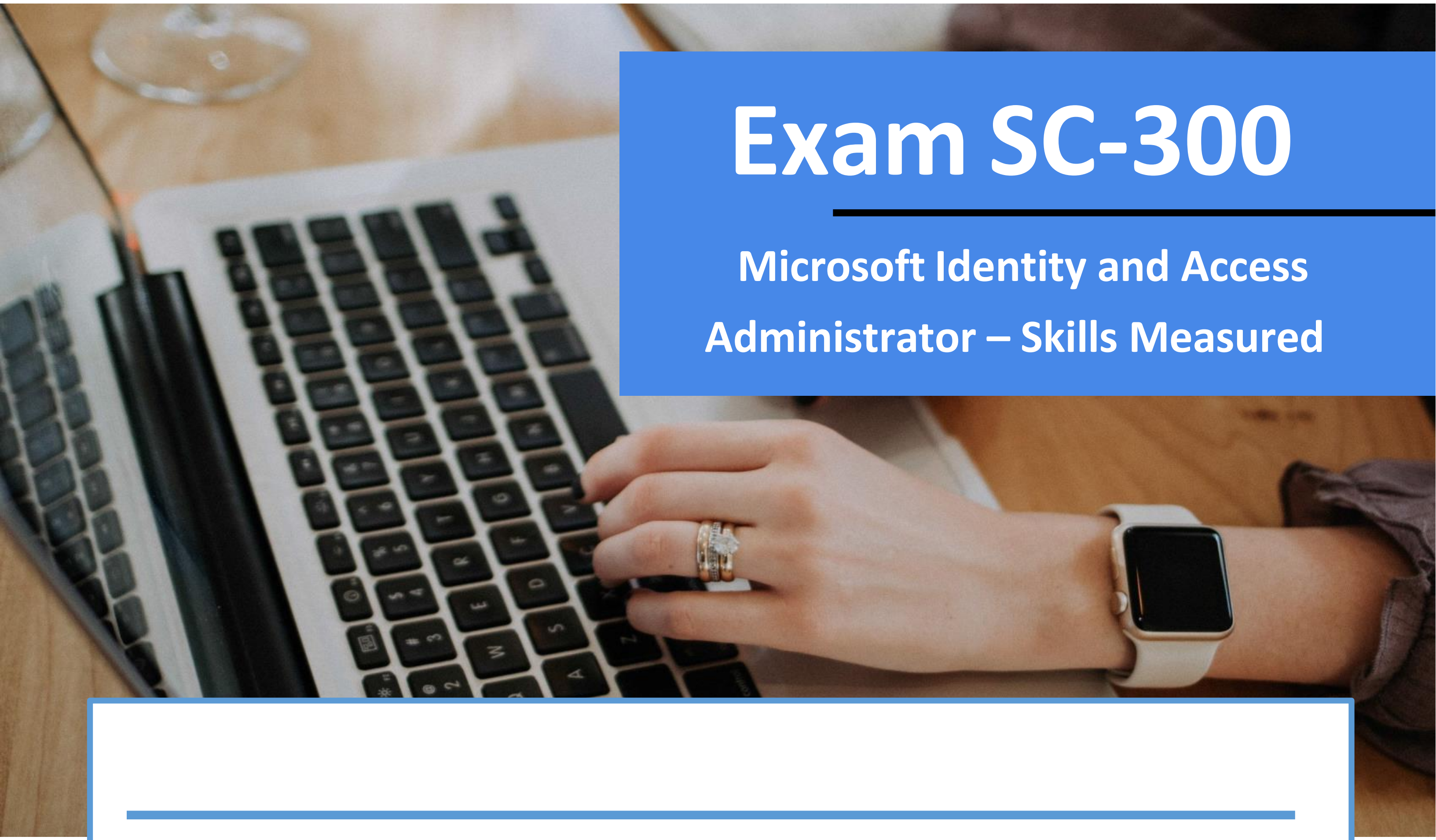
THE QUILL CONSULTANCY



Exam SC-300

Microsoft Identity and Access Administrator – Skills Measured

Address

Level 1, 42 Murray Street, Hobart,
Tasmania 7000 Australia

Phone

03 6234 3883

Email

quill@quill.com.au

Web

www.quill.com.au

Audience Profile

The Microsoft identity and access administrator designs, implements, and operates an organization's identity and access management systems by using Azure Active Directory (Azure AD). They manage tasks such as providing secure authentication and authorization access to enterprise applications. The administrator provides seamless experiences and self-service management capabilities for all users. Adaptive access and governance are core elements to the role. This role is also responsible for troubleshooting, monitoring, and reporting for the identity and access environment.

The identity and access administrator may be a single individual or a member of a larger team. This role collaborates with many other roles in the organization to drive strategic identity projects to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Contents

Audience Profile 2

How to use this guide 5

In the exam 5

Key Learning Objectives 6

