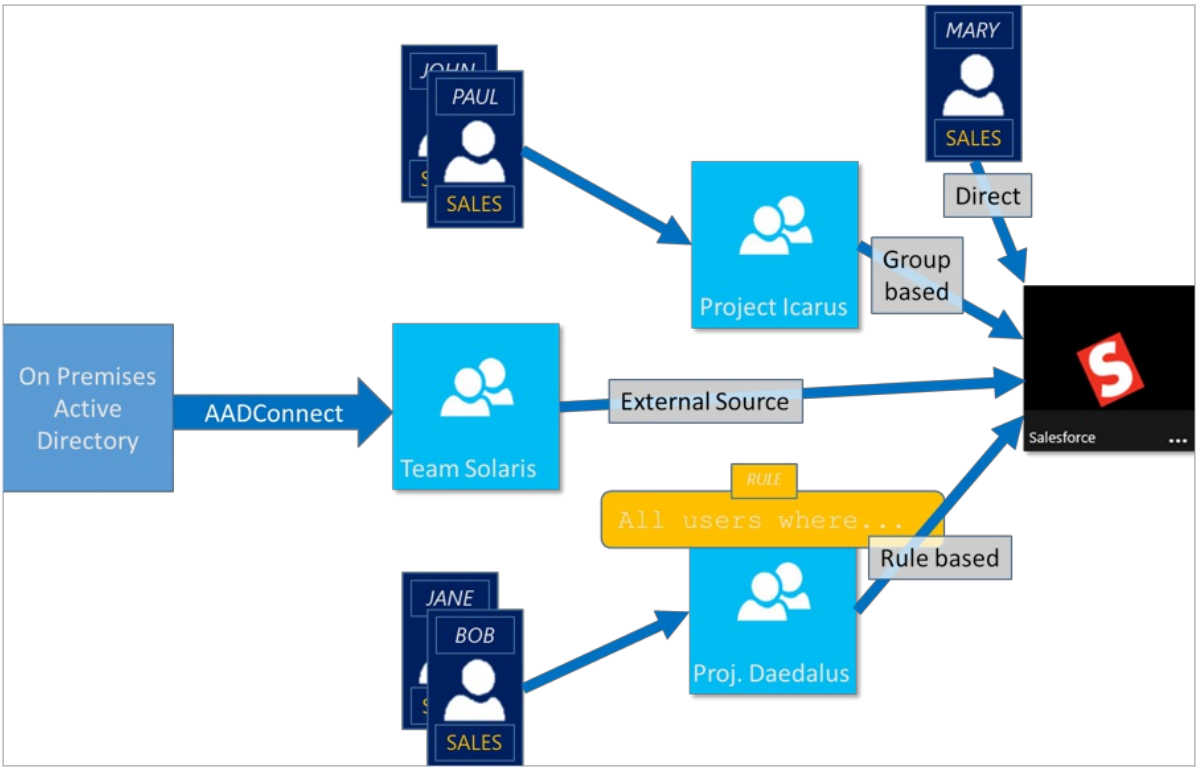
- **Direct assignment.** The resource owner directly assigns the user to the resource.
- **Group assignment.** The resource owner assigns an Azure AD group to the resource, which automatically

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?

10/29/2018 • 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 eliminates the need for automating license management via PowerShell to reflect changes in the organization and departmental structure on a per-user basis.

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 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 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 Office 365 portal, 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.

- A paid or trial subscription for Azure AD Basic or a paid or trial Office 365 Enterprise E3, Office 365 A3 and above editions is required in the tenant to use group-based license management. This feature requires license for each unique user that is a member of groups which are assigned license. You don't have to assign licenses to users for them to be members of groups which are assigned license, but you must have the minimum number of licenses in the tenant to cover all such users. For example, if you had a total of 1,000 unique users in all groups with licenses assigned in your tenant, you would need at least 1,000 licenses to meet the license requirement.

Your feedback is welcome!

If you have feedback or feature requests, please 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 is the Azure Active Directory architecture?

9/17/2018 • 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.

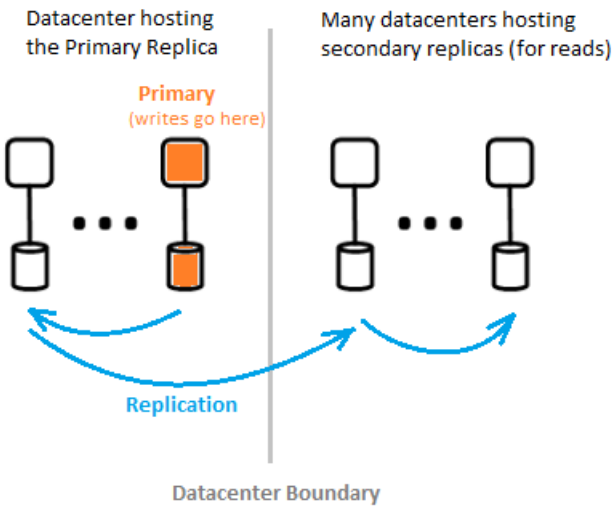
The following architecture elements are covered in this article:

- Service architecture design
- Usability
- Continuous availability
- Data centers

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 data centers.



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 data centers 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 data centers 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 data centers. Each data center is independent, which enables de-correlated failure modes.

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 data centers 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 data center. This write action ensures that a potential catastrophic loss of the data center 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

Data centers

Azure AD's replicas are stored in datacenters located throughout the world. For more information, see Azure datacenters.

Azure AD operates across data centers 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 data centers.
- For *reads*, the directory has secondary replicas and corresponding front-end services in an active-active configuration operating in multiple data centers. In case of a failure of an entire data center, traffic will be automatically routed to a different datacenter.
- For *writes*, the directory will fail over primary (master) replica across data centers 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 data centers.

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 Graph API of Azure AD are abstracted from maintaining affinity to a directory replica for read-write consistency. The Azure AD Graph service maintains a logical session, which has affinity to a secondary replica used for reads; affinity is captured in a "replica token" that the graph service caches using a distributed cache. This token is then used for subsequent operations in the same logical session.

> **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

What are the default user permissions in Azure Active Directory?

9/17/2018 • 5 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 the type of user, their role memberships, and their ownership of individual objects. This article describes those default permissions and contains a comparison of the member and guest user defaults.

Member and guest users

The set of default permissions received depends on if the user is a native member of the tenant (member user) or if the user is a B2B collaboration guest (guest user). For more information about B2B collaboration, see What is Azure AD B2B collaboration? for more information about 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).
- Azure AD B2B 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 cannot view any information about other tenant objects such as groups and applications.

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 owned groups 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
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
Ability to create security groups	Setting this option to No prevents users from creating security groups. Global Administrators and User Account Administrators can still create security groups. See Azure Active Directory cmdlets for configuring group settings to learn how.

PERMISSION	SETTING EXPLANATION
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 Account 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 prevents users from accessing Azure Active Directory.
Ability to read other users	This setting is available in PowerShell only. Setting this to $false prevents all non-admins from reading user information from the directory. This does not prevent reading user information in other Microsoft services like Exchange Online. This setting is meant for special circumstances, and setting this 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.

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 membership. An owner can also add or remove other owners. Unlike Global Administrators and User Account Administrators, owners can only manage groups they own. To assign a group owner, see Managing owners for a group.

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

Azure Active Directory Premium P2 licensing feature checklist

11/15/2018 • 2 minutes to read • Edit Online

It can seem overwhelming to deploy Azure Active Directory (Azure AD) for your organization and keep it secure. This article identifies some common tasks that customers find helpful. Customers typically complete these tasks over the course of 30 days, 90 days, or beyond to enhance their security posture. Even organizations who have already deployed Azure AD can use this checklist to make sure they're getting the most out of their investment.

A well-planned and executed identity infrastructure paves the way for more secure access to your productivity workloads and data only by authenticated users and devices.

Prerequisites

This guide assumes you have Azure AD Premium P2 licenses, Enterprise Mobility + Security E5, Microsoft 365 E5, or a similar license bundle.

Azure AD licensing

Microsoft 365 Enterprise

Enterprise Mobility + Security

Plan and deploy: Day 1-30

- Designate more than one global administrator (break-glass account)
  - Manage emergency-access administrative accounts in Azure AD
- Turn on Azure AD Privileged Identity Management (PIM) to view reports
  - Start using PIM
- Use non-global administrative roles where possible.
  - Assigning administrator roles in Azure Active Directory
- Authentication
  - Roll out self-service password reset
  - Deploy Azure AD Password Protection (preview)
    - Eliminate bad passwords in your organization
    - Enforce Azure AD password protection for Windows Server Active Directory
  - Configure account lockout policies
    - Azure Active Directory smart lockout
    - AD FS Extranet Lockout and Extranet Smart Lockout
  - Deploy Azure AD Multi-Factor Authentication using conditional access policies
  - Enable converged registration for self-service password reset and Azure AD Multi-Factor Authentication (preview)
  - Enable Azure Active Directory Identity Protection
    - Use risk events to trigger Multi-Factor Authentication and password changes
  - Password guidance
    - Maintain an eight-character minimum length requirement, longer is not necessarily better.
    - Eliminate character-composition requirements.

    - Eliminate mandatory periodic password resets for user accounts.
- Synchronize users from on-premises Active Directory
    - Install Azure AD Connect
    - Implement Password Hash Sync
    - Implement Password Writeback
    - Implement Azure AD Connect Health
- Assign licenses to users by group membership in Azure Active Directory

Plan and deploy: Day 31-90

- Plan for guest user access
    - Add Azure Active Directory B2B collaboration users in the Azure portal
    - Allow or block invitations to B2B users from specific organizations
    - Grant B2B users in Azure AD access to your on-premises applications
- Make decisions about user lifecycle management strategy
- Decide on device management strategy
    - Usage scenarios and deployment considerations for Azure AD Join
- Manage Windows Hello for Business in your organization

Plan and deploy: Day 90 and beyond

- Azure AD Privileged Identity Management
    - Configure Azure AD directory role settings in PIM
    - Assign Azure AD directory roles in PIM
- Complete an access review for Azure AD directory roles in PIM
- Manage the user lifecycle holistically
    - Azure AD has an approach to managing Identity lifecycle
    - Remove manual steps from your employee account lifecycle, to prevent unauthorized access:
        - Synchronize identities from your source of truth (HR System) to Azure AD. link to supported HR systems)
        - 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.
        - Use group-based access management provisioning to automatically provision users for SaaS applications.

Next steps

Identity and device access configurations

Common recommended identity and device access policies

Where does Microsoft Azure Active Directory (Azure AD) store identity data for European customers

9/17/2018 • 3 minutes to read • Edit Online

Azure AD helps you to manage user identities and to create intelligence-driven access policies that help secure your organization's resources. Identity data is stored in a location that's based on the address your organization provided when you subscribed to the service. For example, when you subscribed to Office 365 or Azure. For specific info about where your identity data is stored, you can use the Where is your data located? section of the Microsoft Trust Center.

While most Azure AD-related European identity data stays in European datacenters, there are five user-related attributes that are typically stored in U.S. datacenters. These attributes are GivenName, Surname, userPrincipalName, Domain, and PasswordHash. The PasswordHash attribute can be an exception and not stored in the U.S. if someone uses an on-premises, federated authentication method that stops the PasswordHash value from syncing with Azure AD. Additionally, there is some operational, service-specific data that's required for normal Azure AD operation, which is stored in the U.S. and doesn't include any personal data.

Data stored outside of European datacenters for European customers

Most Azure AD-related European identity data, for organizations with European-based addresses, stays in European datacenters. Azure AD data that's not stored in European datacenters, includes:

- **Identity-related attributes**

  The following identity-related attributes will be replicated to the United States:

  - GivenName
  - Surname
  - userPrincipalName
  - Domain
  - PasswordHash
  - SourceAnchor
  - AccountEnabled
  - PasswordPolicies
  - StrongAuthenticationRequirement
  - ApplicationPassword
  - PUID
- **Microsoft Azure multi-factor authentication (MFA) and Azure AD self-service password reset (SSPR)**

  MFA stores all user data at-rest in European datacenters. However, some MFA service-specific data is stored in the U.S., including:

  - Two-factor authentication and its related personal data might be stored in the U.S. if you're using MFA or SSPR.
    - All two-factor authentication using phone calls or SMS might be completed by U.S. carriers.
    - Push notifications using the Microsoft Authenticator app require notifications from the manufacturer's notification service (Apple or Google), which might be outside Europe.
    - OATH codes are always validated in the U.S.

    - Some MFA and SSPR logs are stored in the U.S. for 30 days, regardless of authentication type.
- **Microsoft Azure Active Directory B2C (Azure AD B2C)**

  Azure AD B2C stores all user data at-rest in European datacenters. However, operational logs (with personal data removed) stay at the location from where the person is accessing the services. For example, if a B2C user accesses the service in the U.S., the operational logs stay in the U.S. Additionally, all policy configuration data not containing personal data is stored only in the U.S. 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 all user data at-rest in European datacenters. However, B2B stores its non-personal metadata in tables within U.S. datacenters. This table includes fields like redeemUrl, invitationTicket, resource tenant Id, InviteRedirectUrl, and InviterAppId.

- **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.

- **Services and apps integrated with Azure AD**

  Any services and apps that integrate with Azure AD have access to identity data. Evaluate each service and app to determine how identity data is processed by that specific service and app, 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

How to: Sign up for Azure Active Directory as an organization

9/19/2018 • 2 minutes to read • Edit Online

Sign up for Azure Active Directory (Azure AD) 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

How to: Sign up for Azure Active Directory Premium

10/17/2018 • 3 minutes to read • Edit Online

You can purchase and associate Azure Active Directory (Azure AD) Premium 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 - Existing Customers or How to Purchase Azure Active Directory Premium - New Customers.

Sign up using your Enterprise Mobility + Security licensing plan

Enterprise Mobility + Security is 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

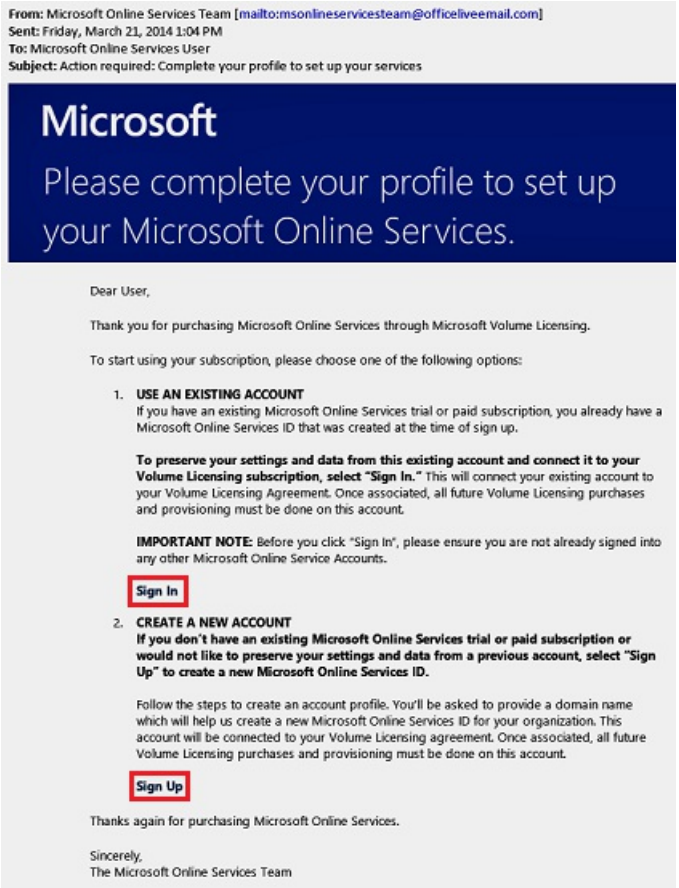
For more information about volume licensing purchase options, see How to purchase through Volume Licensing.

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.

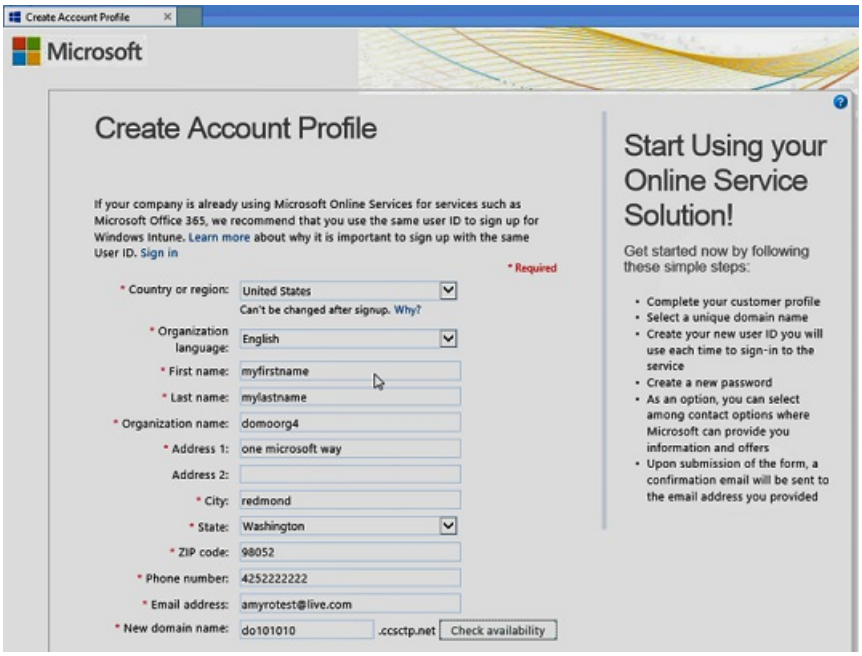
   Follow the steps to create an account profile. You'll be asked to provide a domain name which will help us create a new Microsoft Online Services ID for your organization. This account will be connected to your Volume Licensing agreement. Once associated, all future Volume Licensing purchases and provisioning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

   Sign Up

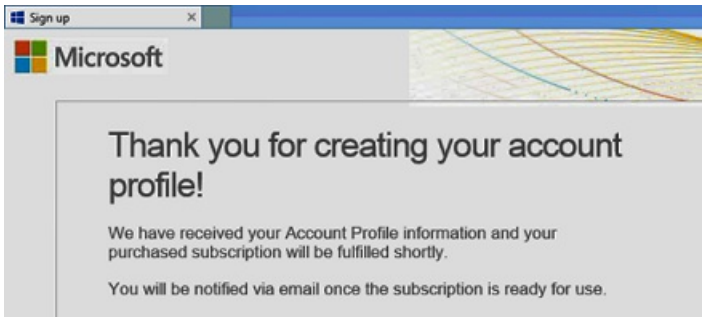
Thanks again for purchasing Microsoft Online Services.

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 administratr 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

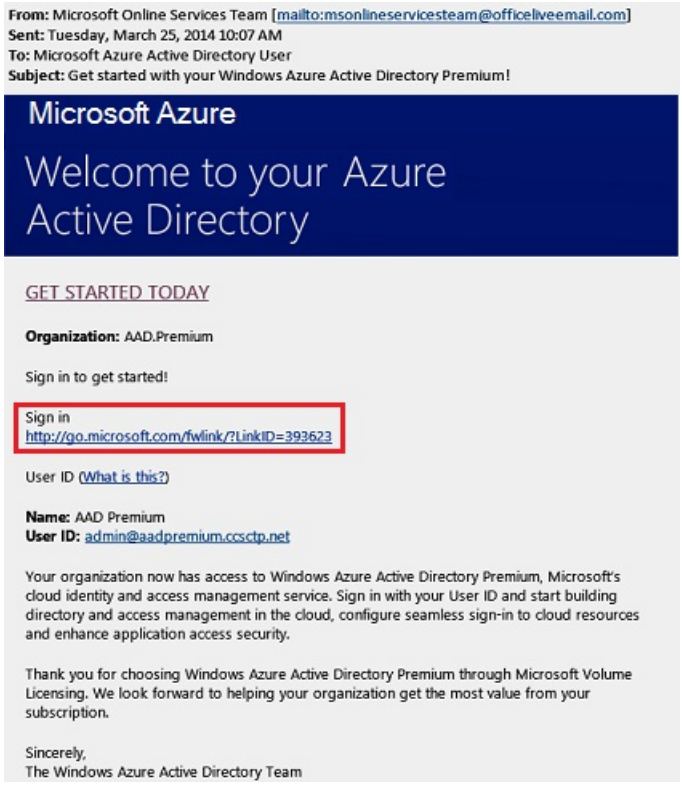
If you're adding new Azure AD Premium licenses to an existing subscription, your Azure AD access should already be activated. Otherwise, you need to activate Azure AD access after you receive the **Welcome email**.

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.

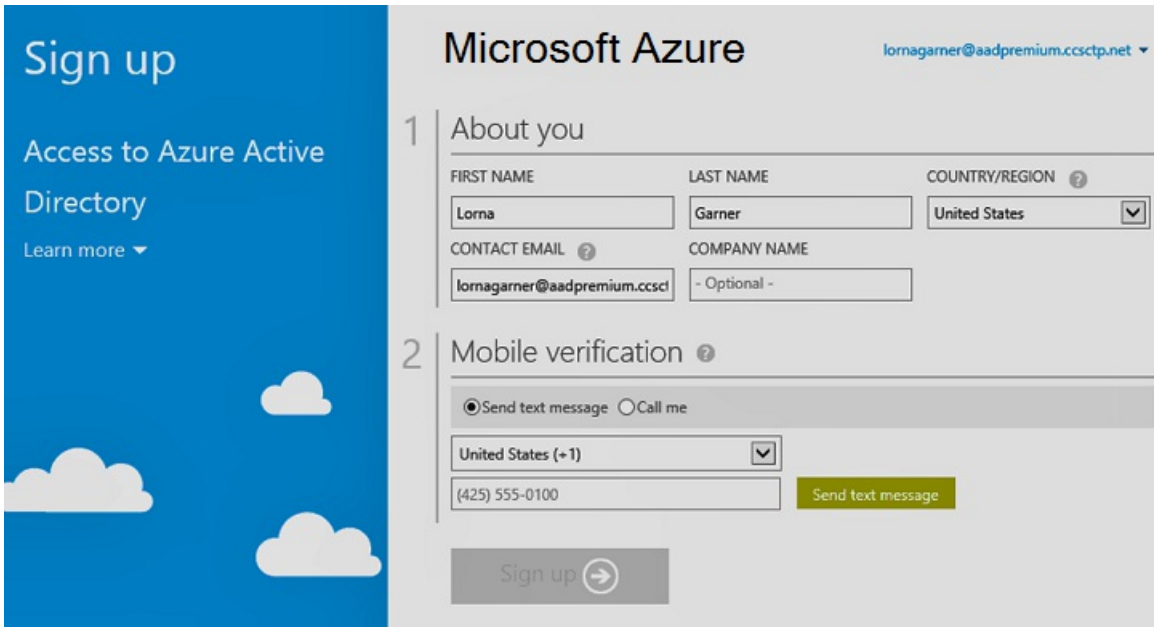
> **TIP**
> You won't be able to access Azure AD for your new tenant until you activate Azure AD directory access from the welcome email.

To activate your Azure AD access

1. Open the **Welcome email**, and then click **Sign In**.



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.

How to: Add your custom domain name using the Azure Active Directory portal

11/7/2018 • 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 to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as *alain@contoso.com*.

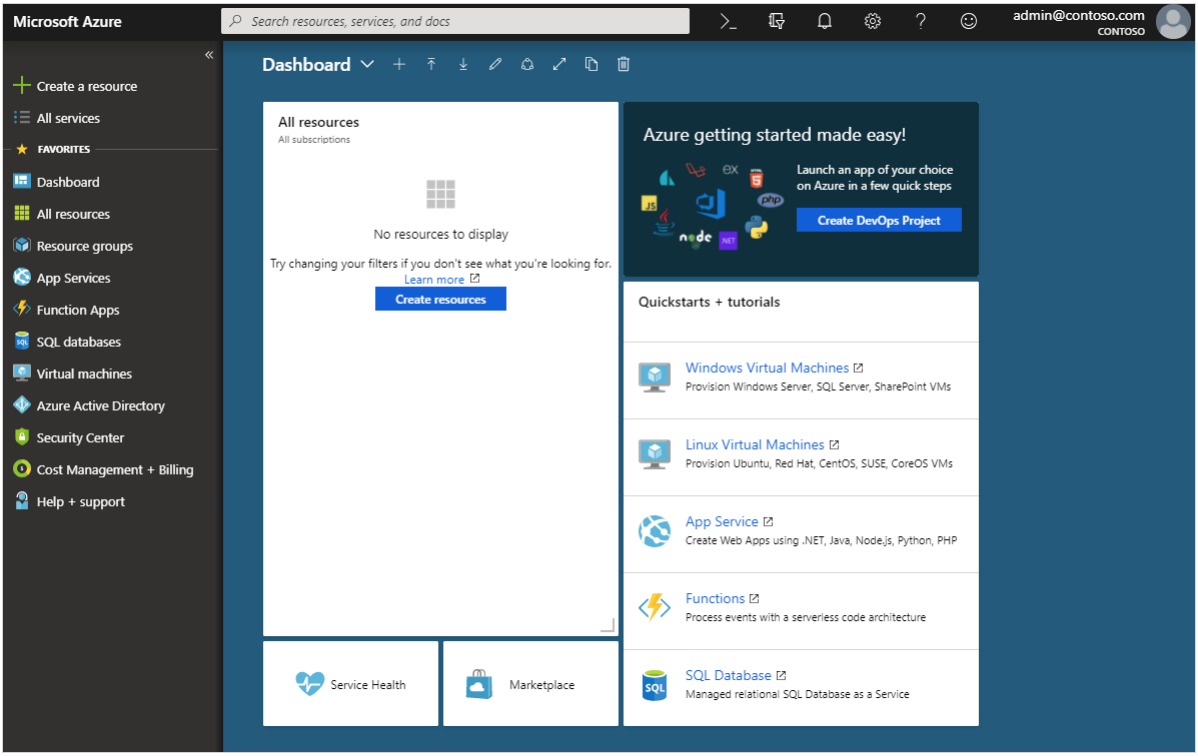
Before you begin

Before you can add a custom domain name, you must 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.

1. Sign in to the Azure portal for your directory, using an account with the **Owner** role for the subscription, and then select **Azure Active Directory**. For more information about subscription roles, see Classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles.



> **TIP**
>
> If you plan to federate your on-premises Windows Server AD with Azure AD, then you need to select the **I plan to configure this domain for single sign-on with my local Active Directory** checkbox 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. You can see what that step in the wizard looks like in these instructions. If you do not have the Azure AD Connect tool, you can download it here.

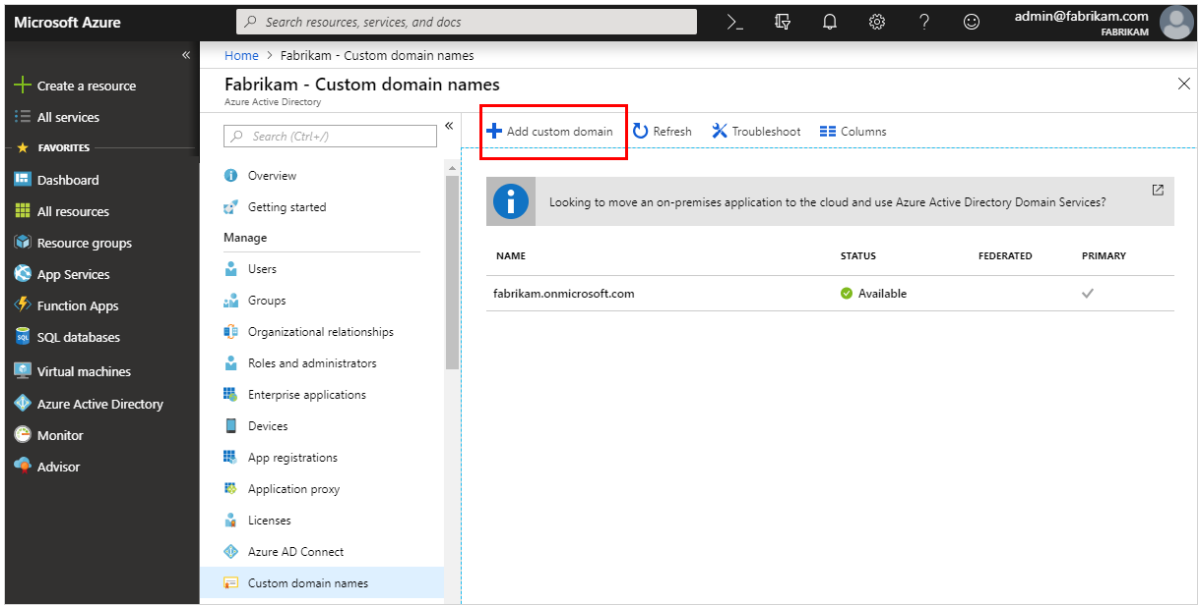
2. Create your new directory by following the steps in Create a new tenant for your organization.

> **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.

Add your custom domain name to Azure AD

After you create your directory, you can add your custom domain name.

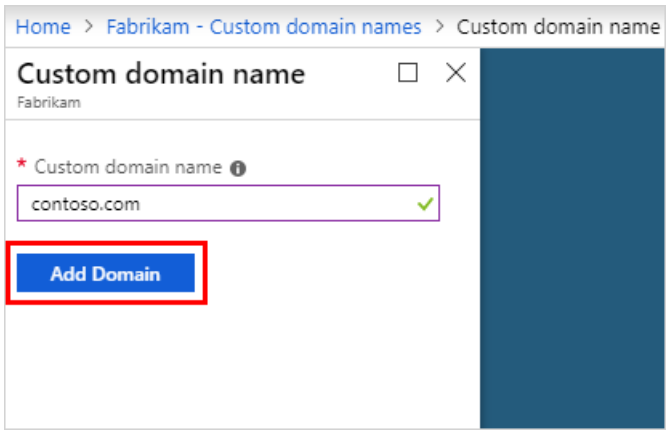
1. Select **Custom domain names**, and then select **Add custom domain**.



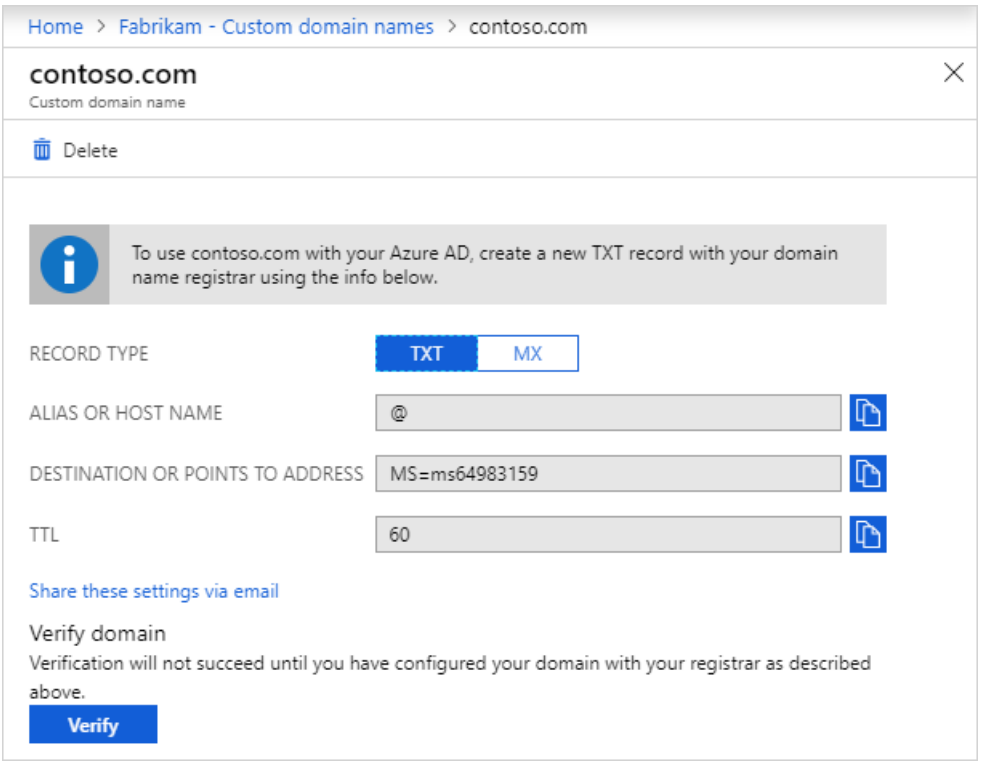
2. Type your organization's new domain name into the **Custom domain name** box (for example, *contoso.com*), and then select **Add domain**.

   The unverified domain is added and the **Contoso** page appears showing you your DNS info.

> **IMPORTANT**
>
> You must include .com, .net, or any other top-level extension for this to work properly.



3. Copy the DNS info from the **Contoso** page. For example, MS=ms64983159.



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, create a new TXT record for your domain based on your copied DNS information, set the **TTL** (time to live) to 60 minutes, and then save the information.

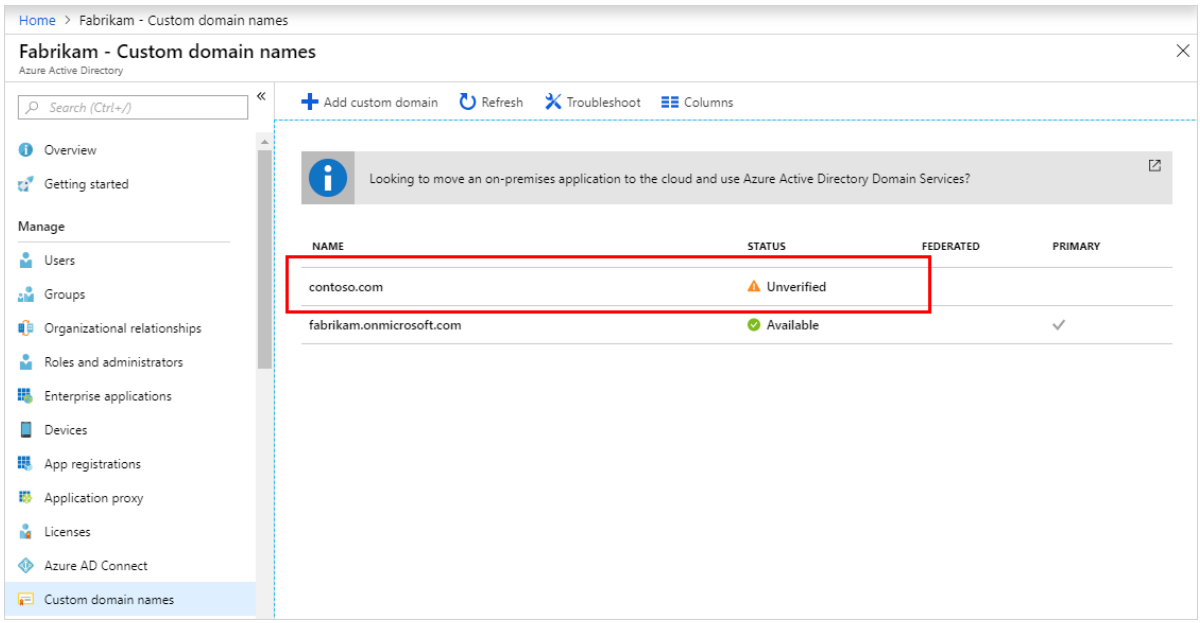
> **IMPORTANT**
> You can register as many domain names as you want. However, each domain gets its own TXT record from Azure AD. Be careful when entering your TXT file information at the domain registrar. If you enter the wrong, or duplicate information by mistake, you'll have to wait until the TTL times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

Verify your custom domain name

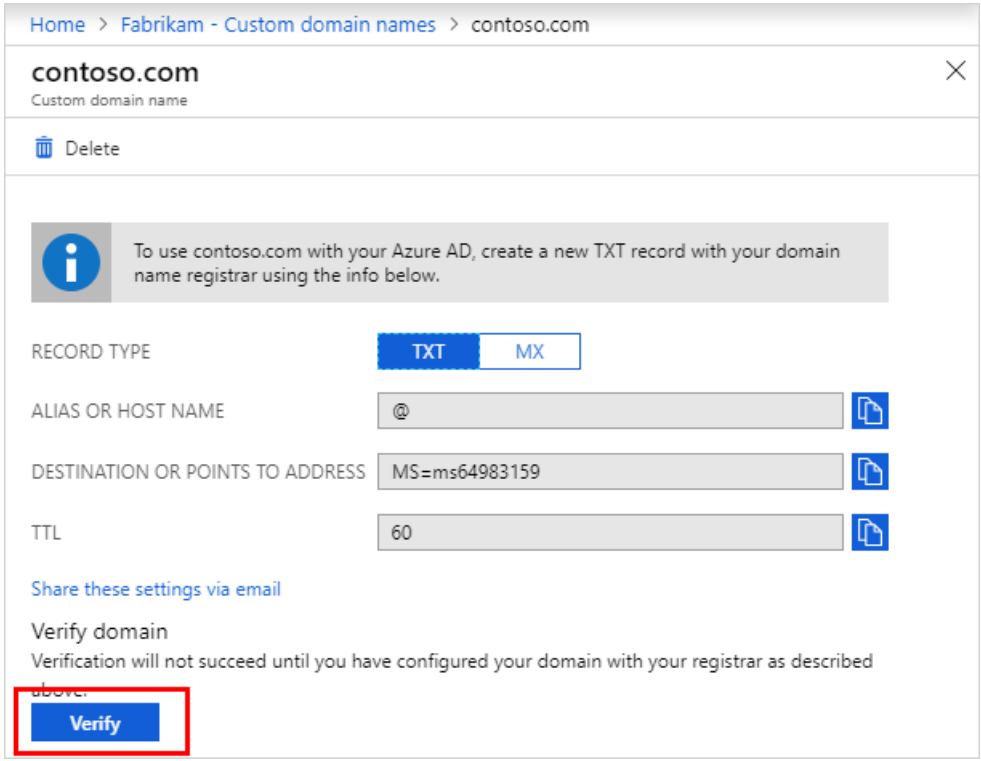
After you register your custom domain name, you need to make sure it's valid in Azure AD. The propagation from your domain registrar to Azure AD can be instantaneous or it can take up to a few days, depending on your domain registrar.

To verify your custom domain name

1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Custom domain names**.
3. On the **Fabrikam - Custom domain names** page, select the custom domain name, **Contoso**.



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



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 and this process can take an hour or more.
  - **Make sure the DNS record is correct.** Go back to the domain name registrar site and 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, you must share the entry with someone that has the right permissions to add the entry and verify it's accurate.
- **Make sure the domain name isn't already in use in another directory.** A domain name can only be verified in one directory, which means that 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. To learn more about how to take over an unmanaged directory, 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, 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.

How to: Add branding to your Azure Active Directory sign-in page

9/19/2018 • 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

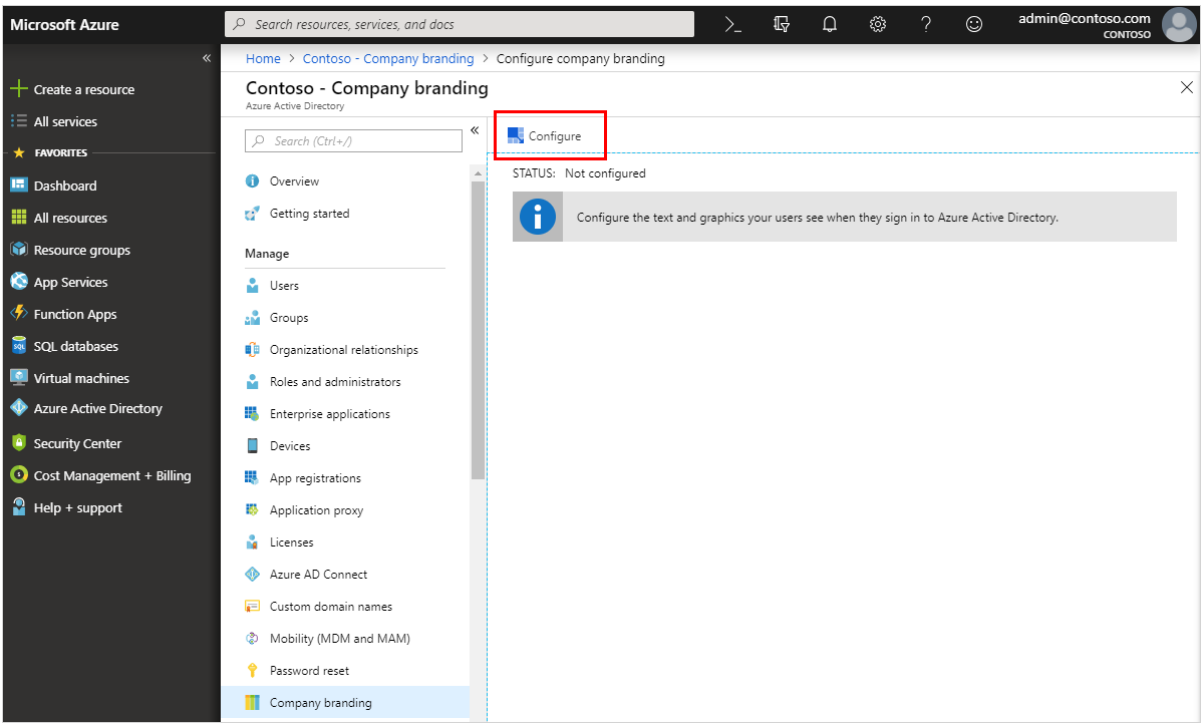
You can customize your Azure AD sign-in pages, which appear when users sign in to your organization's tenant-specific apps, such as *https://outlook.com/contoso.com*, or when passing a domain variable, such as *https://passwordreset.microsoftonline.com/?whr=contoso.com*.

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.

> **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

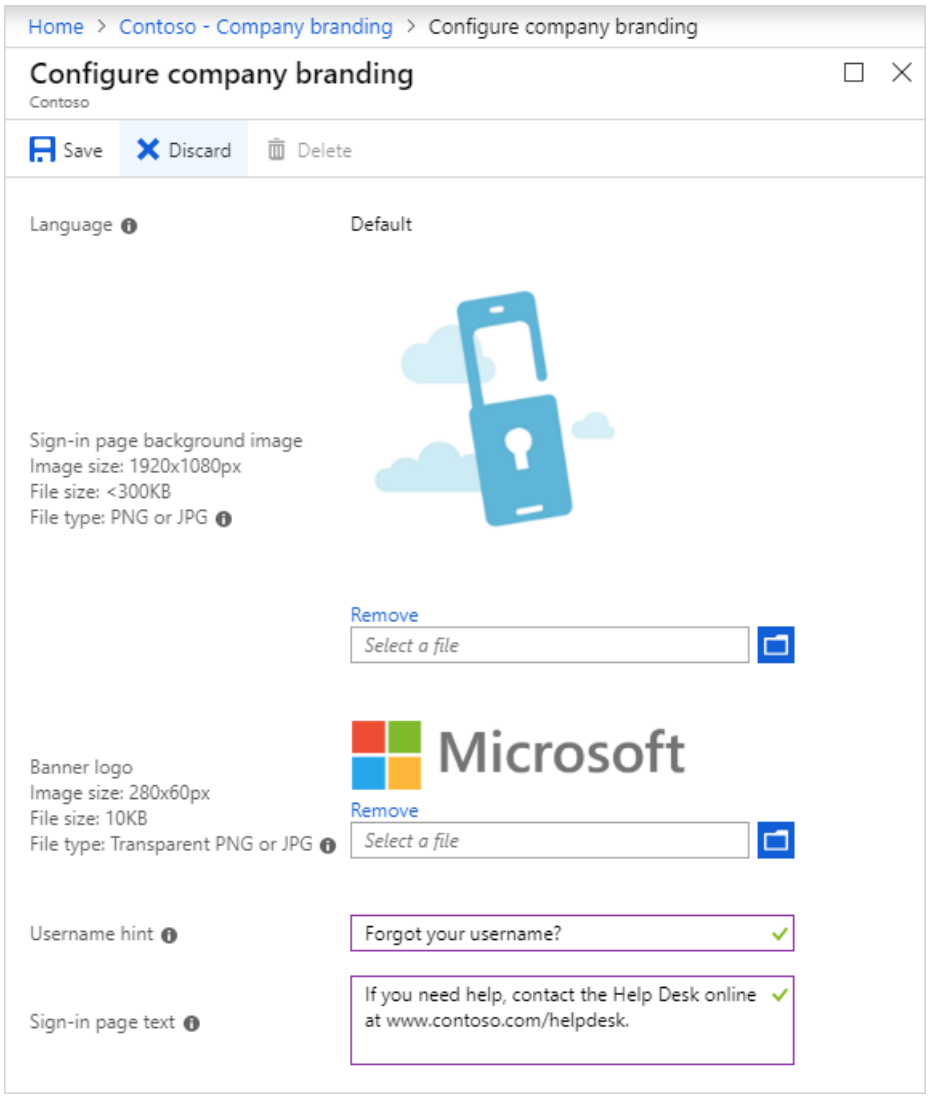
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **Configure**.



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**

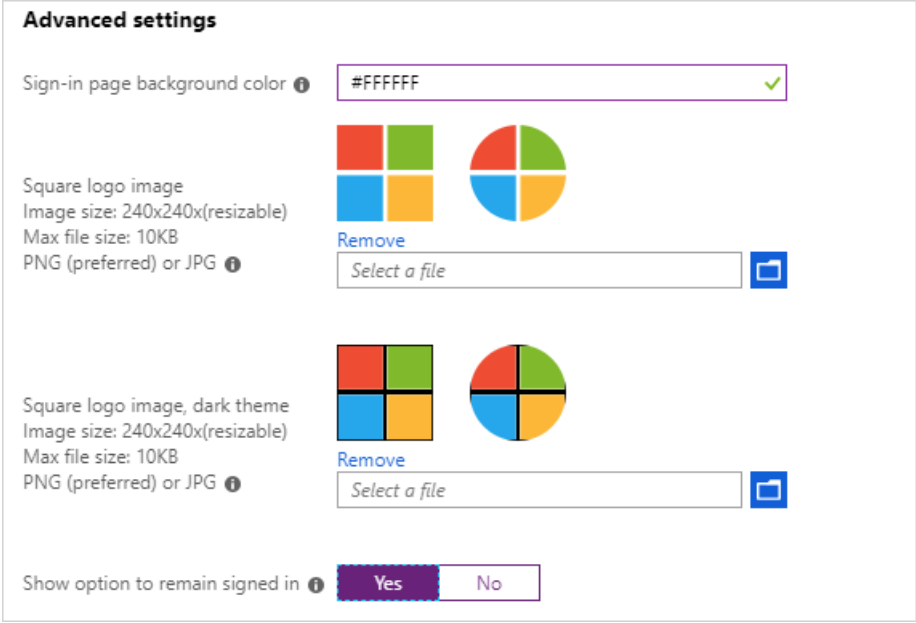


- **Language.** The language is automatically set as your default and can't be changed.
- **Sign-in page background image.** Select a .png or .jpg image file to appear as the background for your sign-in pages.

  The image can't be larger than 1920x1080 pixels in size and must have a file size of less than 300 KB.
- **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 36 pixels or wider than 245 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.** 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 256 characters. We also suggest not including links or HTML tags.

- **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.

  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.

  > **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

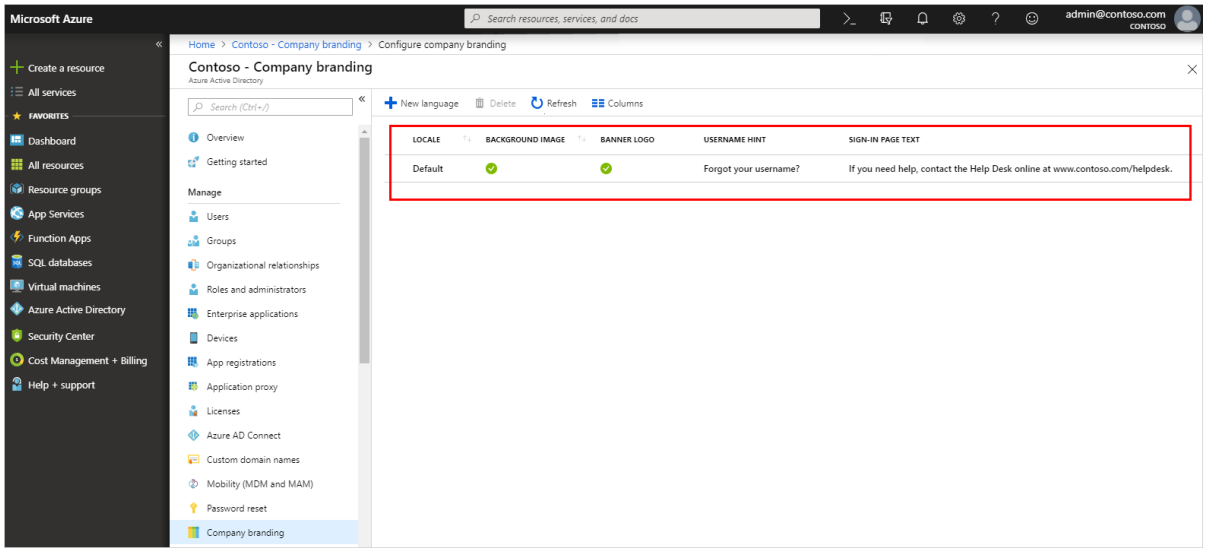
To add more corporate branding configurations to your tenant, you must choose **New language** on the **Contoso - Company branding** page. This opens the **Configure company branding** page, where you can follow the same steps as above.

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**.