Implement an Identity Management Solution (25-30%) 6

Implement initial configuration of Azure Active Directory 6

Create, configure, and manage identities 15

Implement and manage external identities 19

Implement and manage hybrid Identity 24

Implement an authentication and access management solution (25-30%) 33

Plan and implement Azure Multifactor Authentication 33

Manage user authentication 36

Plan, implement, and administer conditional access 41

Manage Azure AD Identity Protection 46

Contents

Implement Access Management for Apps (10-15%) 49

Plan, implement, and monitor the integration of

Enterprise Apps for Single Sign-On (SSO) 49

Implement app registrations 57

Plan and implement an Identity Governance Strategy (25-30%) 64

Plan and implement entitlement management 64

Plan, implement, and manage access reviews 68

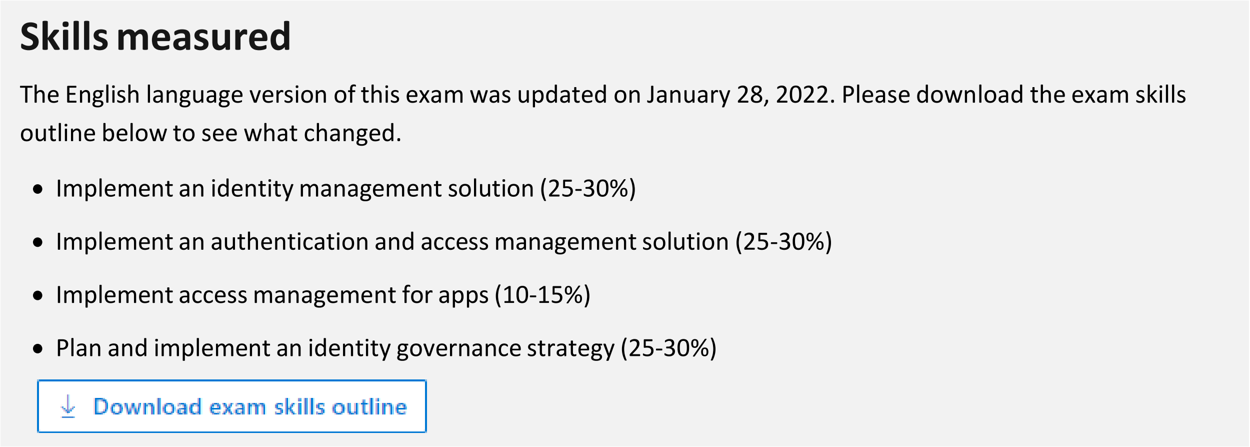
Plan and implement privileged access 75

Monitor and maintain Azure Active Directory 85

How to use this guide

This guide is here to help you prepare and take the exam. It is designed to complement your existing learning and to help guide you in the areas of focus for the exam. You should use this as a framework to help fill in the blanks on information that you have.