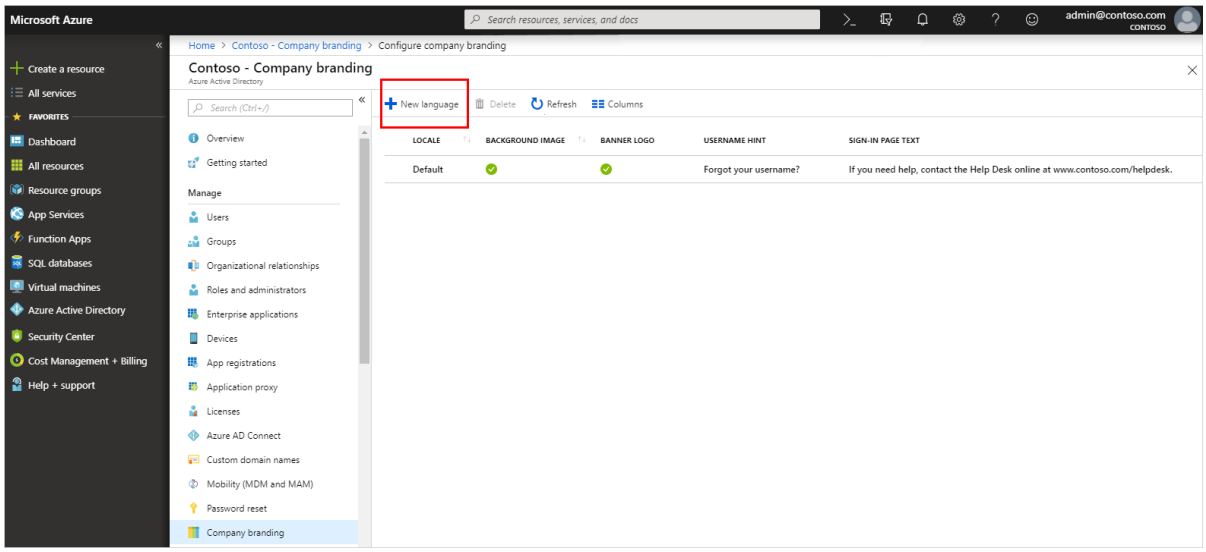
   It can take up to an hour for any changes you made to the sign-in page branding to appear.

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

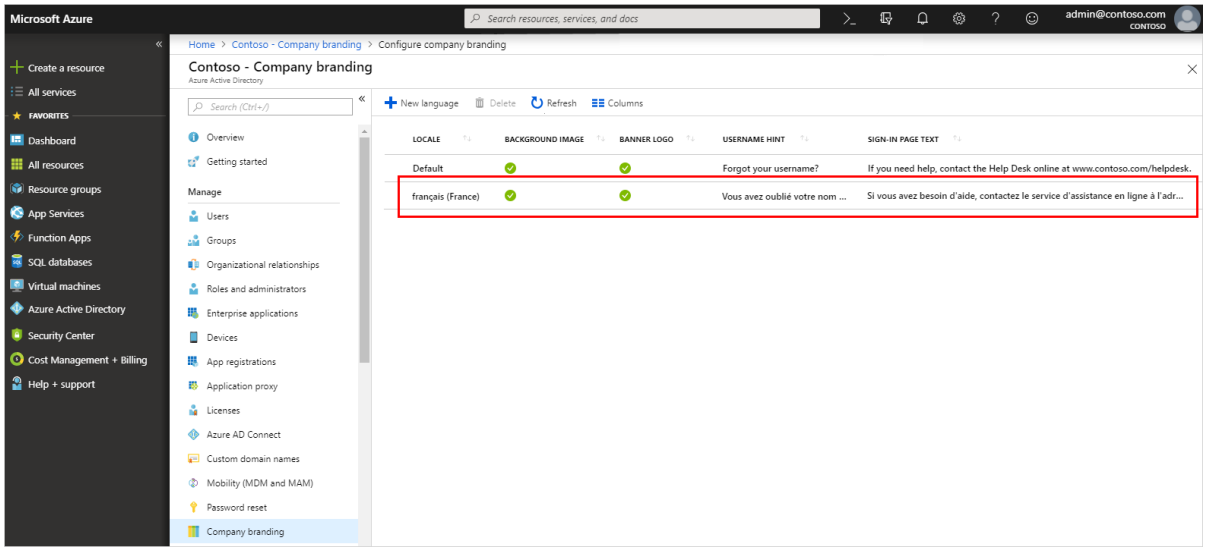
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **New language**.



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

How to: Associate or add an Azure subscription to Azure Active Directory

9/17/2018 • 2 minutes to read • Edit Online

The Azure subscription has a trust relationship with Azure Active Directory (Azure AD), which means that the subscription trusts Azure AD to authenticate users, services, and devices. Multiple subscriptions can trust the same Azure AD directory, but 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, letting you associate and manage the directory using a different Azure subscription.

All of your users have a single "home" directory for authentication. However, 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**
> All Role-Based Access Control (RBAC) users with assigned access, along with all subscription admins will lose access after the subscription directory changes. Additionally, if you have any key vaults, they'll also be affected by the subscription move. To fix that, you must change the key vault tenant ID before resuming operations.

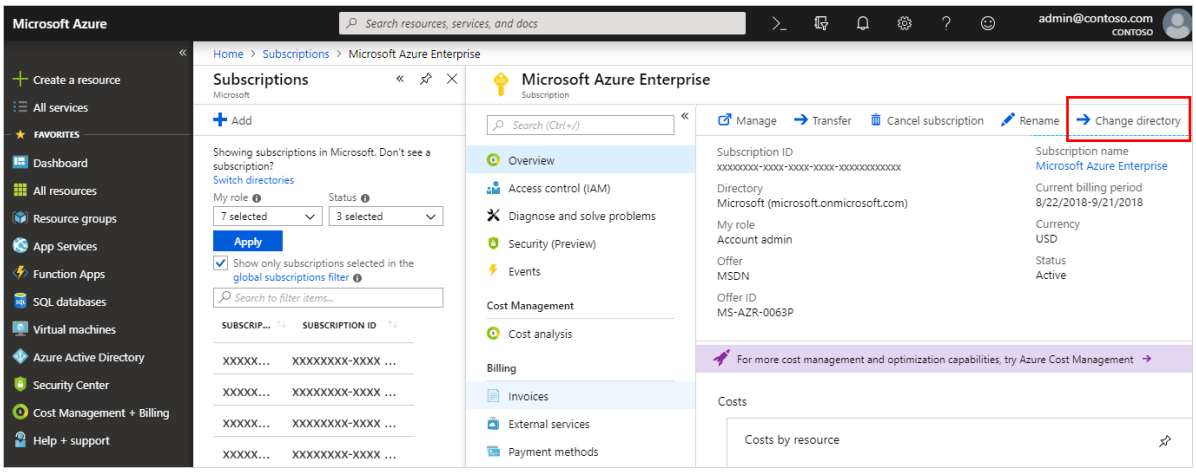
Before you begin

Before you can associate or add your subscription, you must perform the following tasks:

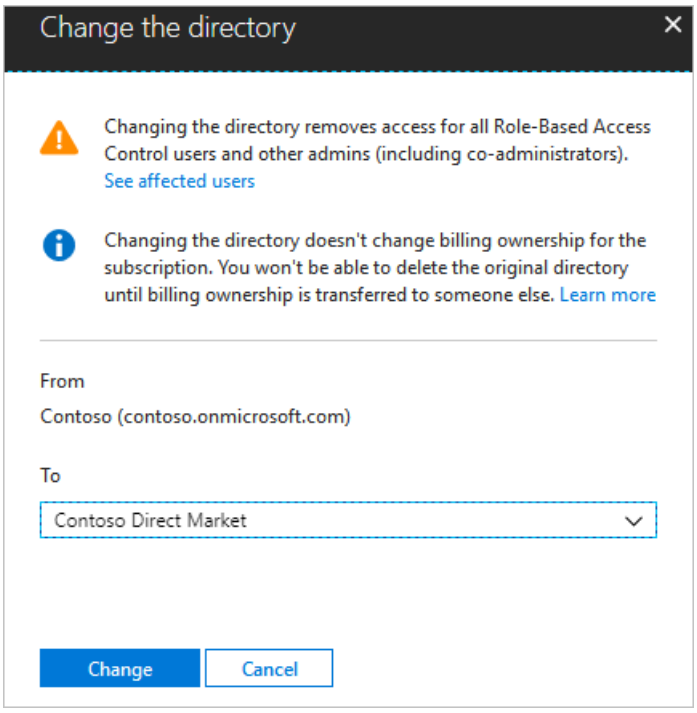
- Sign in using an account that:
  - Has **RBAC Owner** access to the subscription.
  - Exists in both the current directory that's associated with the subscription and in the new directory that's where you want to associate the subscription going forward. For more information about getting access to another directory, see How do Azure Active Directory admins add B2B collaboration users?.
- 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).

To associate an existing subscription to your Azure AD directory

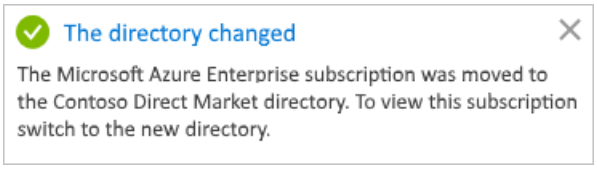
1. Sign in and select the subscription you want to use from the Subscriptions page in Azure portal.
2. Select **Change directory**.



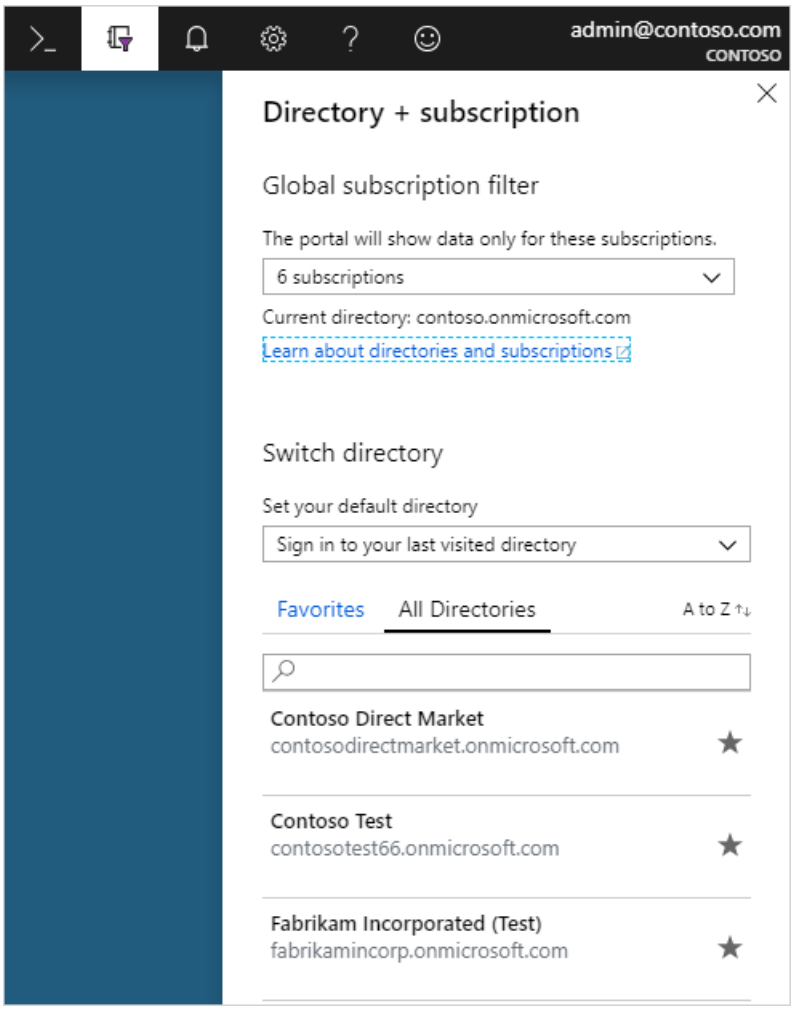
3. Review any warnings that appear, and then select **Change**.



The directory is changed for the subscription and you get a success message.



4. Use the Directory switcher to go to your new directory. It might take up to 10 minutes for everything to show up properly.



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.

Next steps

- To create a new Azure AD tenant, see Access Azure Active Directory to create a new tenant
- To learn more about how resource access is controlled in Microsoft Azure, see Understanding resource access in Azure
- To learn more about how to assign roles in Azure AD, see How to assign directory roles to users with Azure Active Directory

How-to: Add your privacy info using Azure Active Directory

10/9/2018 • 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**
> If you're interested in viewing or deleting personal data, please see the Azure Data Subject Requests for the GDPR article. If you're looking for general info about GDPR, see the GDPR section of the Service Trust portal.

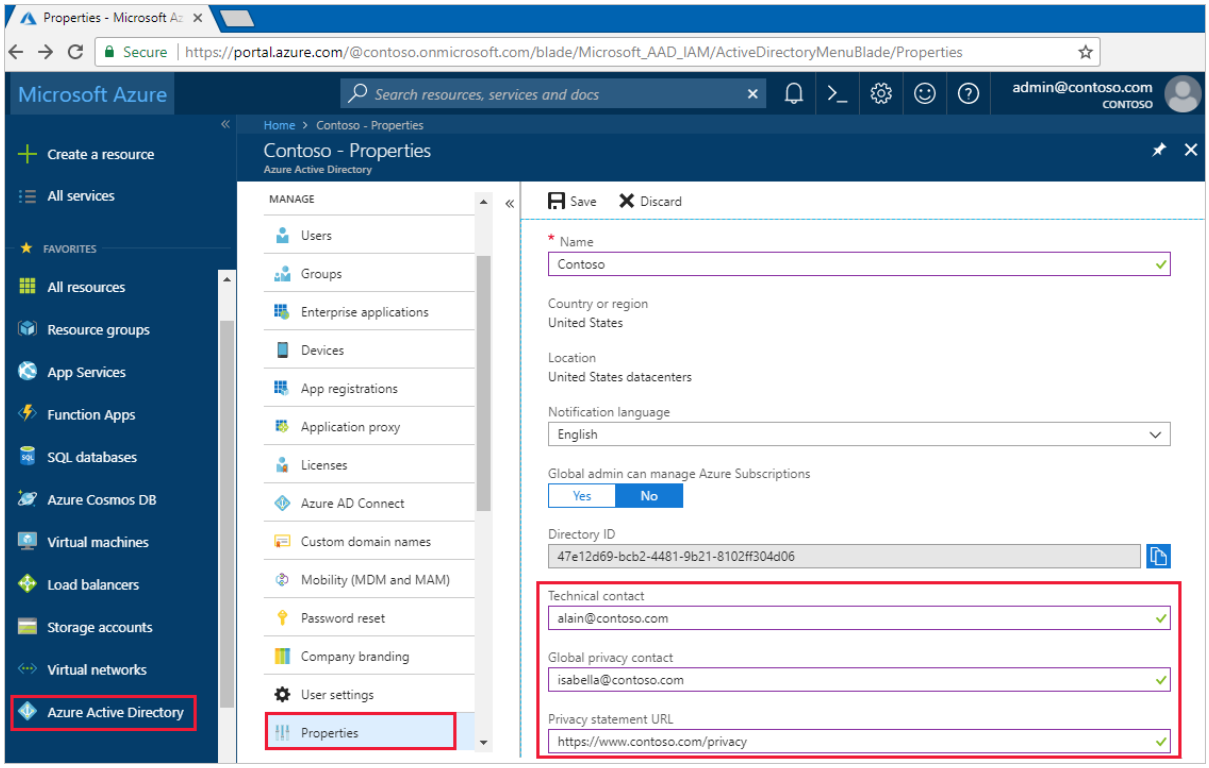
Add your privacy info on Azure AD

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.



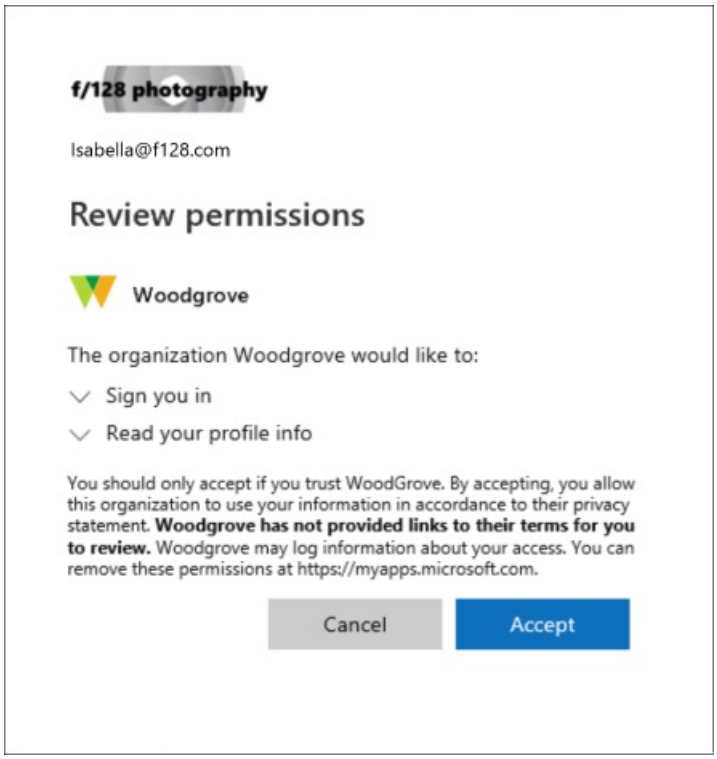
3. Add your privacy info for your employees:

   - **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

How to: Create a basic group and add members using Azure Active Directory

9/13/2018 • 3 minutes to read • Edit Online

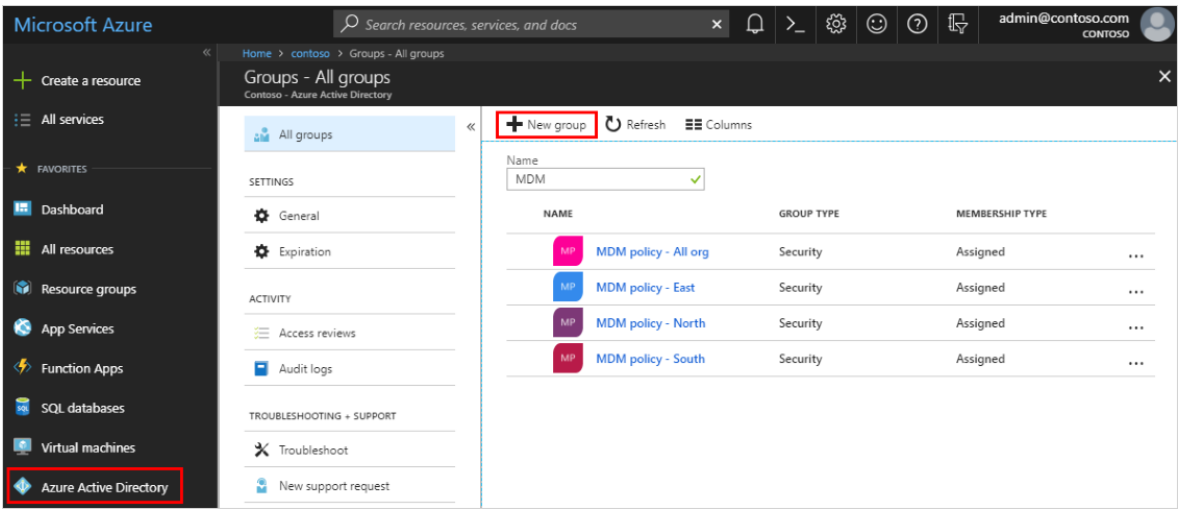
You can create a basic group using the Azure Active Directory (Azure AD) portal. For the purposes of this article, a basic group is added to a single resource by the resource owner (administrator) and includes specific members (employees) that need to access that resource. For more complex scenarios, including dynamic memberships and rule creation, see the Azure Active Directory user management documentation.

Create a basic group and add members

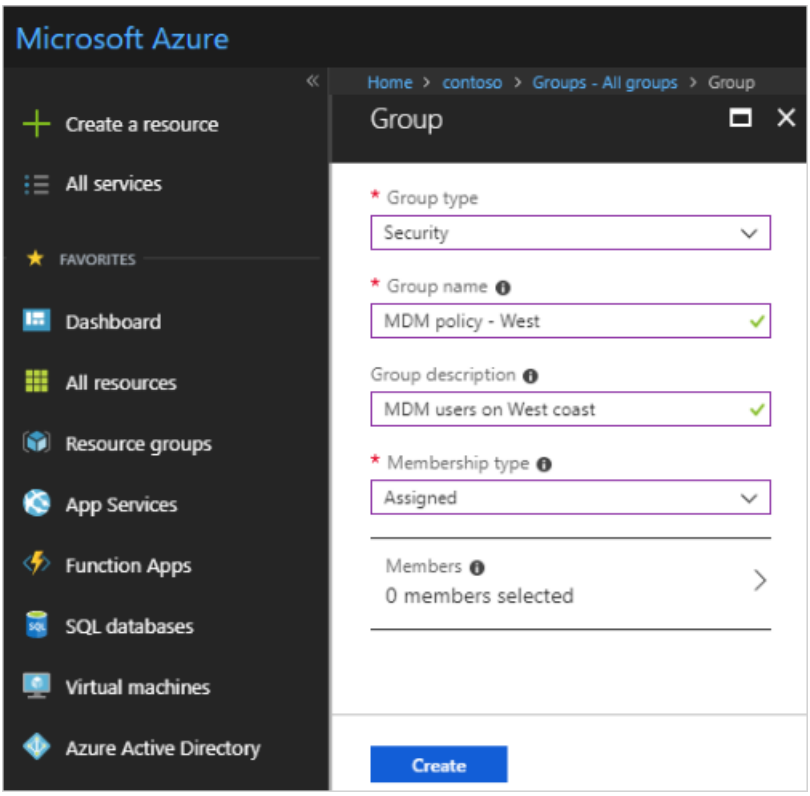
You can create a basic group and add your members at the same time.

To create a basic group and add members

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



3. In the **Group** page, fill out the required information.



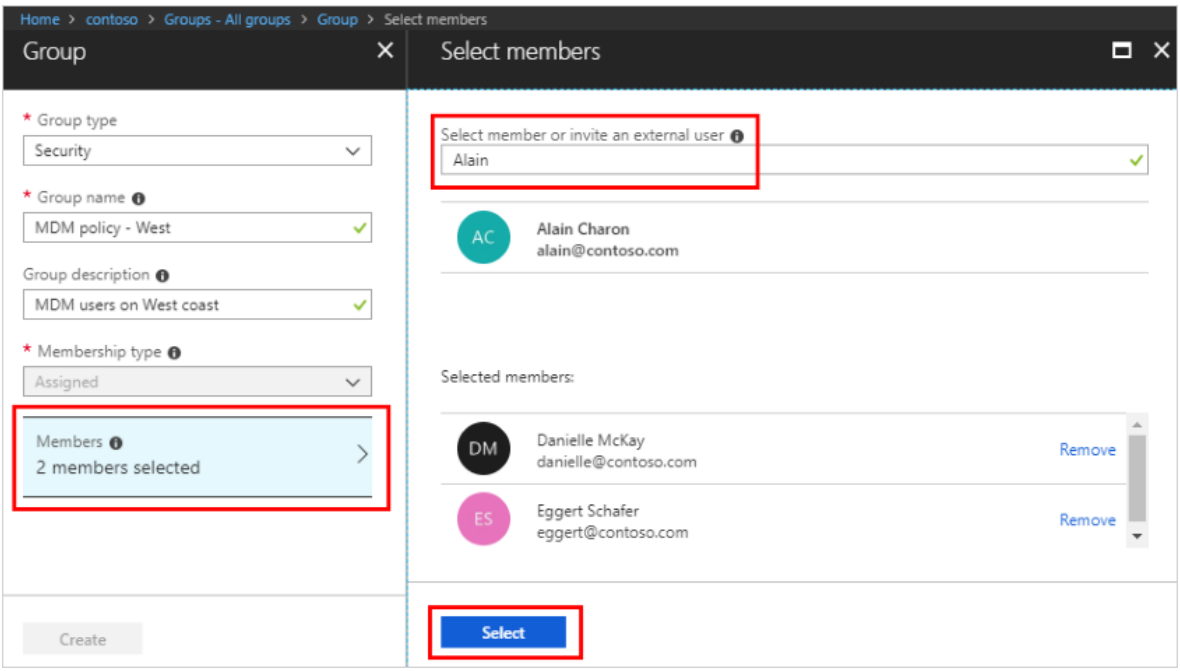
- **Group type (required).** Select a pre-defined group type. This includes:
  - **Security**. Used to manage member and computer access to shared resources for a group of users. For example, you can create a security group for a specific security policy. By doing it this way, you can give a set of permissions to all the members at once, instead of having to add permissions to each member individually. 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. For more info about Office 365 Groups, see Learn about Office 365 Groups.
- **Group name (required).** Add a name for the group, something that you'll remember and that makes sense.
- **Group description.** Add an optional description to your group.
- **Membership type (required).** Select a pre-defined membership type. This includes:
  - **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 group 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 dyncamic group and check status.

4. Select **Create**.

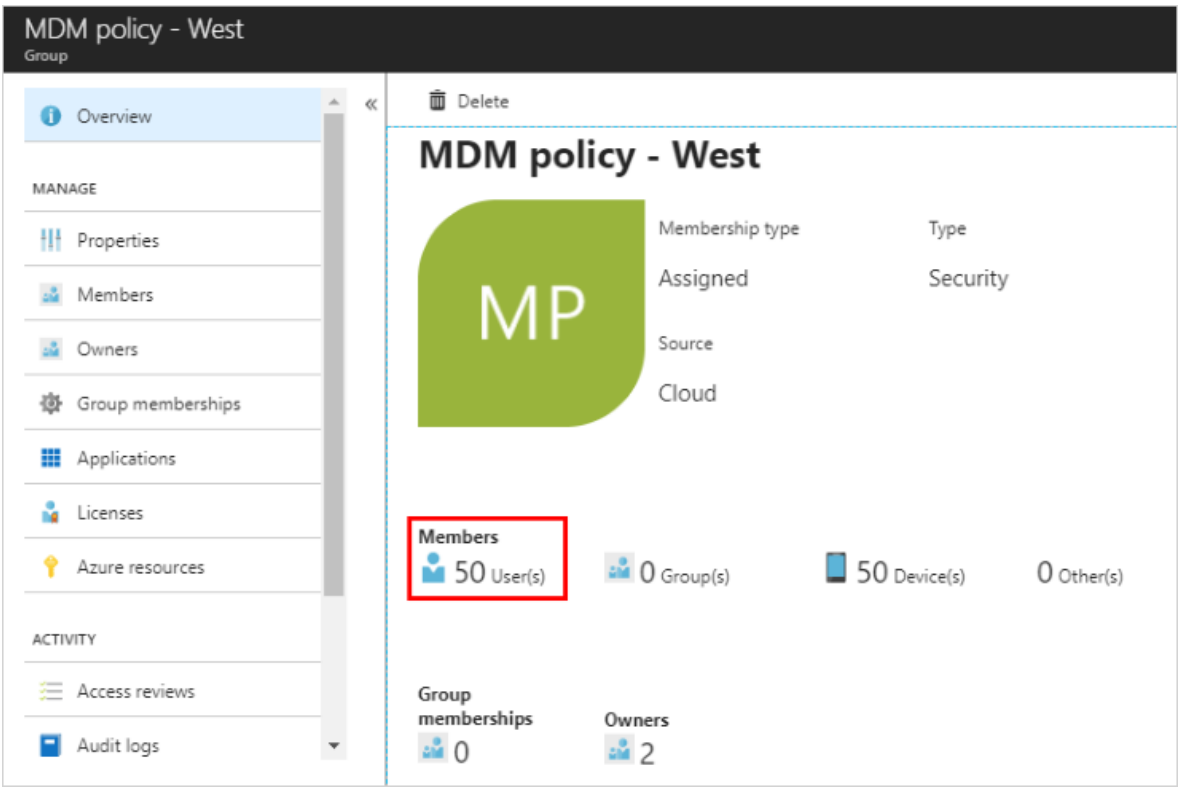
   Your group is created and ready for you to add members.

5. 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.



6. 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.



Next steps

Now that you've added a group and at least one user, you can:

- View your groups and members
- Manage group membership
- Manage dynamic rules for users in a group
- Edit your group settings
- Manage access to resources using groups
- Manage access to SaaS apps using groups
- Manage groups using PowerShell commands
- Associate or add an Azure subscription to Azure Active Directory

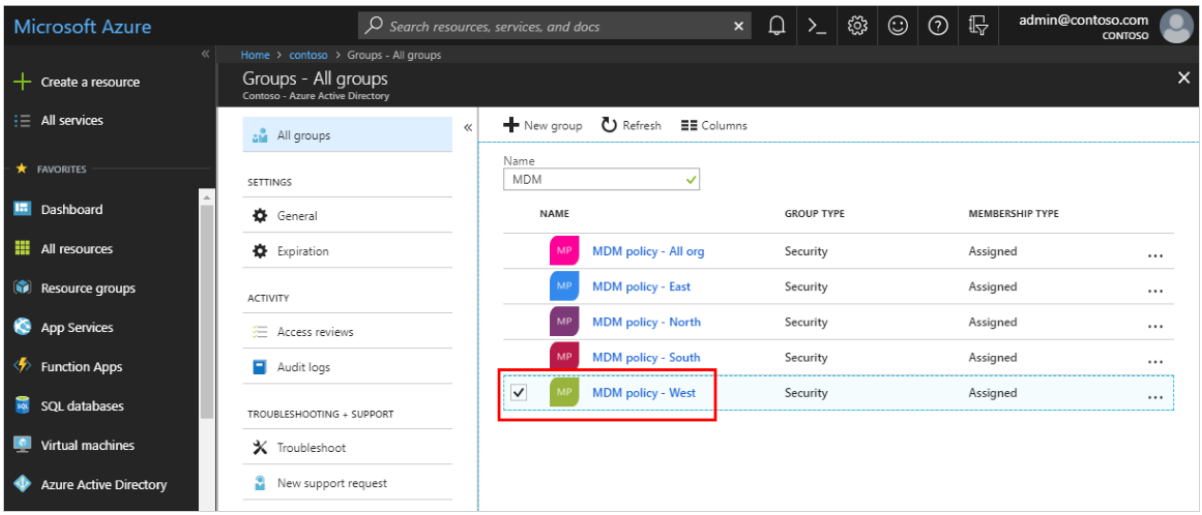
How to: Add or remove group members using Azure Active Directory

9/17/2018 • 2 minutes to read • Edit Online

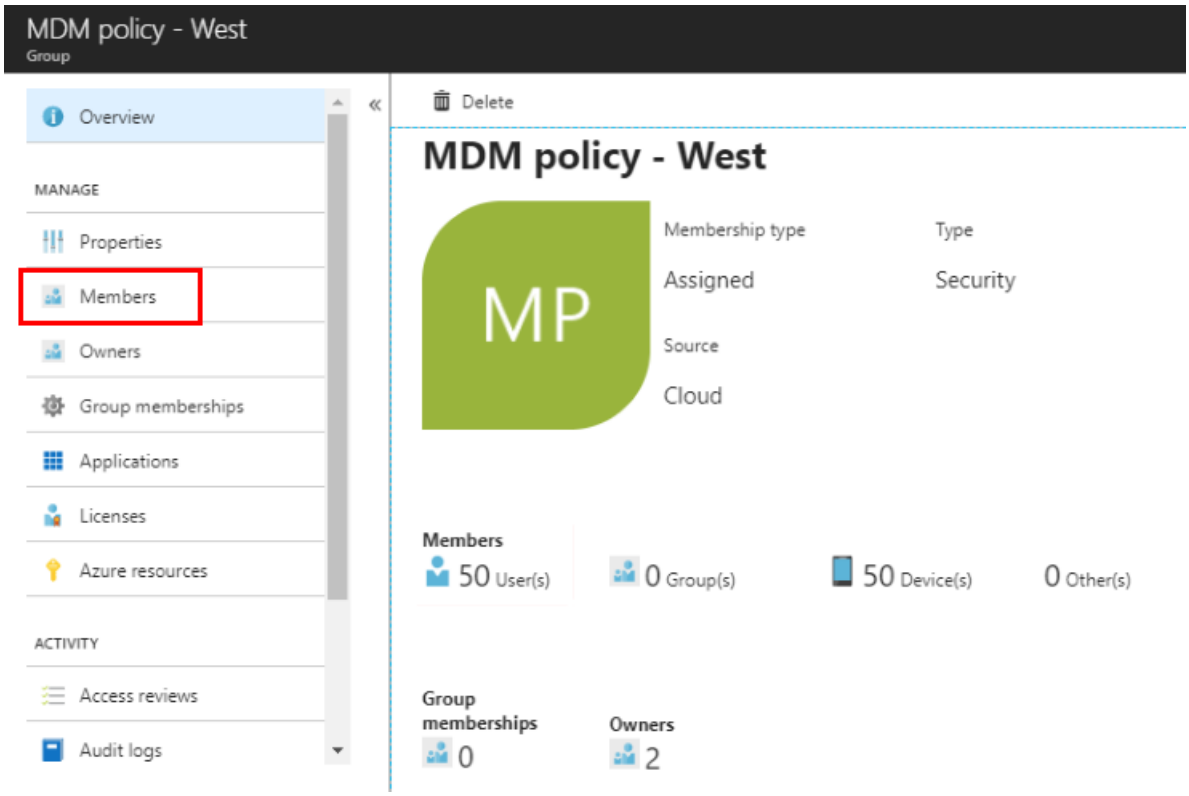
Using Azure Active Directory, you can continue to add and remove group members.

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**.

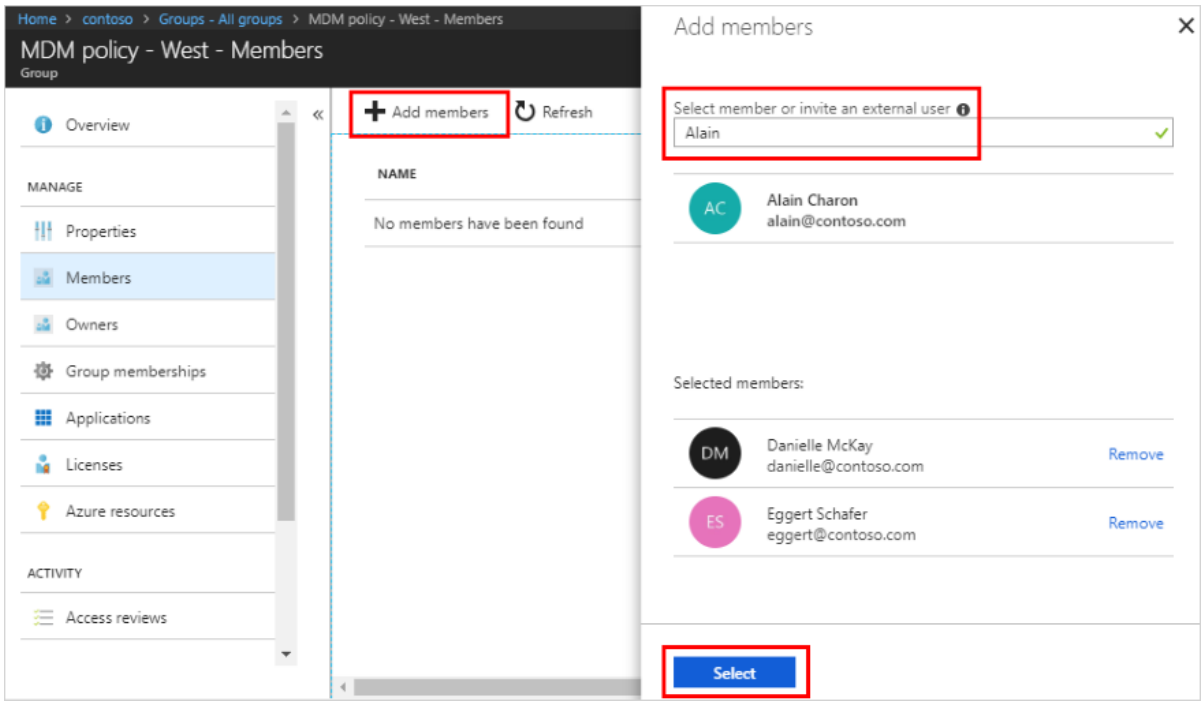


4. From the **MDM policy - West Overview** page, select **Members** from the **Manage** area.



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.

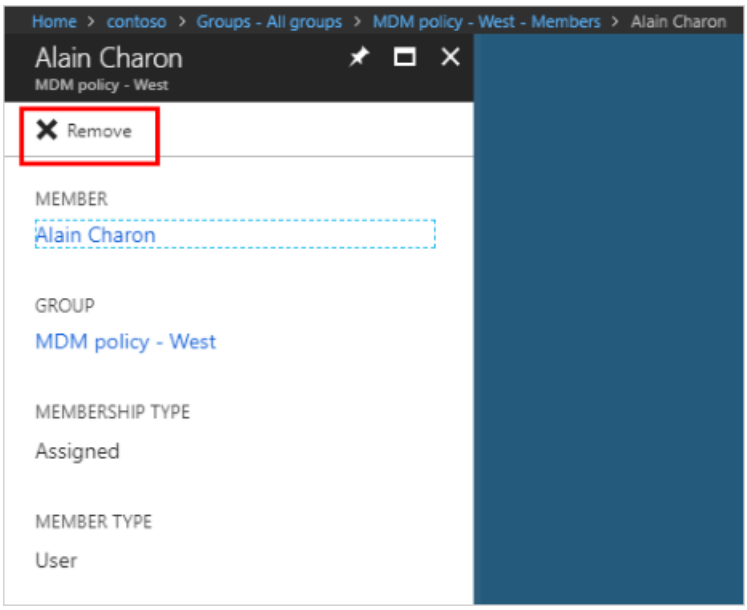


6. Refresh the screen to see all of the member names added to the group.

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

How to: Delete a group using Azure Active Directory

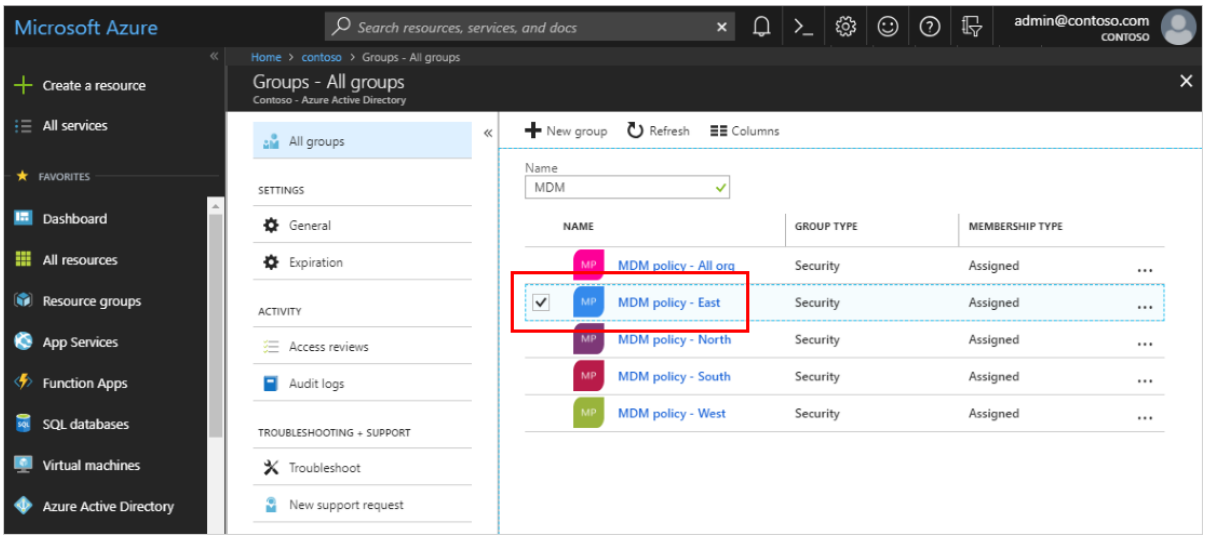
9/13/2018 • 2 minutes to read • Edit Online

You can delete a 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

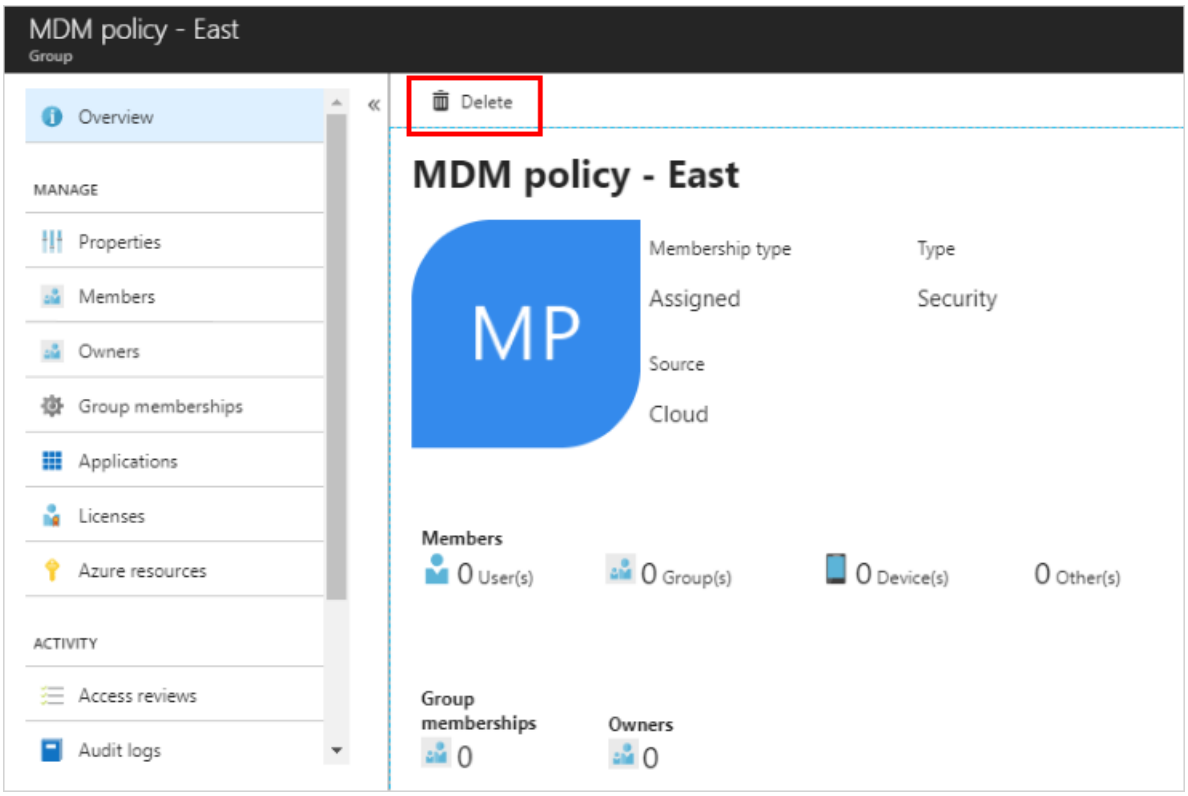
To delete a group

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.

How to: Add or remove a group from another group using Azure Active Directory

10/19/2018 • 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

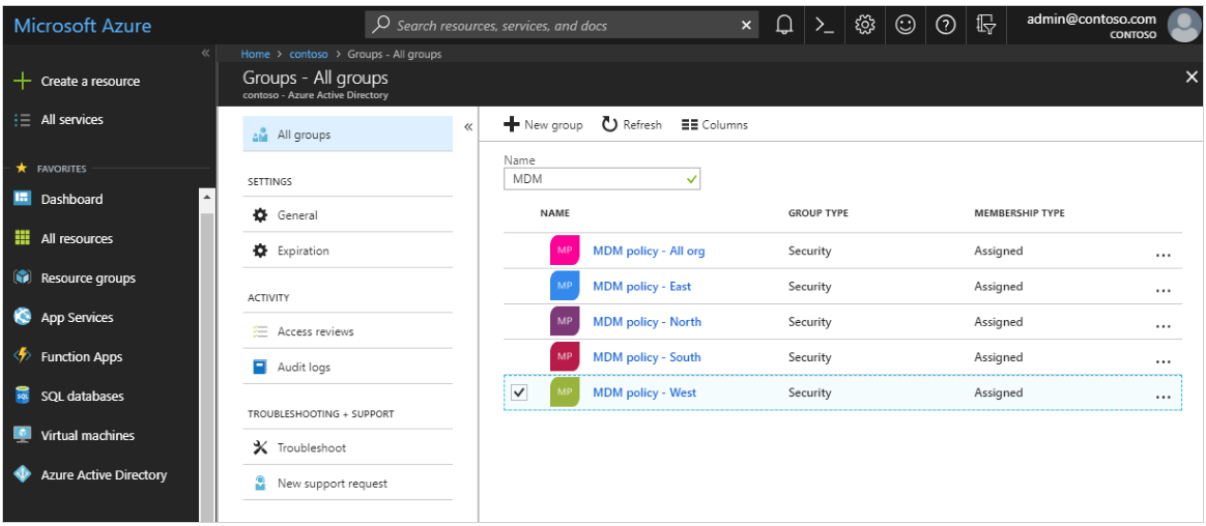
You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

> **IMPORTANT**
> We don't currently support:
>
> - Adding 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

To add a group as a member of another group

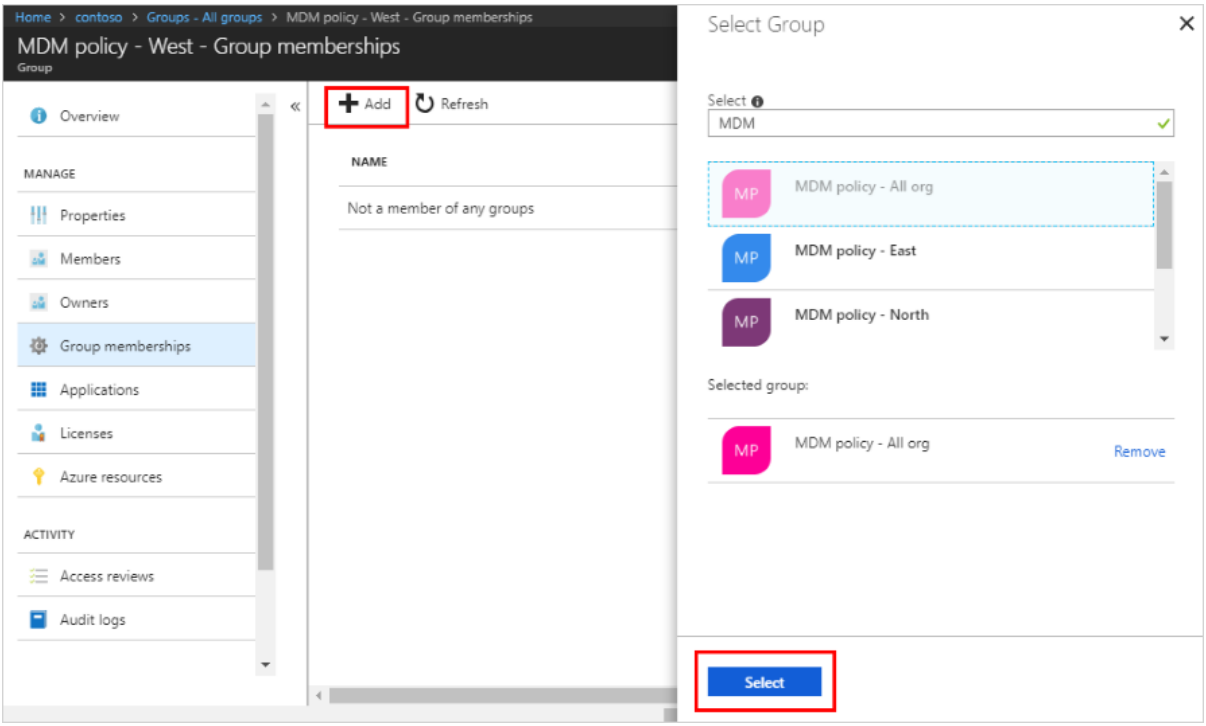
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.
3. On the **Groups - All groups** page, search for and select the group that's to become a member of another group. For this exercise, we're using the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

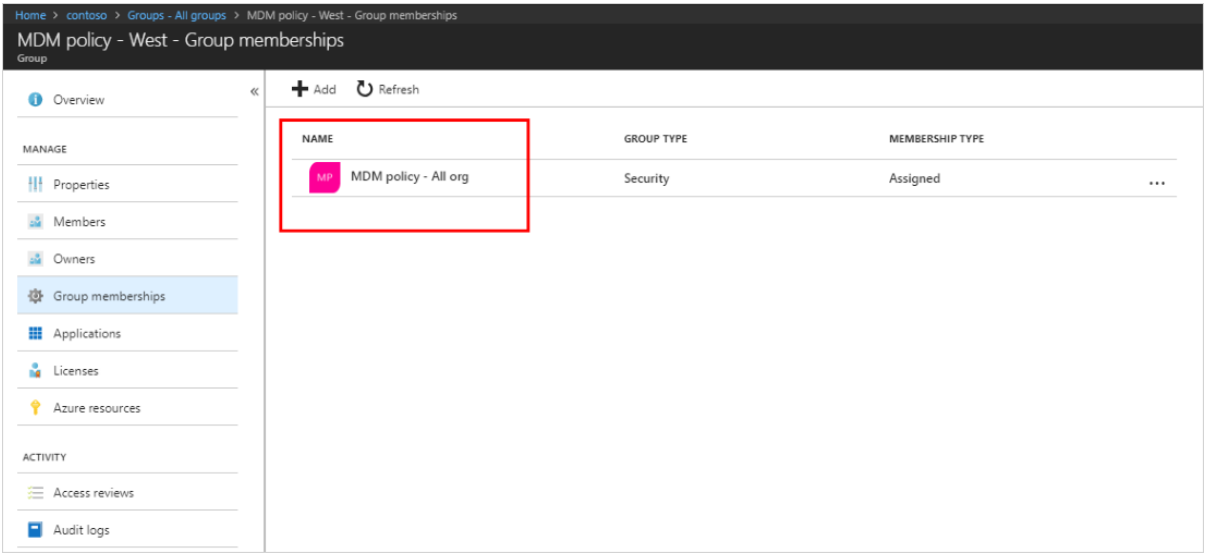


4. On the **MDM policy - West - Group memberships** page, select **Group memberships**, select **Add**, locate the group you want your group to be a member of, and then choose **Select**. For this exercise, we're using the **MDM policy - All org** group.

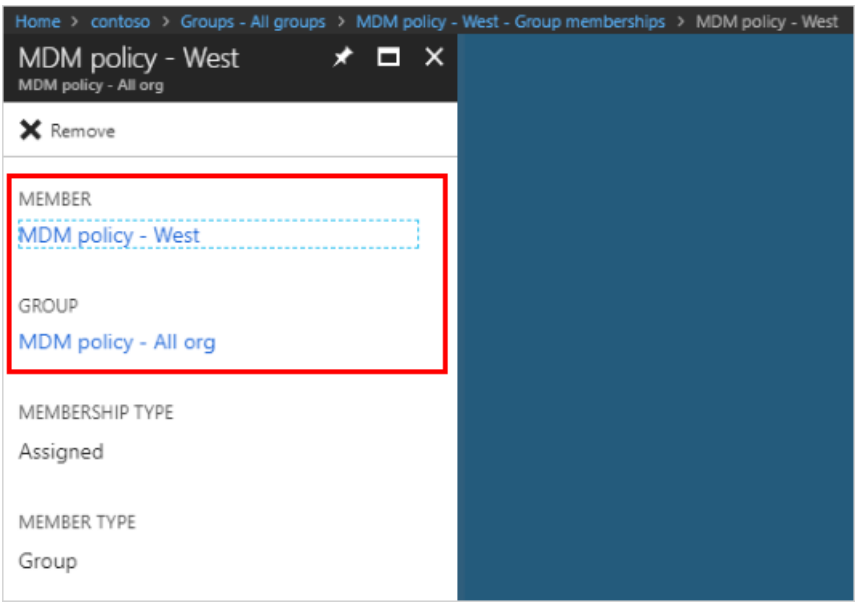
   The **MDM policy - West** group is now a member of the **MDM policy - All org** group, inheriting all the properties and configuration of the MDM policy - All org group.



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.



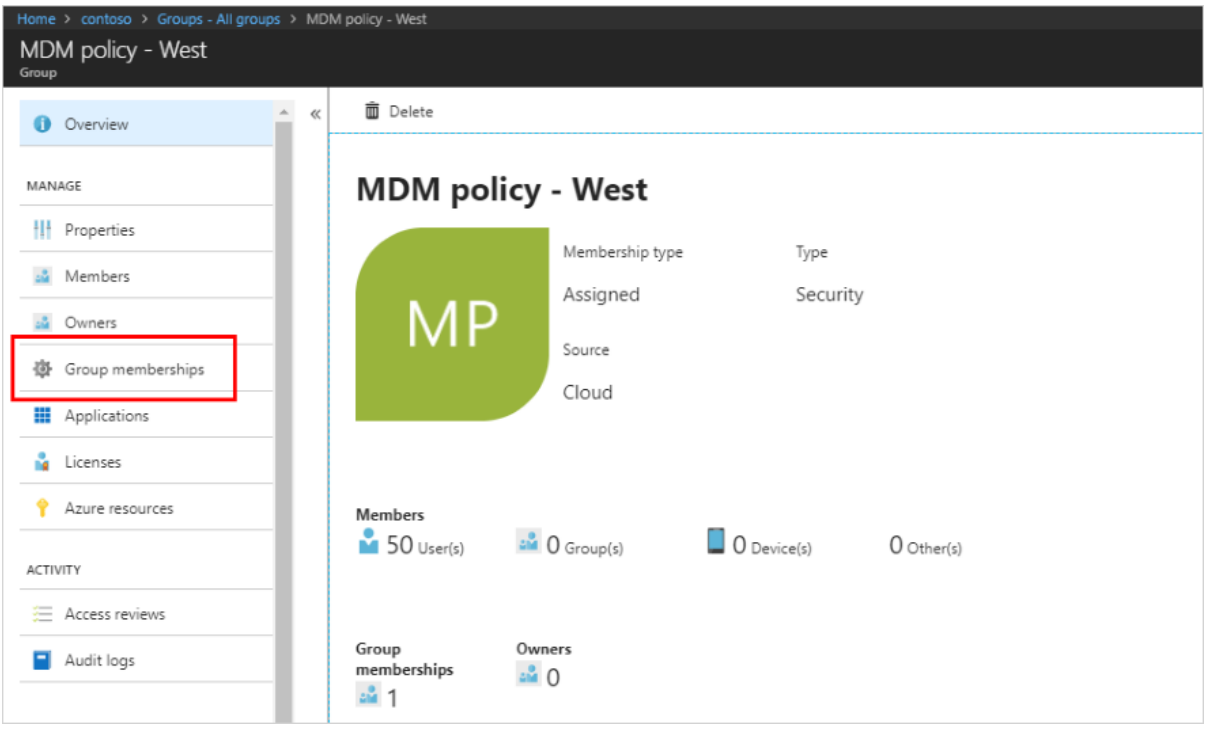
Remove a group from another group

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.

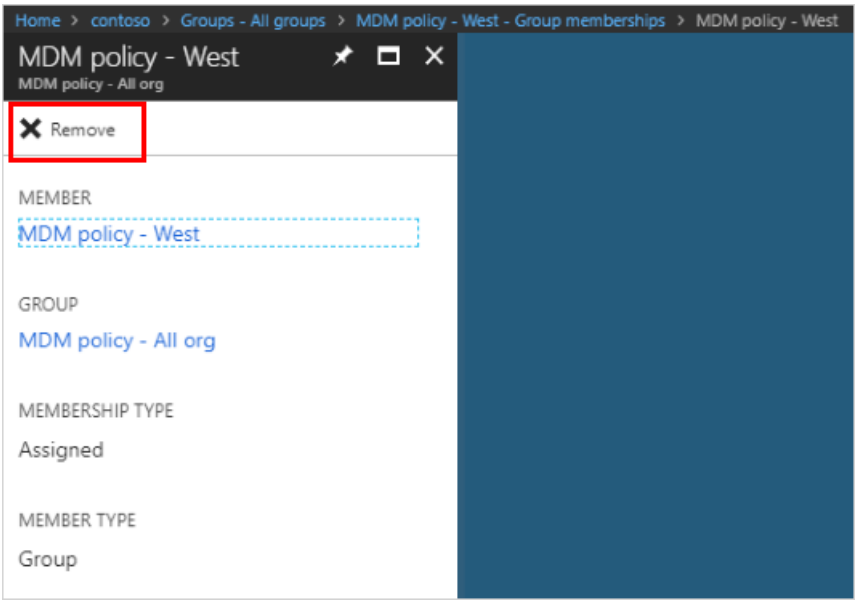
To remove a member group from another group

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

How to: Edit your group information using Azure Active Directory

9/17/2018 • 2 minutes to read • Edit Online

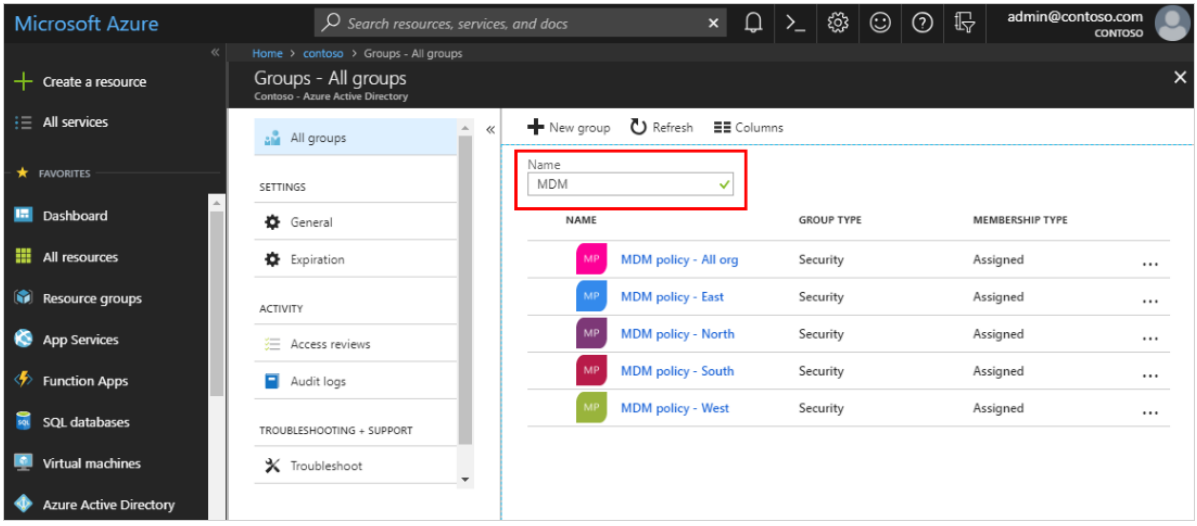
Using Azure Active Directory, you can edit a group's settings, including updating its name, description, or membership type.

To edit your group settings

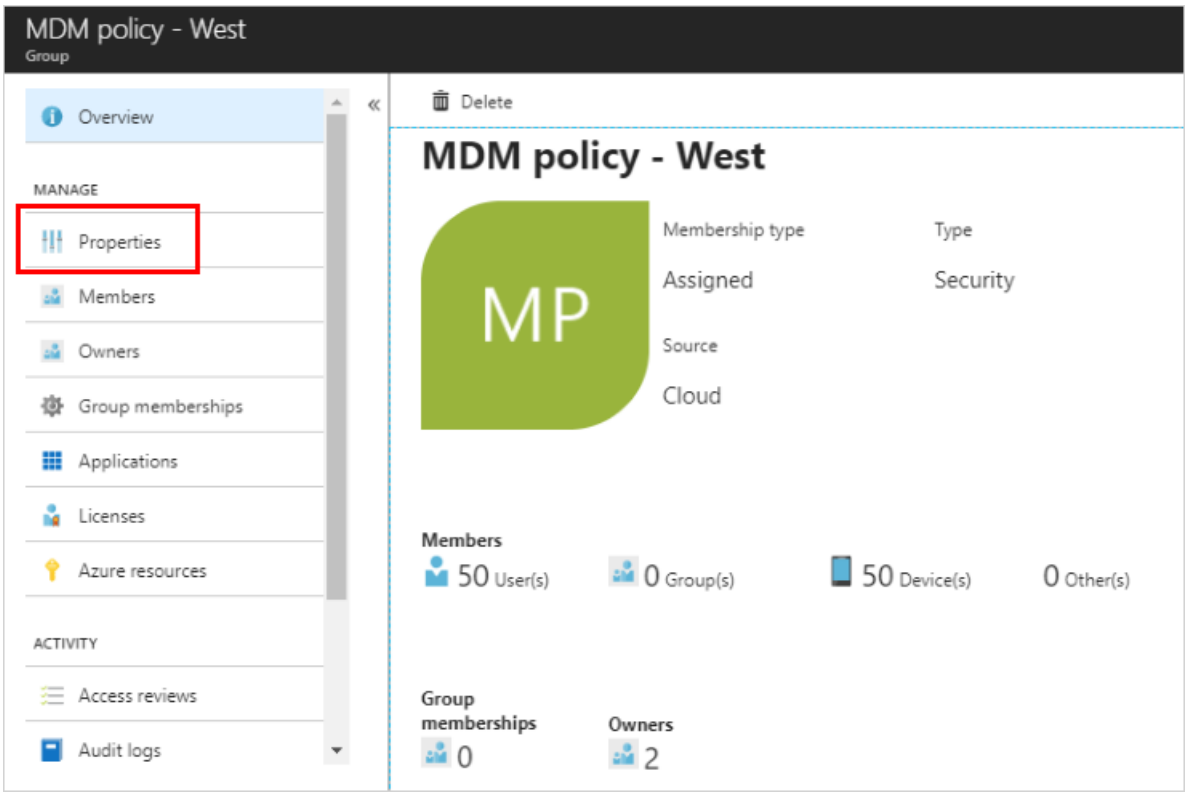
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Groups**.

   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.

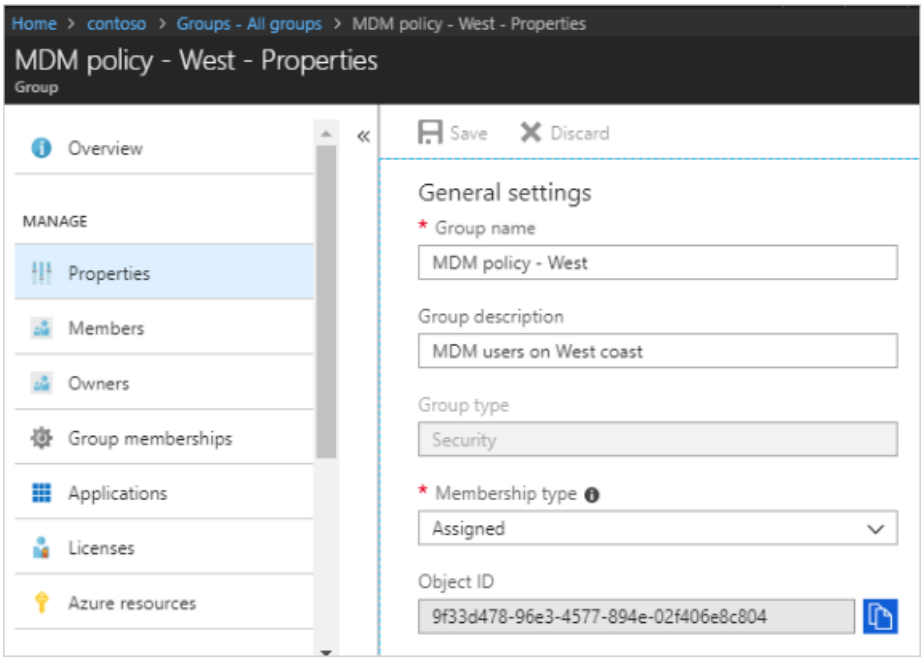
   The search results appear under the **Search** box, updating as you type more characters.



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

How to: Add or remove group owners in Azure Active Directory

10/26/2018 • 2 minutes to read • Edit Online

Azure Active Directory (Azure AD) groups are owned and managed by group owners. Group owners are assigned to manage a group and its members by a resource owner (administrator). Group owners aren't required to be members of the group. After a group owner has been assigned, only a resource owner can add or remove owners.

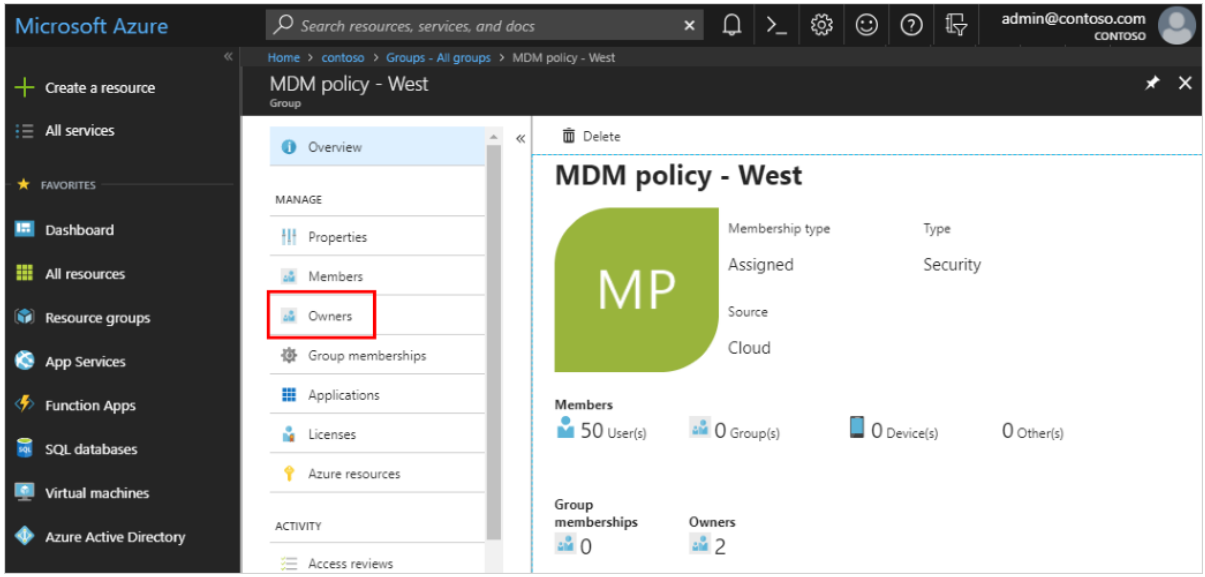
In some cases, you as the administrator might decide not to assign a group owner. In this case, you become the group owner. Additionally, owners can assign other owners to their group, unless you've restricted this in the group settings.

Add an owner to a group

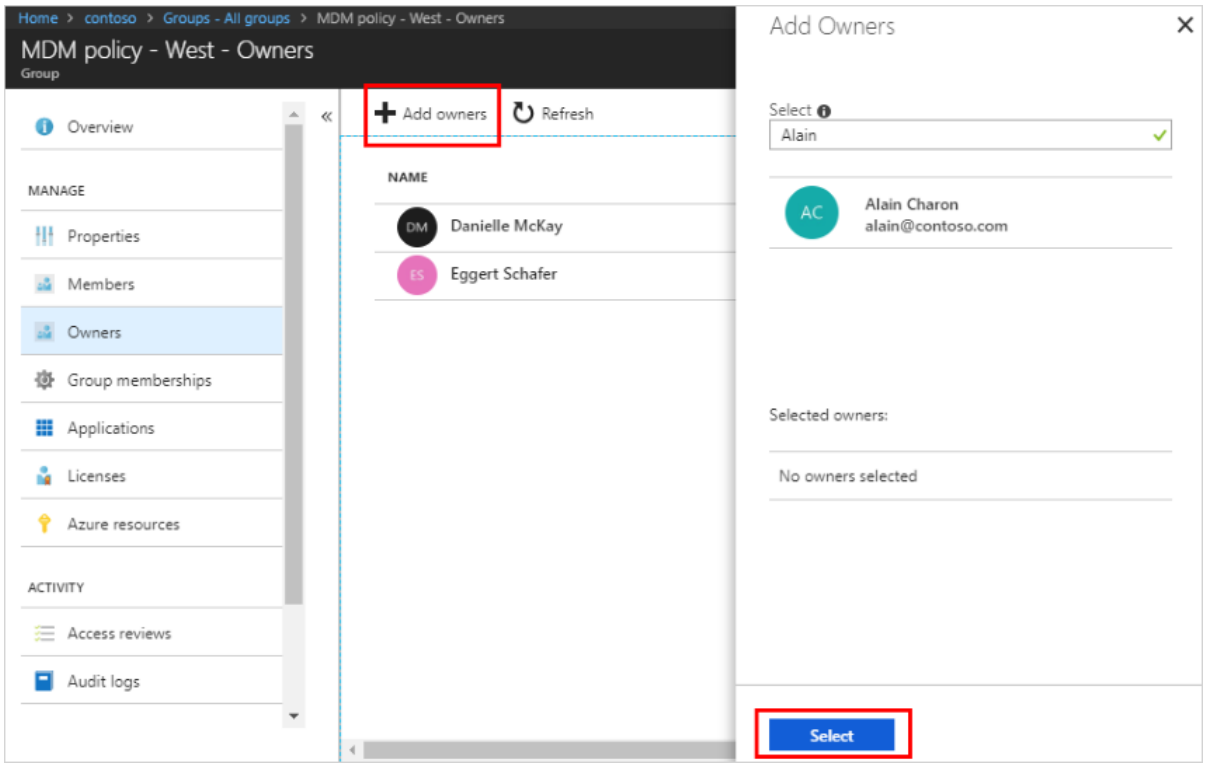
Add additional group owners to a group using Azure AD.

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**.



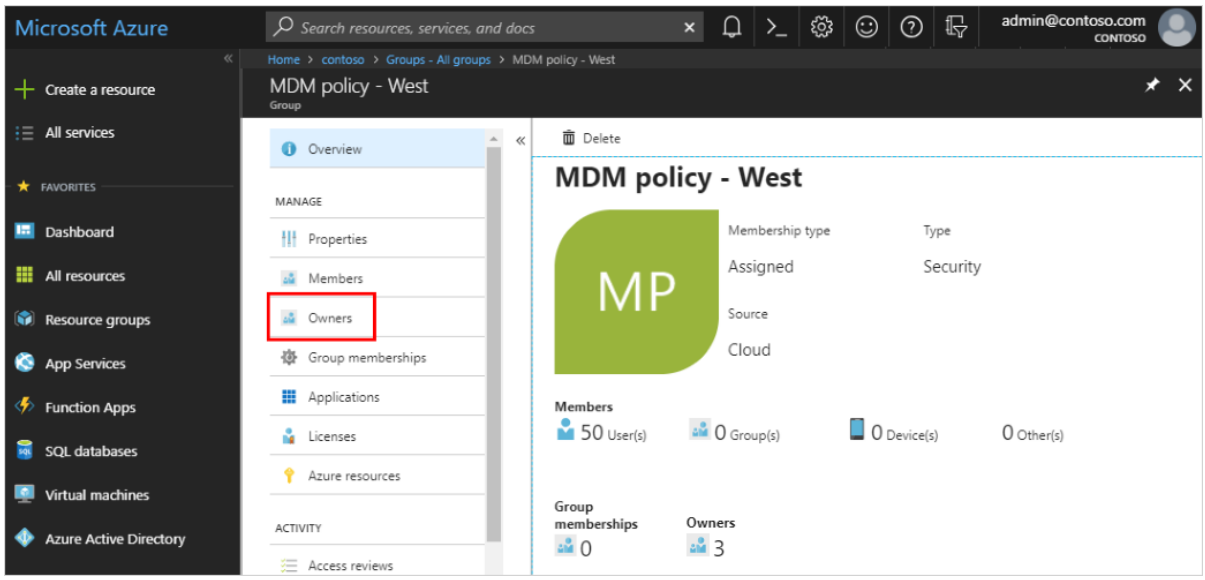
After you select the new owner, you can refresh the **Owners** page and see the name added to the list of owners.

Remove an owner from a group

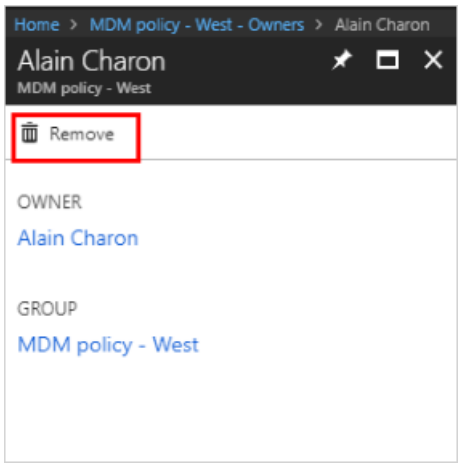
Remove an owner from a group using Azure AD.

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

How to: Add or delete users using Azure Active Directory

9/18/2018 • 3 minutes to read • Edit Online

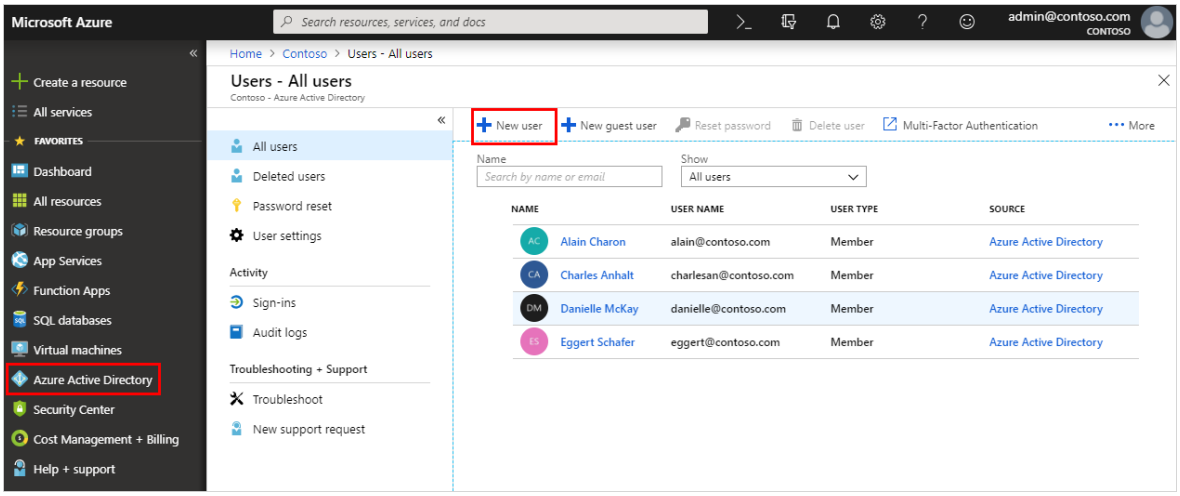
Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant, using Azure AD.

Add a new user

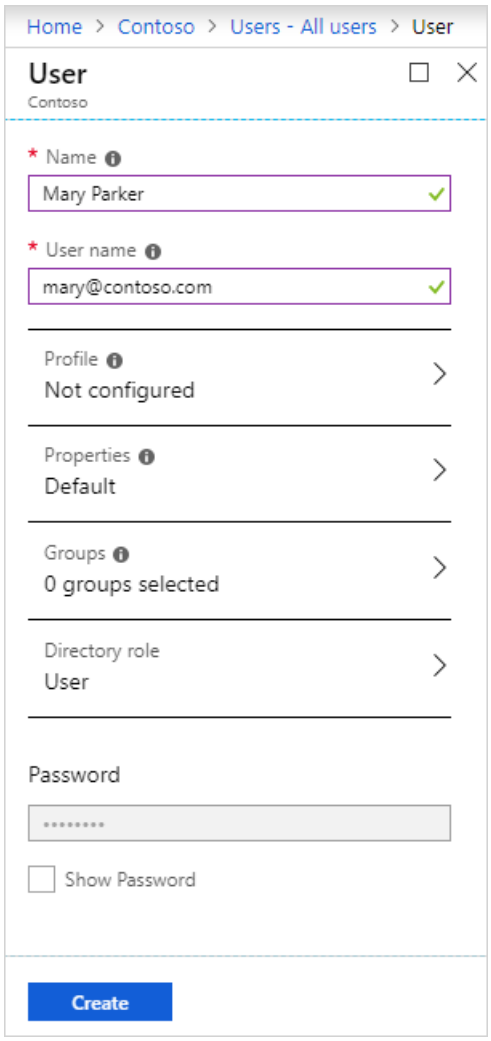
You can create a new user using the Azure Active Directory.

To add a new user

1. Sign in to the Azure portal as a Global administrator or user administrator for the directory.
2. Select **Azure Active Directory**, select **Users**, and then select **New user**.



3. On the **User** page, fill out the required information.



- **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 How to add a custom domain name to Azure Active Directory.
- **Profile.** Optionally, you can add more information about the user. You can also add user information at a later time. For more information about adding user info, see How to add or change user profile information.
- **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 How to create a basic group and add members.
- **Directory role.** Optionally, you can add the user to a directory role. You can assign the user to be a global administrator, or to one or more of the other administrator roles in Azure AD. For more information about assigning roles, see How to assign roles to users.

4. Copy the auto-generated password provided in the **Password** box. You'll need to give this password to the user for the initial sign-in process.
5. Select **Create**.

   The user is created and added to your Azure AD tenant.

Add a new user within a hybrid environment

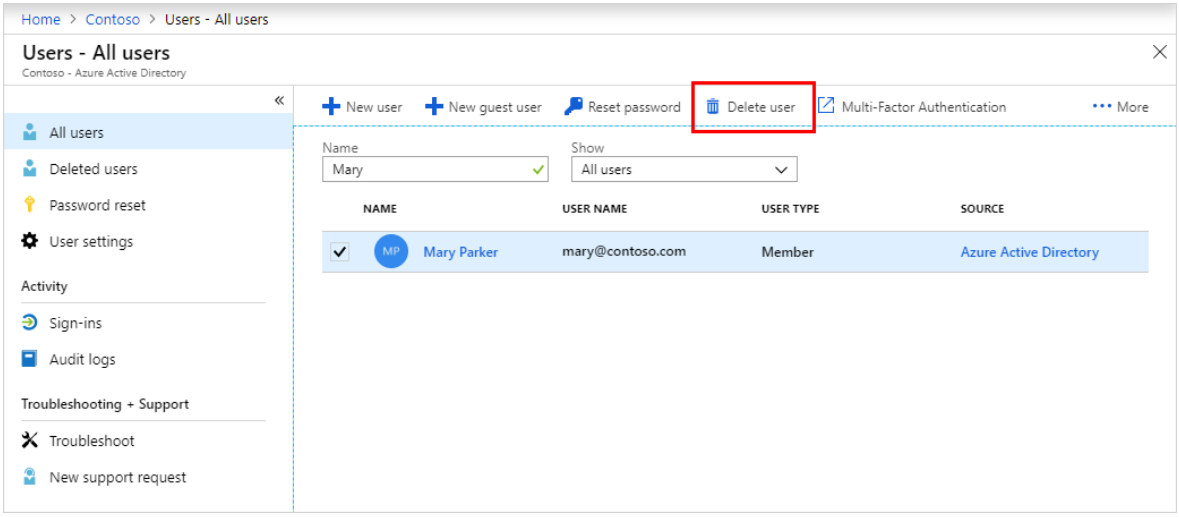
If you have an environment with both Azure Active Directory (cloud) and Windows Server Active Directory (on-premises), you can add new users by syncing the existing user account data. For more information about hybrid environments and users, see Integrate your on-premises directories with Azure Active Directory.

Delete a user

You can delete an existing user using Azure Active Directory.

To delete a user

1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, select **Users**, and then search for and select the user you want to delete from your Azure AD tenant. For example, *Mary Parker*.
3. 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 How to restore or permanently remove a recently deleted 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 added your users, you can perform 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 perform 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.

How to: Add or update a user's profile information using Azure Active Directory

9/17/2018 • 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.

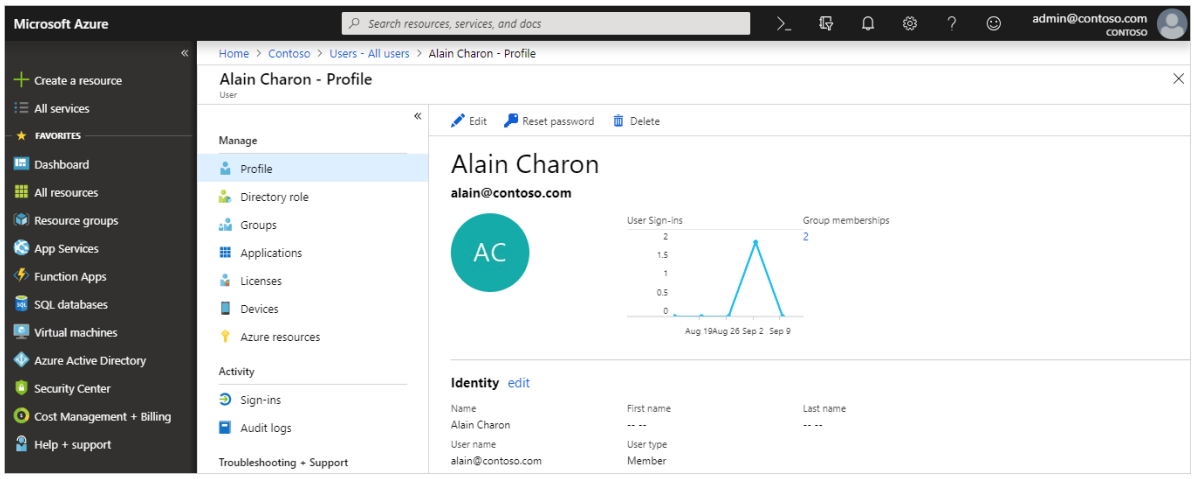
Add or change profile information

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.

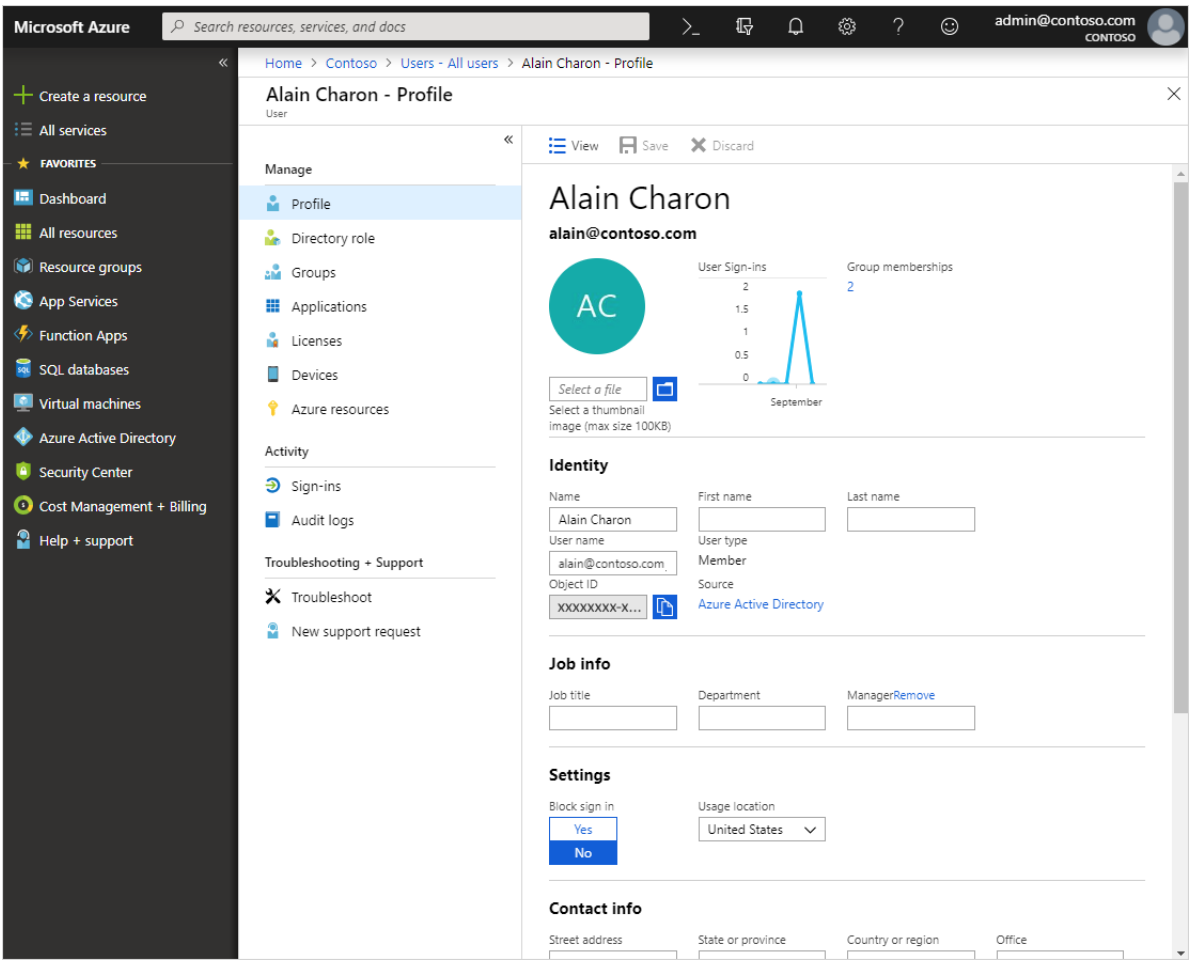
To add or change profile information

1. Sign in to the Azure portal as a Global administrator or user administrator for the directory.
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 any account-related information, such as a married last name or a changed user name.
- **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. For example, a street address or a mobile phone number.
- **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.

How to: Reset a user's password using Azure Active Directory

9/17/2018 • 2 minutes to read • Edit Online

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.

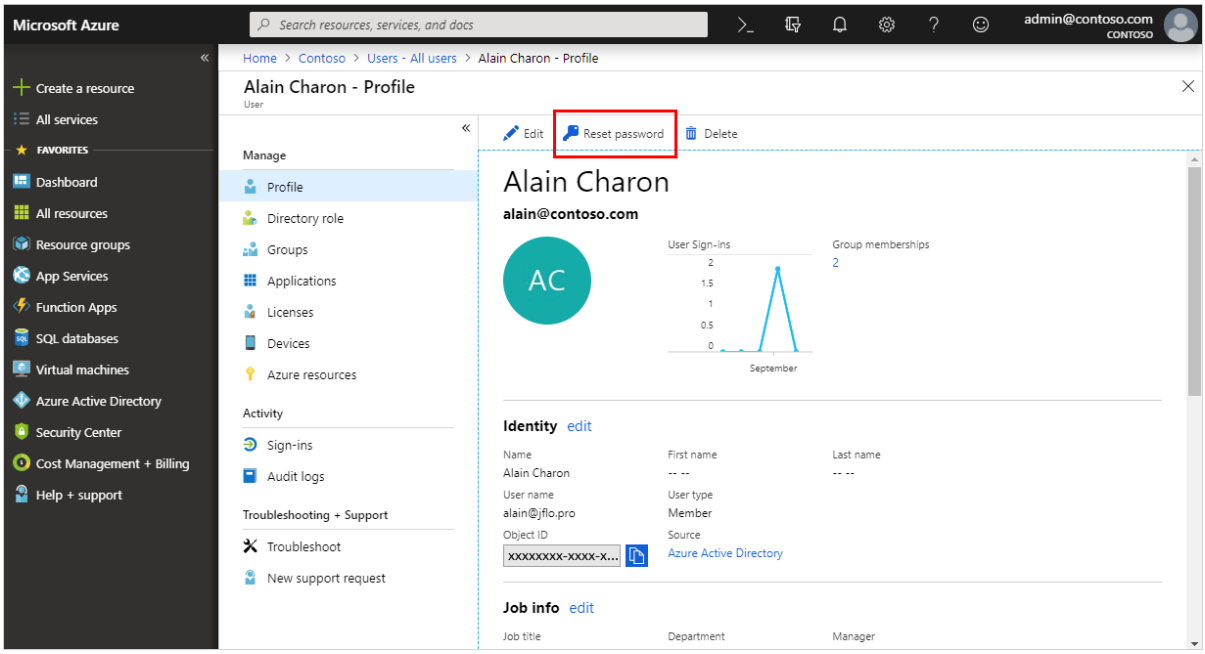
> **NOTE**
>
> Unless your Azure AD tenant is the home directory for a user, you won't be able reset their password. This means that if your user is signing in to your organization using an account from another organization, a Microsoft account, or a Google account, you won't be able to reset their password.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

To reset a password

1. Sign in to the Azure portal as a global administrator, 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**.

   A temporary password is auto-generated 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.

How to: Assign roles and administrators to users with Azure Active Directory

9/17/2018 • 2 minutes to read • Edit Online

If a user in your organization needs permission to manage Azure Active Directory (Azure AD) resources, you must assign the user an appropriate role in Azure AD, based on the actions the user needs permission to perform.

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

Assign roles

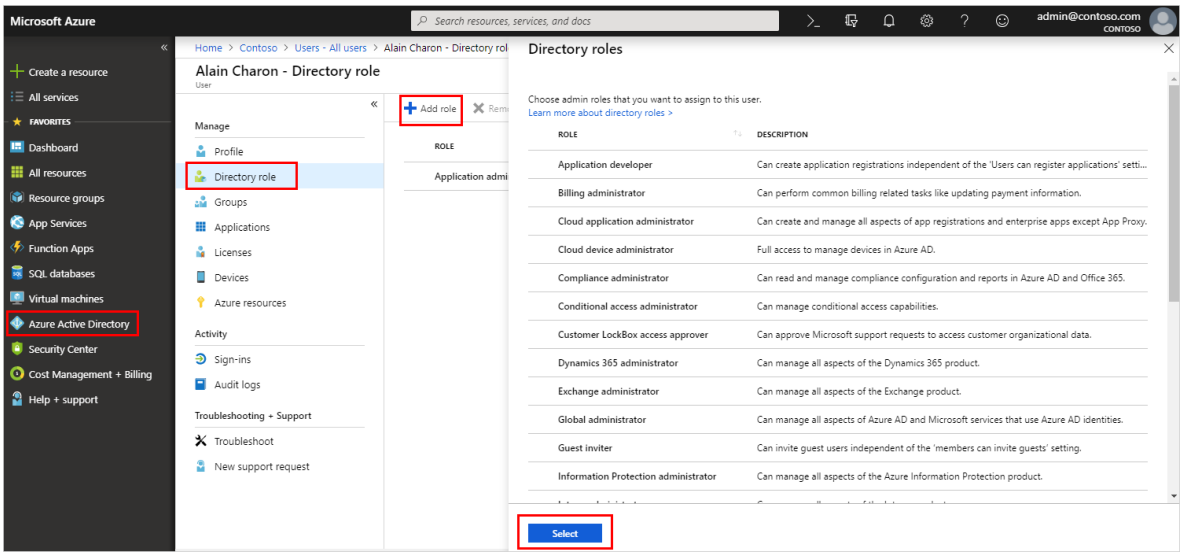
A common way to assign Azure AD roles to a user is on the **Directory role** page for a user.

You can also assign roles using Privileged Identity Management (PIM). For more detailed information about how to use PIM, see Privileged Identity Management.

To assign a role to a user

1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select **Azure Active Directory**, select **Users**, and then search for and select the user getting the role assignment. For example, *Alain Charon*.
3. On the **Alain Charon - Profile** page, select **Directory role**.

   The **Alain Charon - Directory role** page appears.
4. Select **Add role**, 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 - Directory role** page.

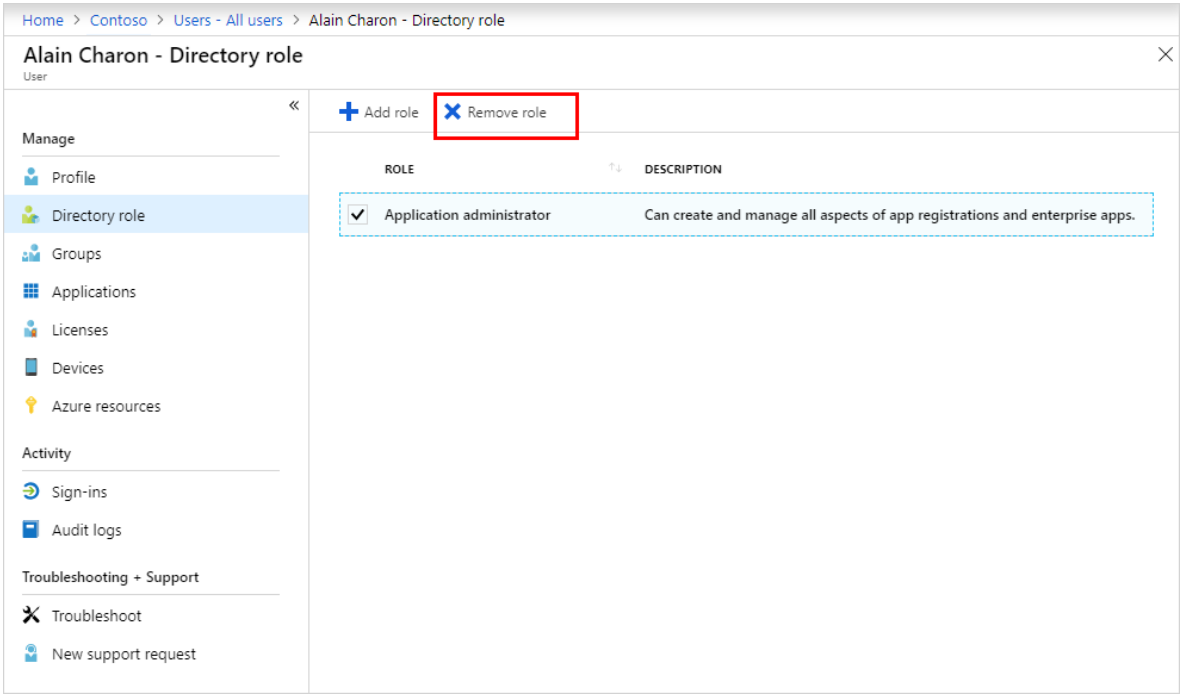
Remove a role assignment

If you need to remove the role assignment from a user, you can also do that from the **Alain Charon - Directory**

role 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 **Directory role**, select **Application administrator**, and then select **Remove role**.



The Application administrator role is removed from Alain Charon and it no longer appears on the **Alain Charon - Directory role** page.

Next steps

- Add or delete users
- Add or change profile information
- Add guest users from another directory

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.

How to: Assign or remove Azure Active Directory licenses

9/14/2018 • 4 minutes to read • Edit Online

Many Azure Active Directory (Azure AD) services require you to activate an Azure AD product and to license each of your users or groups (and associated members) for that product. Only users with active licenses will be able to access and use the licensed Azure AD services.

Available product editions

There are several editions available for the Azure AD product.

- Azure AD Free
- Azure AD Basic
- Azure AD Premium 1 (Azure AD P1)
- Azure AD Premium 2 (Azure AD P2)

For specific information about each product edition and the associated licensing details, see What license do I need?.

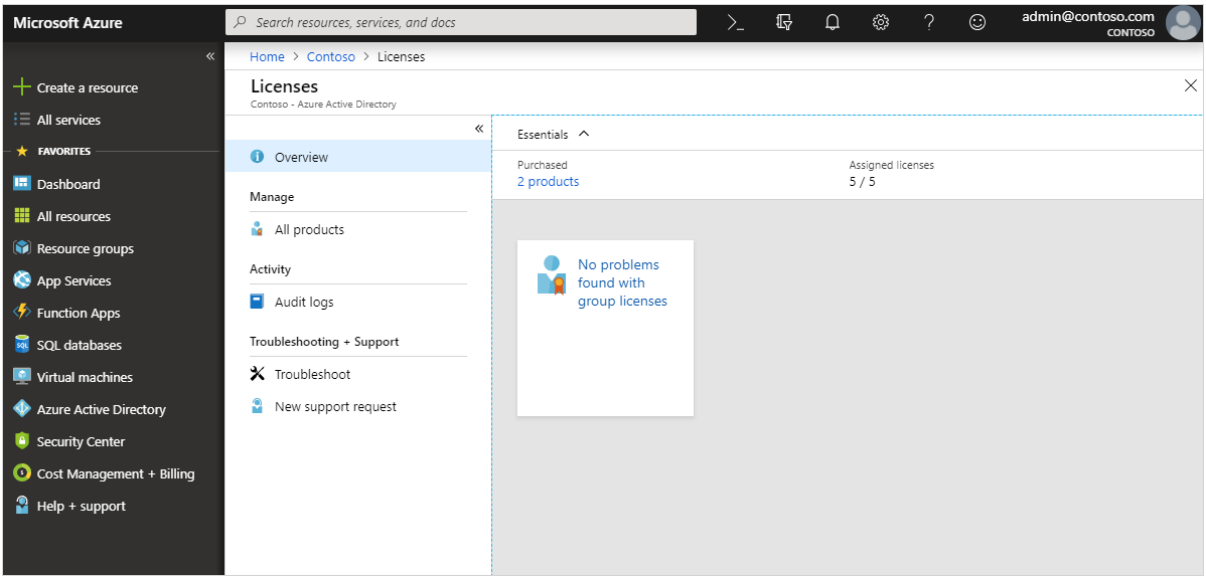
View your product edition and license details

You can view your available products, including the individual licenses, checking for any pending expiration dates and the number of assignments available.

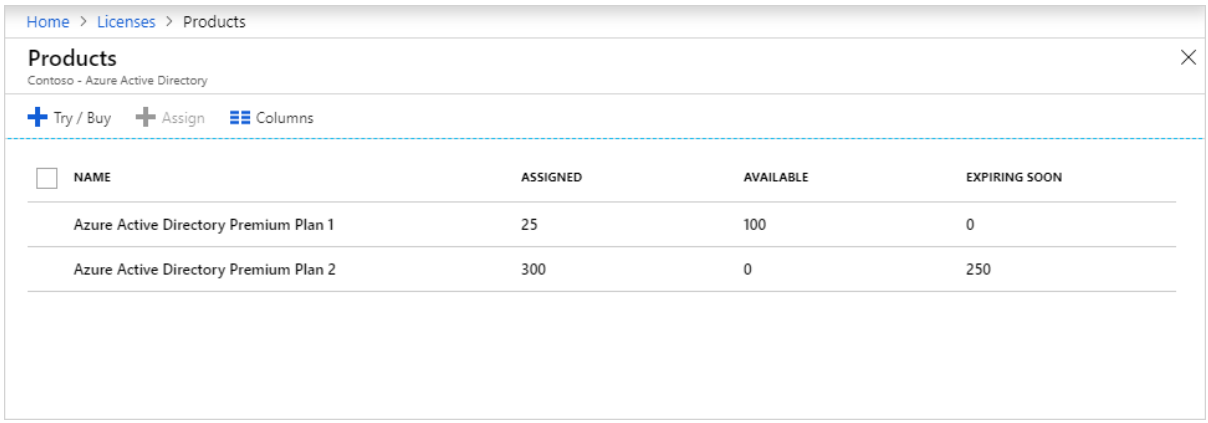
To find your product and license details

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

   The **Licenses** page appears.



3. Select the **Purchased products** link to view the **Products** page and to see the **Assigned**, **Available**, and **Expiring soon** details for each specific product edition.



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

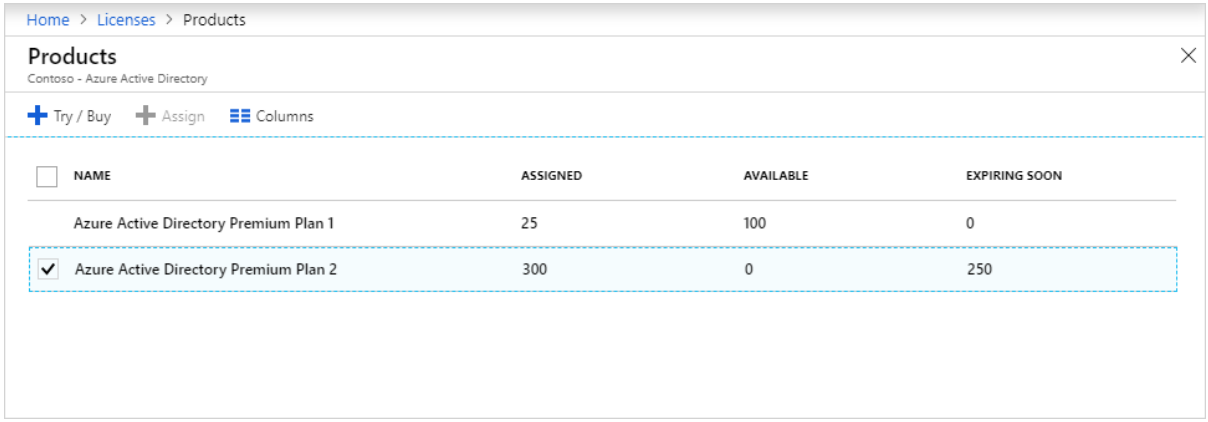
Assign licenses to users or groups

Make sure that anyone needing to use a licensed Azure AD service has the appropriate license. It's up to you whether you want to add the licensing rights to individual users or to an entire group.

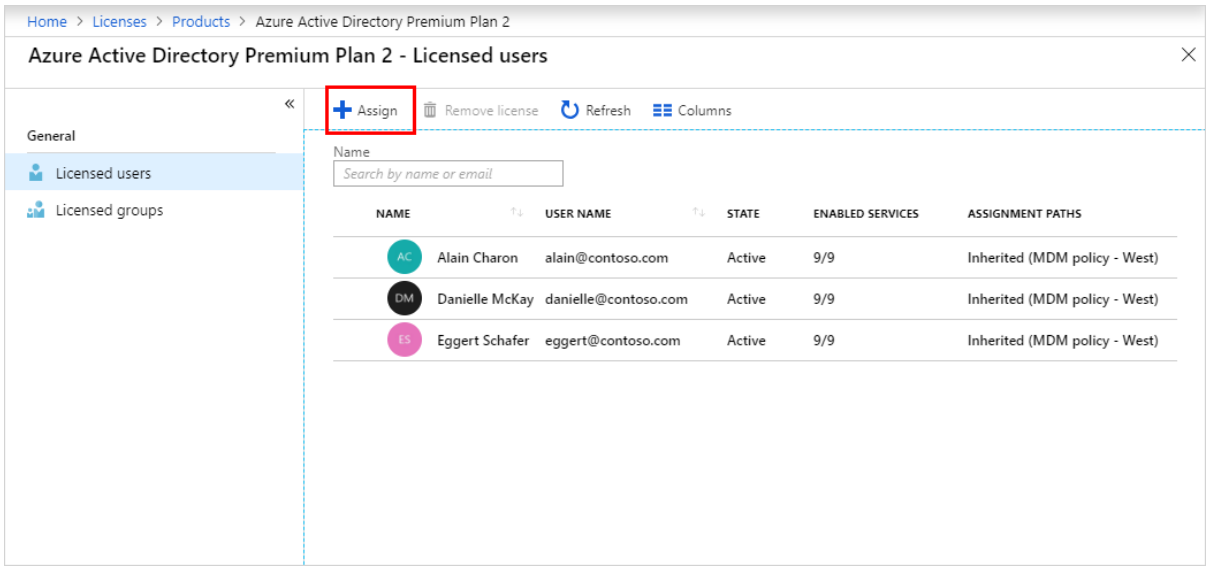
> ![Note] Group-based licensing is a public preview feature of Azure AD and is available with any paid Azure AD license plan. For more information about previews, see Supplemental Terms of Use for Microsoft Azure Previews.
>
> For detailed information about how to add users, see How to add or delete users in Azure Active Directory. For detailed information about how to create groups and add members, see Create a basic group and add members.

To assign a license to a specific user

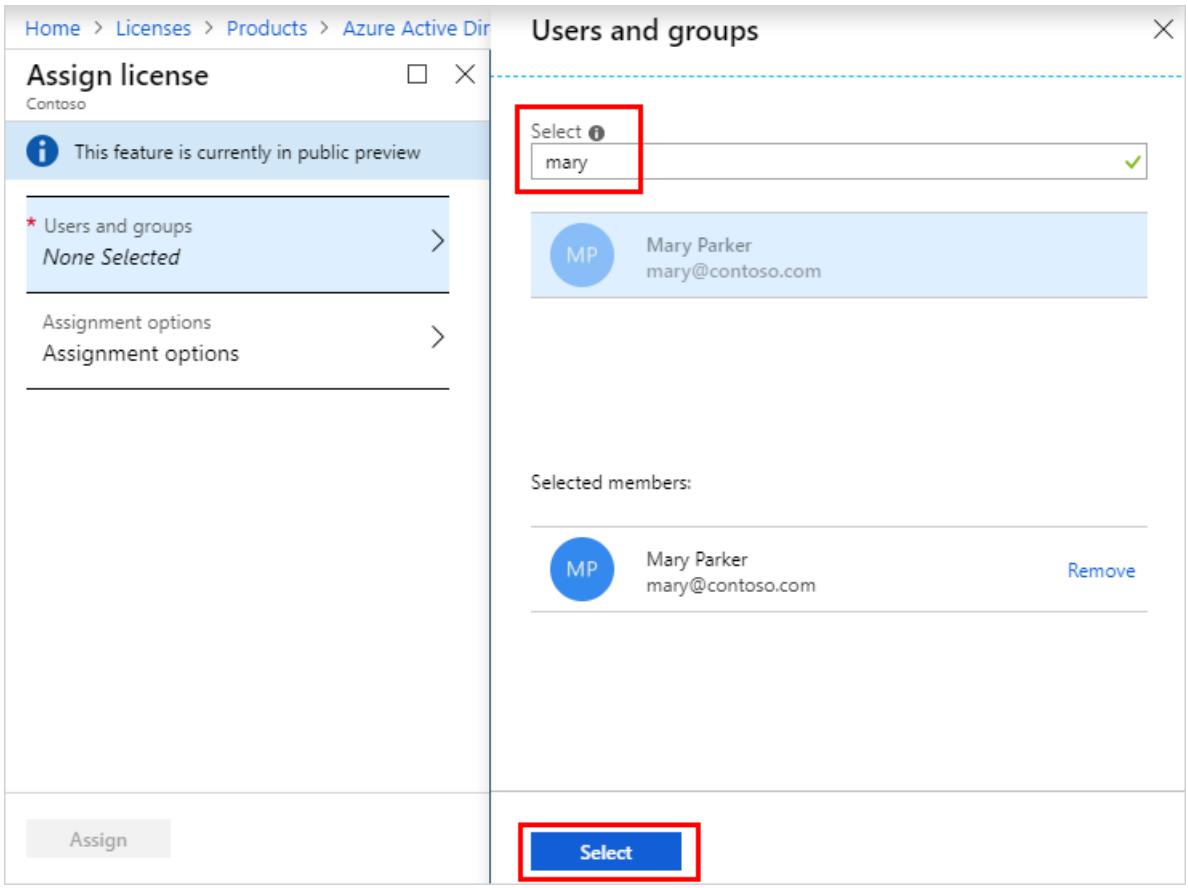
1. On the **Products** page, select the name of the edition you want to assign to the user. For example, *Azure Active Directory Premium Plan 2*.



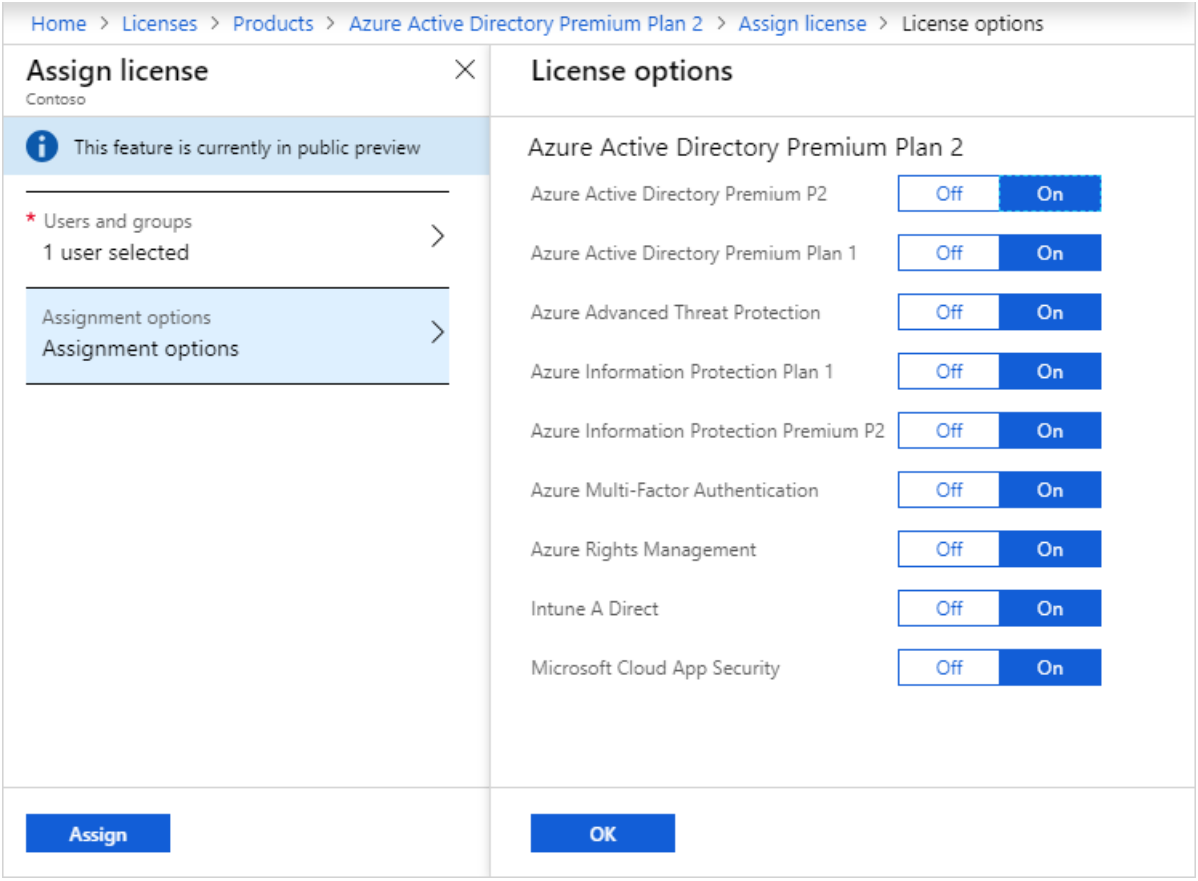
2. On the **Azure Active Directory Premium Plan 2** page, select **Assign**.



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



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.

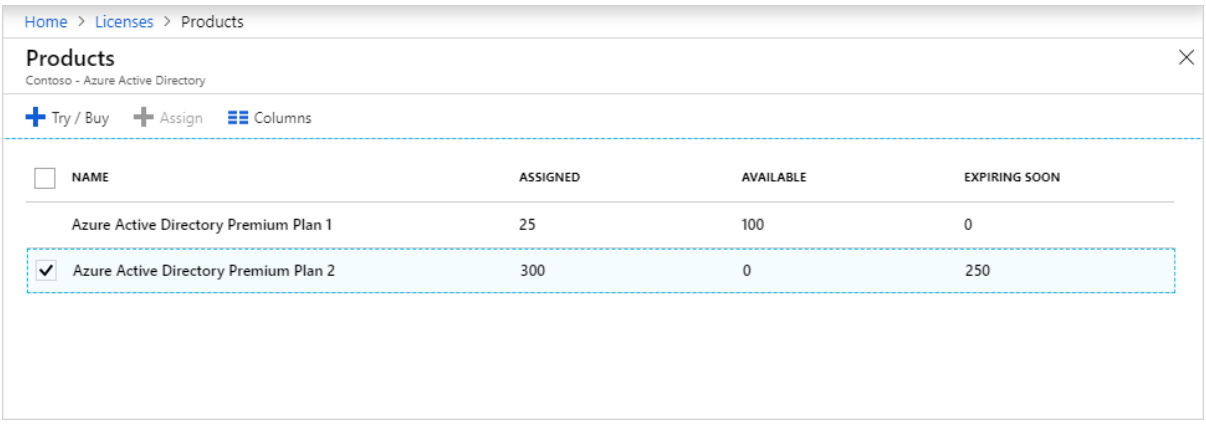
> **NOTE**
>
> Not all Microsoft services are available in all locations. Before a license can be assigned to a user, you must specify the **Usage location**. You can set this value in the **Azure Active Directory > Users > Profile > Settings** area in Azure AD.

5. Select **Assign**.

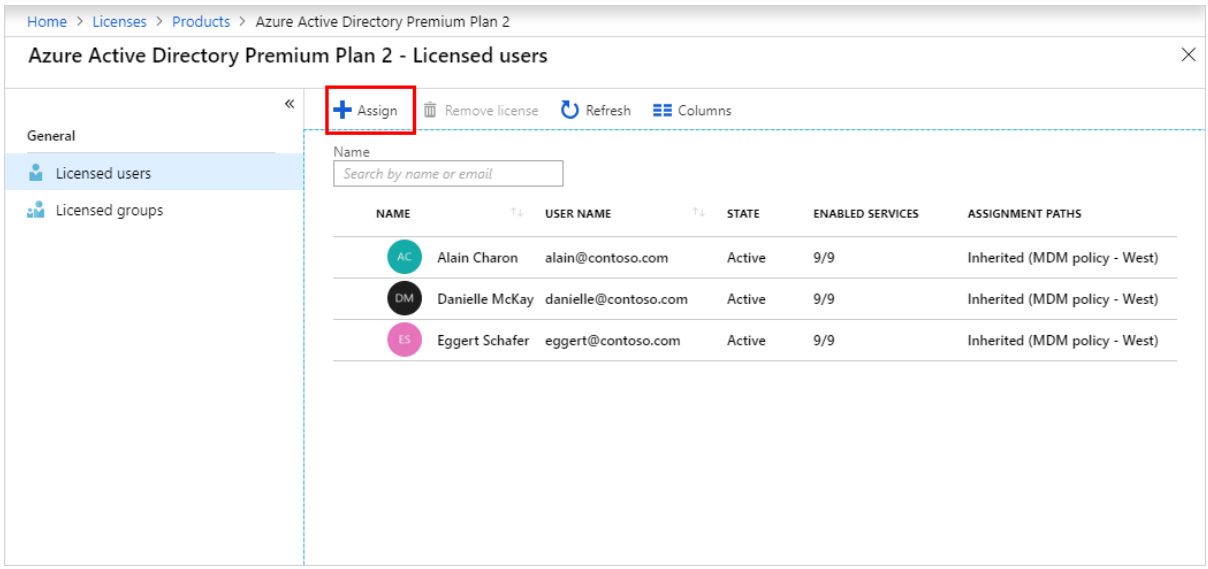
   The user is added to the list of licensed users and has access to the included Azure AD services.

To assign a license to an entire group

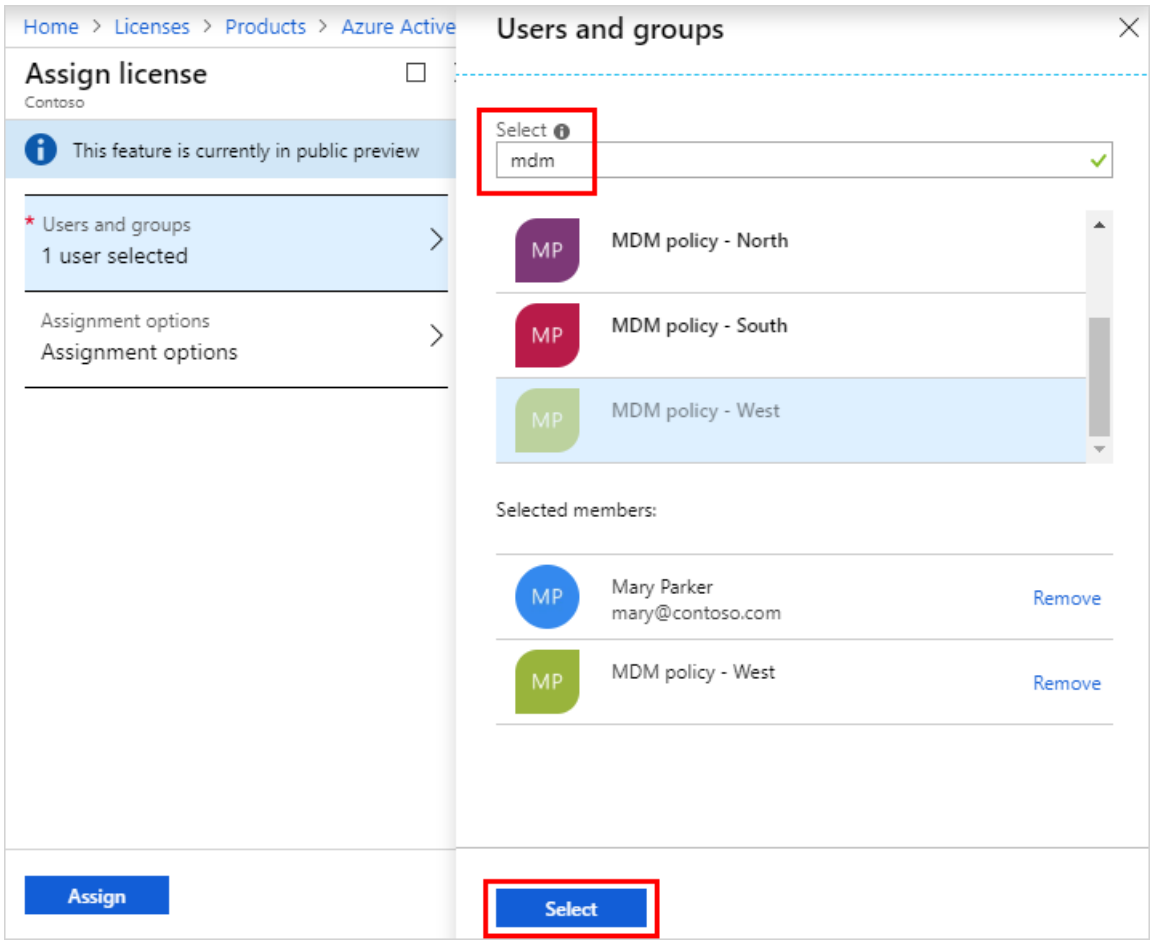
1. On the **Products** page, select the name of the edition you want to assign to the user. For example, *Azure Active Directory Premium Plan 2*.



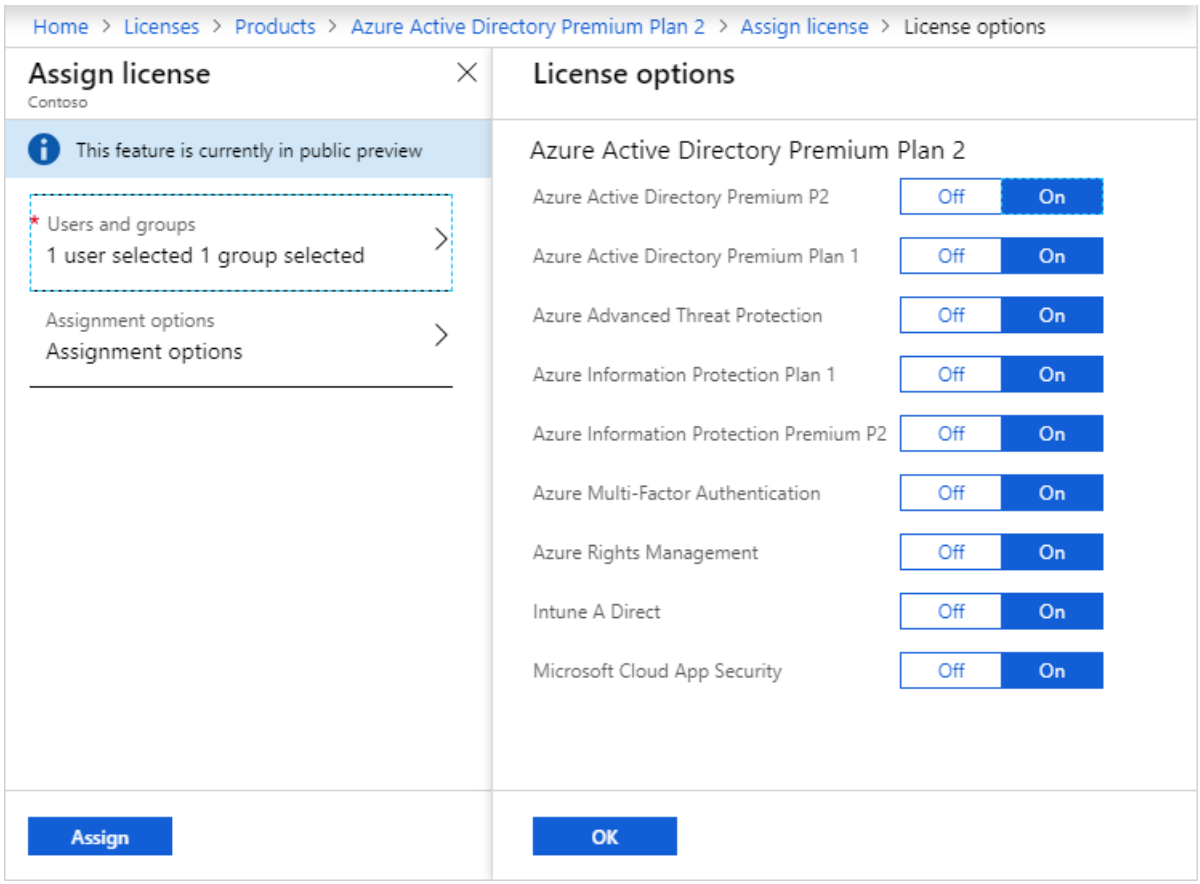
2. On the **Azure Active Directory Premium Plan 2** page, select **Assign**.



3. On the **Assign** page, select **Users and groups**, and then search for and select the group you're assigning the license. For example, *MDM policy - West*.



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 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 tenant.

5. Select **Assign**.

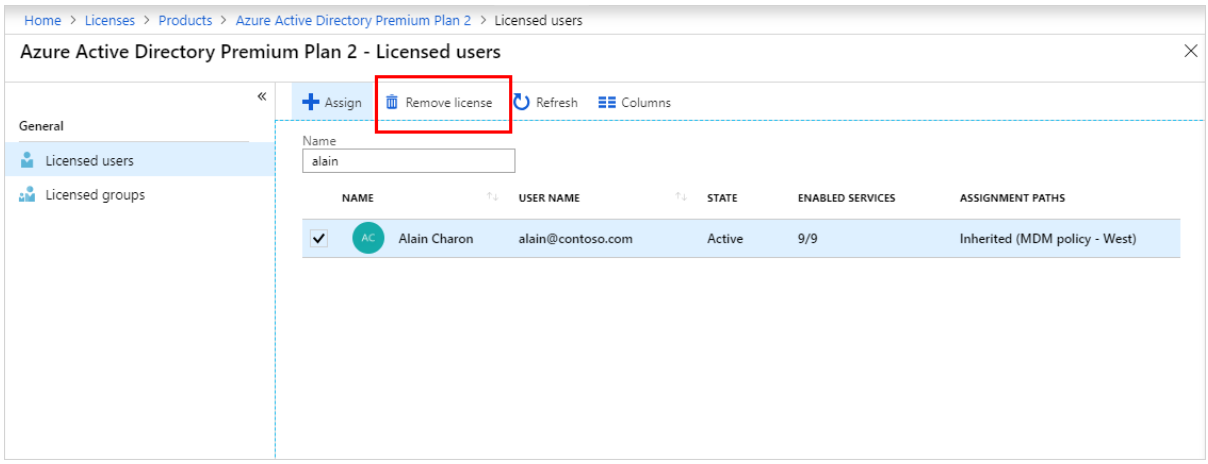
   The group is added to the list of licensed groups and all of the members have access to the included Azure AD services.

Remove a license

You can remove a license from either a user or a group from the **Licenses** page.

To remove a license from a specific user

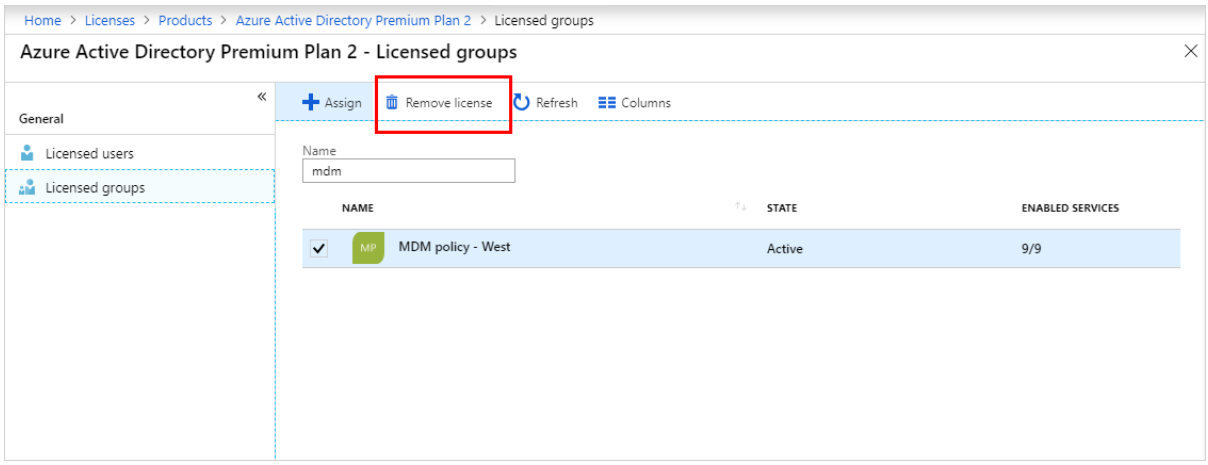
1. On the **Licensed users** page for the product edition, select the user that should no longer have the license. For example, *Alain Charon*.
2. Select **Remove license**.



To remove a license from a group

1. On the **Licensed groups** page for the product edition, select the group that should no longer have the license. For example, *MDM policy - West*.

2. Select **Remove license**.



> **IMPORTANT**
>
> Licenses inherited by a user 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.

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

How to: Restore or permanently remove a recently deleted user with Azure Active Directory

9/17/2018 • 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.

- Company Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- User Account Administrator

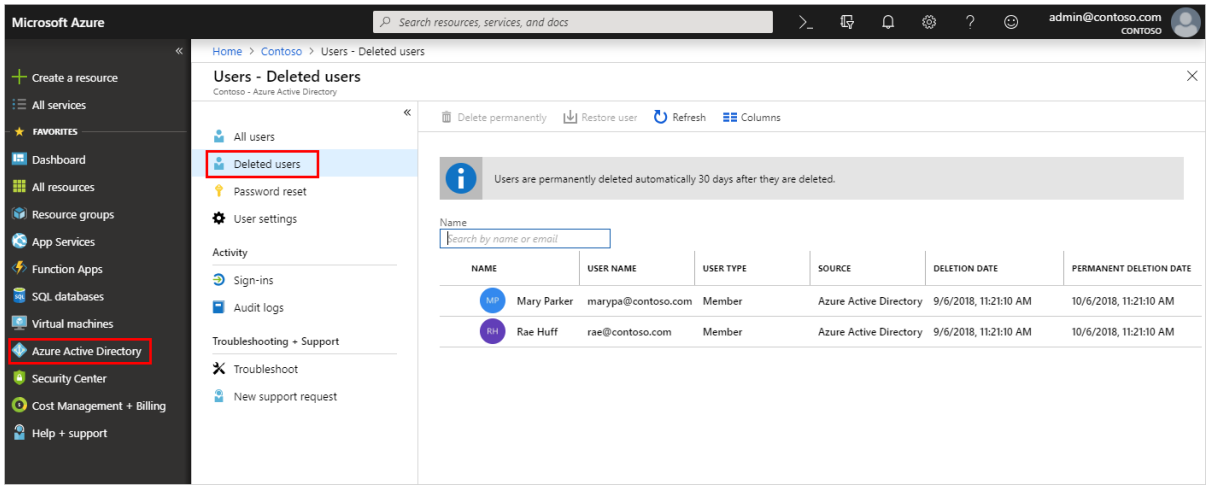
View your restorable users

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 directory.
2. Select **Azure Active Directory**, select **Users**, and then select **Deleted users**.

   Review the list of users that are available to restore.

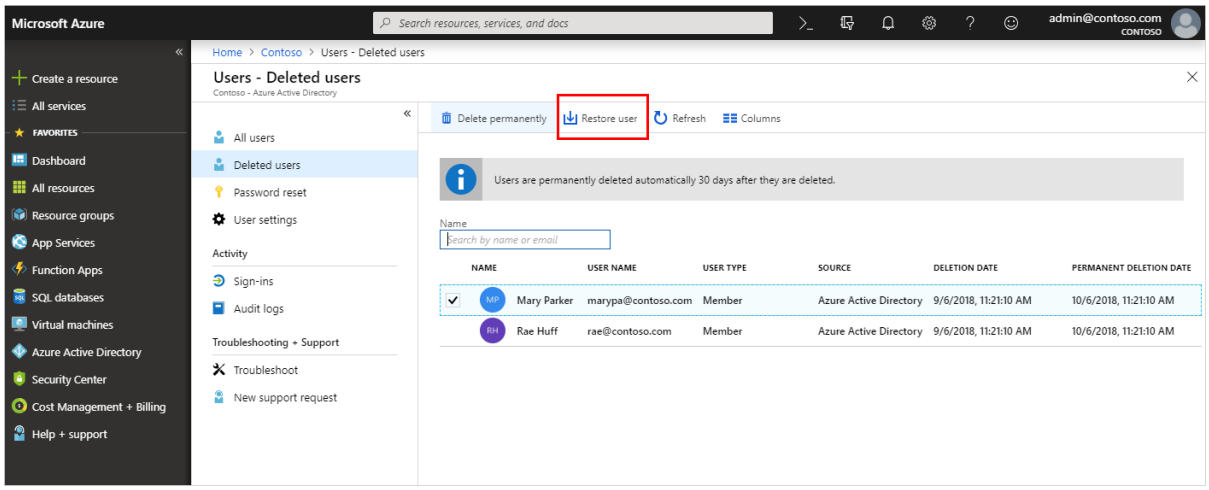


Restore a recently deleted user

While a user's account is suspended, all the related directory information is preserved. When you restore a user, this directory information is also restored.

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**.



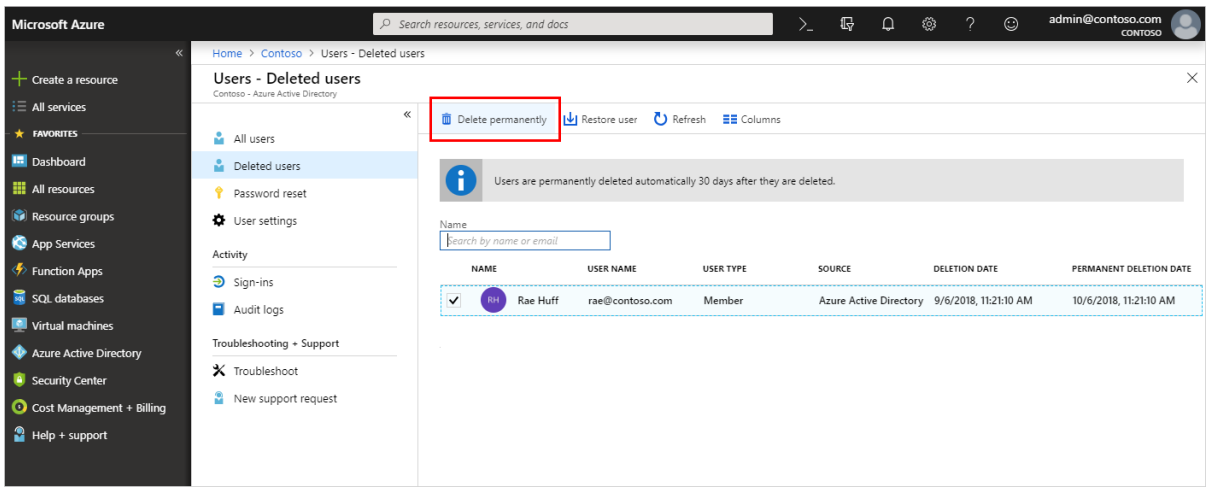
Permanently delete a user

You can permanently delete a user from your directory 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 directory

For more information about other available user management tasks, Azure Active Directory user management documentation.

How to: Get support for Azure Active Directory

9/17/2018 • 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 Tech Community is the place for our IT pro partners and customers to collaborate, share, and learn. The Microsoft Tech 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.

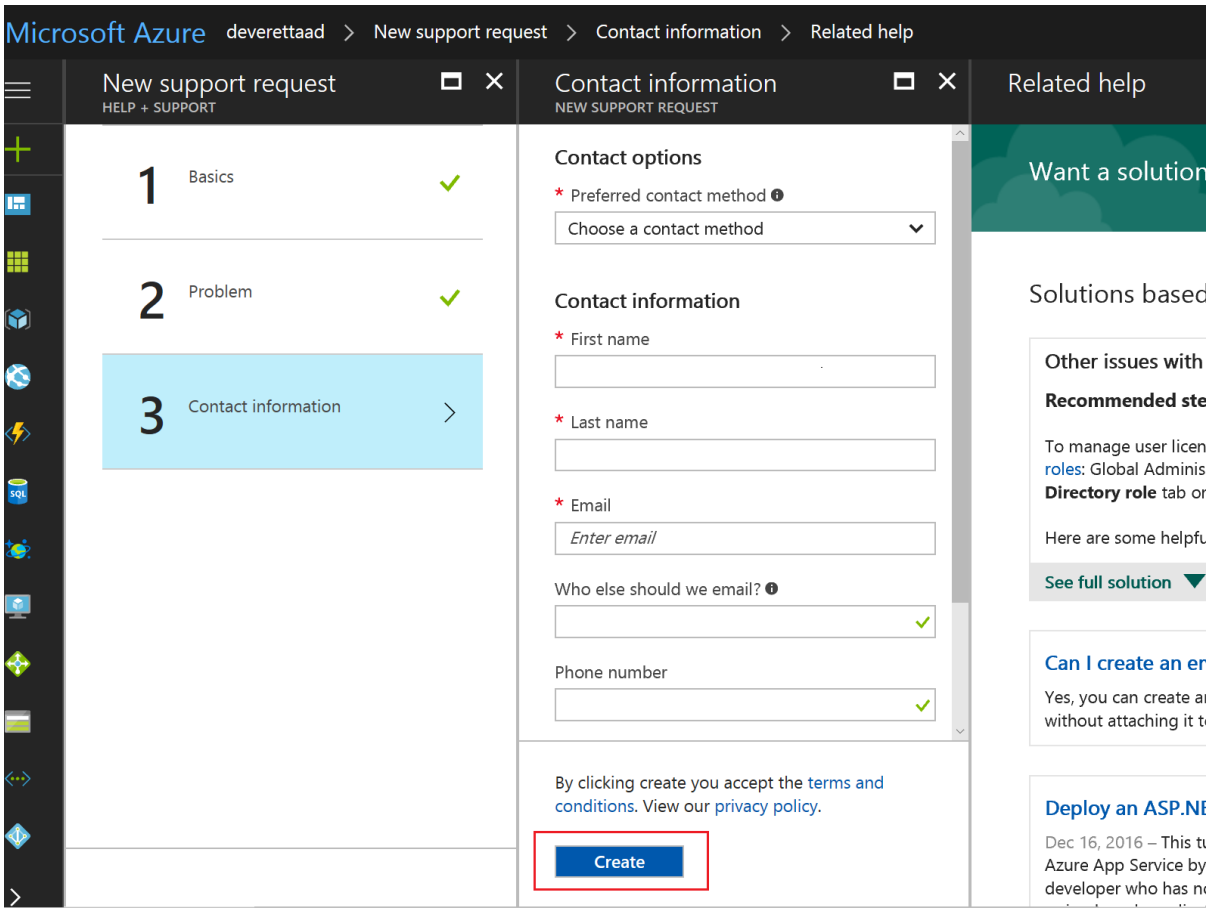
Open a support ticket

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 Office 365 admin center.

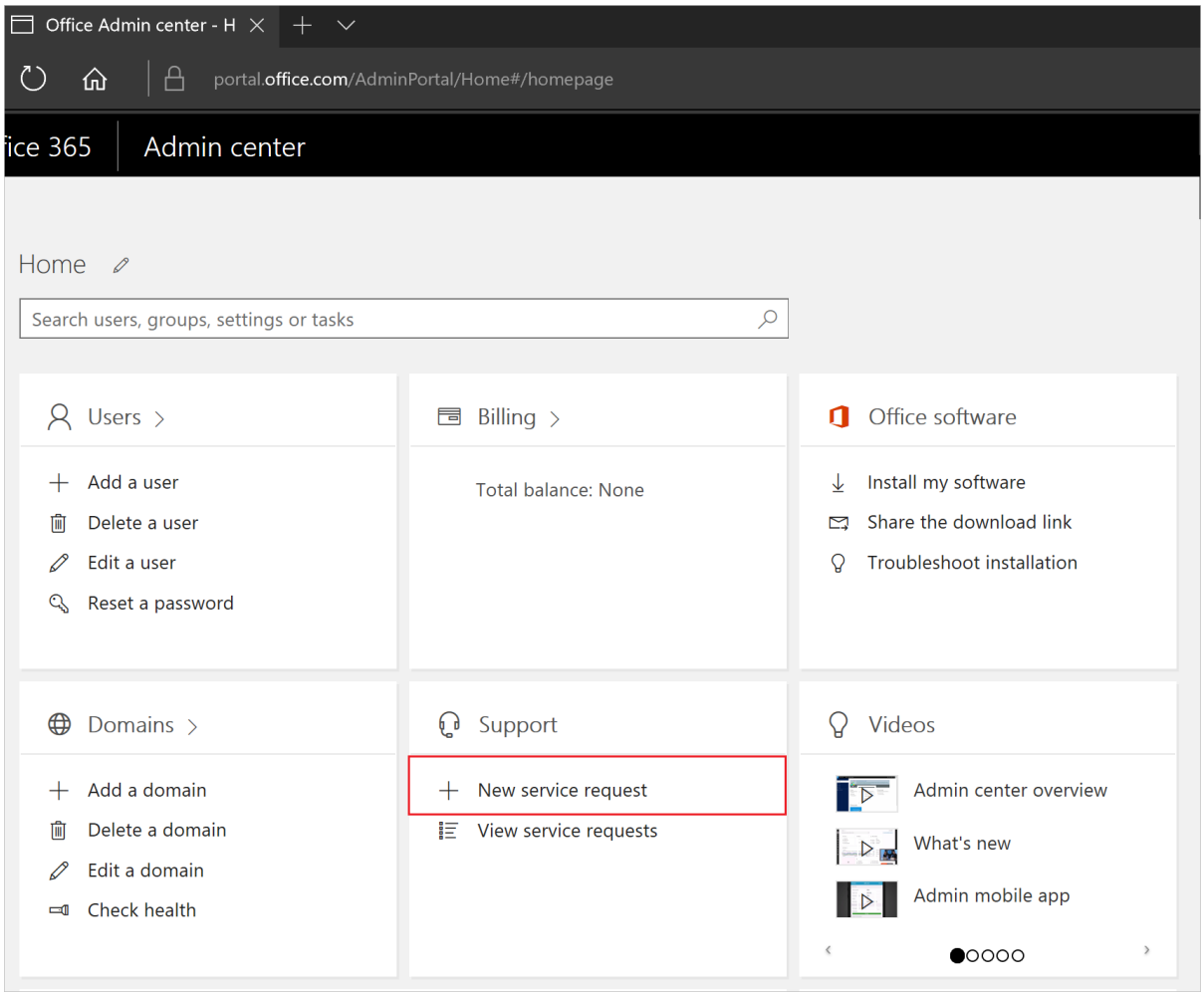
1. Sign in to the Azure portal and open **Azure Active Directory**.
2. Scroll down to **Troubleshooting + Support** and select **New support request**.
3. On the **Basics** blade, for **Issue type**, select **Technical**.
4. For **Service**, select **Azure Active Directory**, and then select **Next**.
5. On the **Problem** blade, select a Severity).
6. 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.
7. Add the rest of your problem information and click **Next**.
8. Provide your contact information and select **Create**.



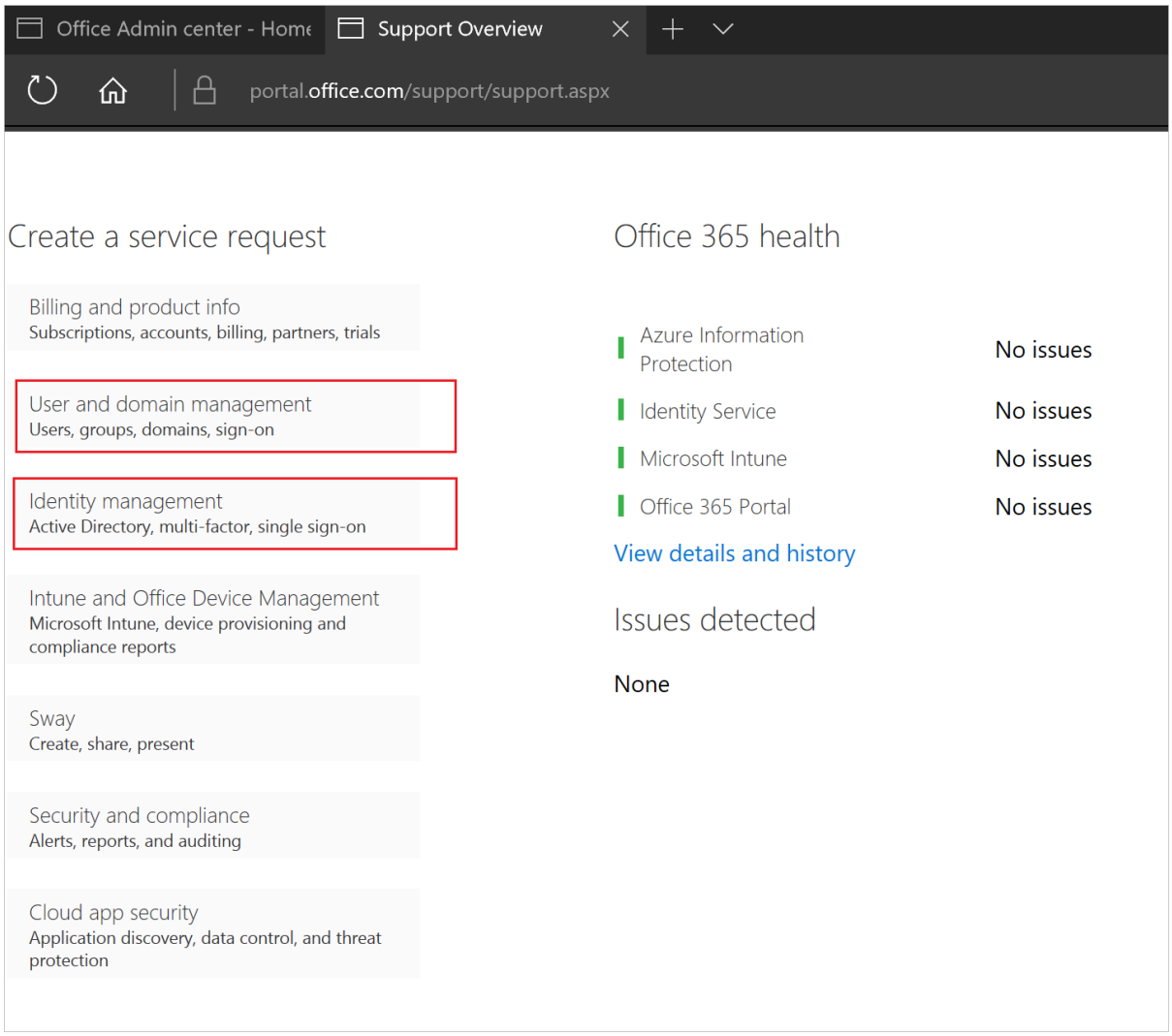
How to open a support ticket for Azure AD in the Office 365 portal

> **NOTE**
> Support for Azure AD in the Office 365 admin center is offered for administrators only.

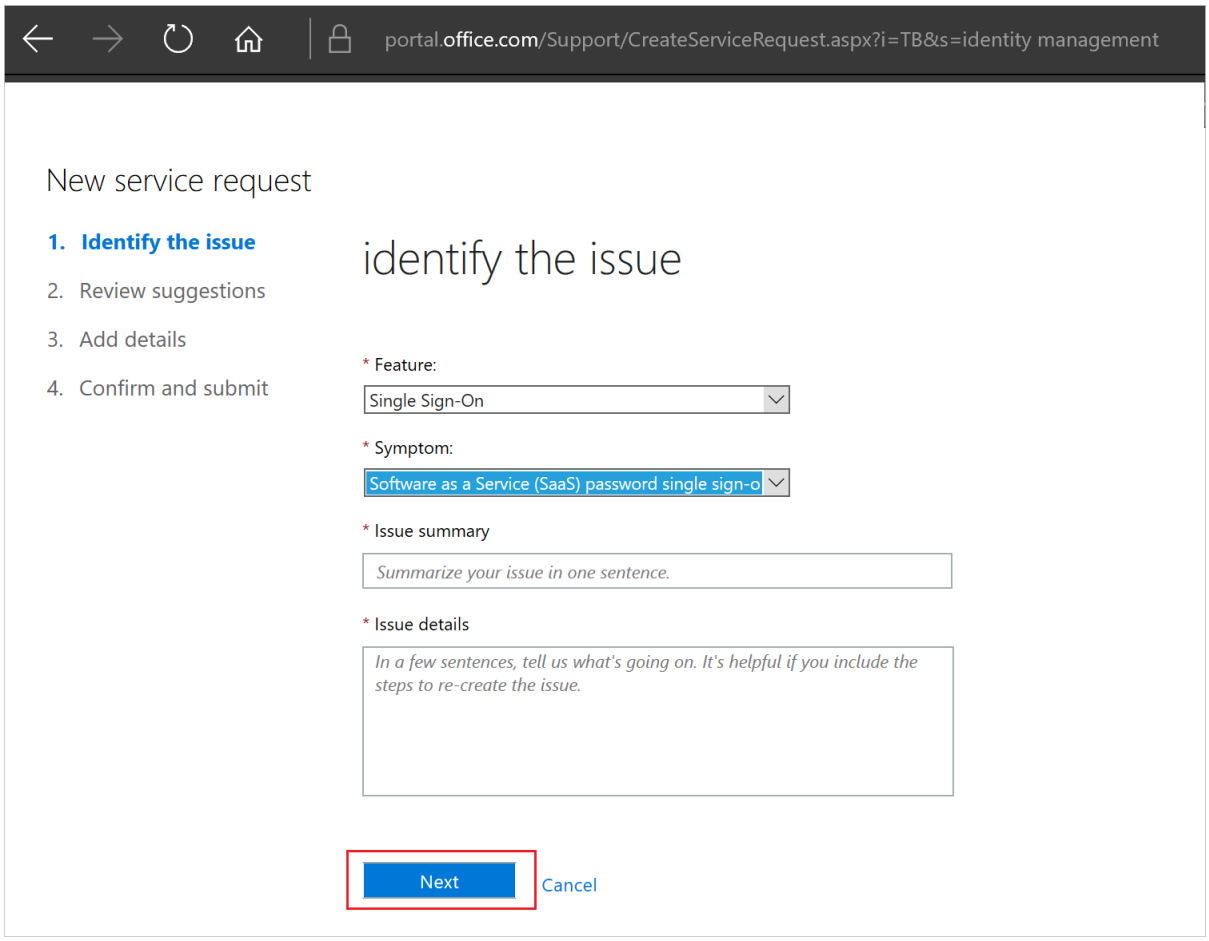
1. Sign in to the Office 365 admin center with an account that has an Enterprise Mobility + Security (EMS) license.
2. On the **Support** tile, select **New service request**:



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

Azure Active Directory FAQ

11/13/2018 • 8 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 have a paid Office 365 or Azure AD subscription, go to https://aka.ms/accessAAD for a one-time activation step. Otherwise, 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 LDAP protocol. However, you can configure secure LDAP with Azure AD Domain Services.

Azure Active Directory deployment plans

9/28/2018 • 3 minutes to read • Edit Online

Looking for end-to-end guidance about how to deploy some of Azure Active Directory (Azure AD) capabilities? The following deployment plans walk through the business value, planning considerations, design, and operational procedures needed to successfully roll a few of the more common Azure AD capabilities.

Within the documents you will find e-mail templates, system architecture diagrams, common test cases, and more.

We'd love your feedback on the documents. Take this short survey about how the documents worked for you.

SCENARIO	DESCRIPTION
Single sign-on	Single sign-on helps you access all the apps and resources you need to do business, while signing in only once, using a single user account. After you've signed in, you can go from Microsoft Office to SalesForce, to Box without being required to authenticate (for example, type a password) a second time.
Workday-driven Inbound User Provisioning	Workday-driven Inbound 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, 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, Delete accounts).
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, such as the ability to request access to new apps and groups, or manage access to these resources on behalf of others.
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.
Multi-Factor Authentication	Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution. Using admin-approved authentication methods, Azure MFA helps safeguard your access to 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.

SCENARIO	DESCRIPTION
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 your users a better experience - one less password to remember, and reduces IT helpdesk costs because your 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.
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 to authenticate users with no interaction with the on-premises Active Directory
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. After you turn on this feature, users won't need to type in their passwords to sign in to Azure AD, and usually, won't even need to type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.
Self-service password reset	Self-service password reset helps your users reset their password, without administrator intervention, when and where they need to.
Azure AD Application Proxy	Employees today want to be productive at any place, at any time, and from any device. They want to work on their own devices, whether they are tablets, phones, or laptops. And employees expect to be able to access all their applications, both SaaS apps in the cloud and corporate apps on-premises. Providing access to on-premises applications has traditionally involved virtual private networks (VPNs) or demilitarized zones (DMZs). Not only are these solutions complex and hard to make secure, but they are costly to set up and manage. There is a better way! - Azure AD Application Proxy

Archive for What's new? in Azure Active Directory

11/15/2018 • 35 minutes to read • Edit Online

The primary What's new release notes article contains the latest 6 months of information, while this article includes all the older information.

The What's new release notes provide you with information about:

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

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 Changing dynamic membership to static and vice-versa

---

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 our Graph APIs.

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 event 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 event Sign-in with additional risk detected.

For more information, see Azure Active Directory risk events.

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 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 events 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 events

Type: Changed feature
Service category: Identity protection
Product capability: Identity security and protection

In Azure AD Identity Protection, all real-time risk events that originated from the same IP address on a given day are now aggregated for each risk event type. This change limits the volume of risk events 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 Events 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.