We have developed the following content in direct alignment to the current Learning objectives. These can be viewed directly, by selecting the "Download exam skills outline" from the exam page at: https://docs.microsoft.com/en-us/learn/certifications/exams/sc-300



Skills measured

The English language version of this exam was updated on January 28, 2022. Please download the exam skills outline below to see what changed.

- Implement an identity management solution (25-30%)
- Implement an authentication and access management solution (25-30%)
- Implement access management for apps (10-15%)
- Plan and implement an identity governance strategy (25-30%)

There are loads of exciting and interesting topics we can begin to follow on from these core objectives, but remember for the exam we do need to stay focused and constrain ourselves to these key topics.

In the exam

The exam itself is quite straight forward with no complicated case studies or longwinded questions. The majority of the questions will be "Multiple Choice" or "Choose all that apply" type of questions. You may also come across some "Drag and Drop" questions where you need to place answers in order. The key thing to note is that all of the questions will have the answer in front of you.

Remembering that all of the answers are presented to you, you need to make sure that you answer each question. There is no loss of marks for incorrect answers, so even if you don't know the answer, you should attempt it.

The exam itself will have between 40 and 50 questions, depending on the pool of questions that have been allocated. You will have 60 minutes to complete the exam. As you can see you will need to move at a steady pace throughout. Don't get too stuck on any question, instead select your answer and then mark the question for "Review". Then if you have time at the end of the exam you can go back and review these questions.

Key Learning Objectives

Implement an Identity Management Solution (25-30%)

Learn to create and manage your initial Azure Active Directory (Azure AD) implementation and configure the users, groups, and external identities you will use to run your solution. Aligned to SC-300 Exam.

You can access the Microsoft Learn materials online content here:
https://docs.microsoft.com/en-us/learn/paths/implement-identity-management-solution/

Implement initial configuration of Azure Active Directory

Configure and manage Azure AD directory roles

In Azure Active Directory (Azure AD), if one of your users needs permission to manage Azure AD resources, you must assign them to a role that provides the permissions they need. For info on which roles manage Azure resources and which roles manage Azure AD resources

Assign roles

A common way to assign Azure AD roles to a user is on the Assigned roles page for a user. You can also configure the user eligibility to be elevated just-in-time into a role using Privileged Identity Management (PIM). For more information about how to use PIM, see Privileged Identity Management.

Assign a role to a user

1. Go to the Azure portal and sign in using a Global administrator account for the directory.

2. Search for and select **Azure Active Directory**.

3. Select Users.

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

5. On the Alain Charon - Profile page, select Assigned roles.

6. The Alain Charon - Administrative roles page appears.

7. Select Add assignments, select the role to assign to Alain (for example, Application administrator), and then choose Select.

To remove a role assignment from a user

1. Select Azure Active Directory, select Users, and then search for and select the user getting the role assignment removed. For example, Alain Charon.

2. Select Assigned roles, select Application administrator, and then select Remove assignment

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

Admin Roles

Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers.

The Microsoft 365 admin center lets you manage Azure AD roles and Microsoft Intune roles. However, these roles are a subset of the roles available in the Azure AD portal and the Intune admin center.

https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

Assign Azure AD roles to users

To grant access to users in Azure Active Directory (Azure AD), you assign Azure AD roles. A role is a collection of permissions. This article describes how to assign Azure AD roles using the Azure portal and PowerShell.

1. Sign in to the Azure portal or Azure AD admin center.

2. Select **Azure Active Directory** > **Roles and administrators** to see the list of all available roles.

3. Select a role to see its assignments.
   To help you find the role you need, use Add filters to filter the roles.

4. Select Add assignments and then select the users you want to assign to this role.

5. Select Add to assign the role.

Assign a role using PIM

If you have Azure AD Privileged Identity Management (PIM) enabled, you have additional role assignment capabilities. For example, you can make a user eligible for a role or set the duration. When PIM is enabled, there are two ways that you can assign roles using the Azure portal. You can use the Roles and administrators page or the PIM experience. Either way uses the same PIM service.

https://docs.microsoft.com/en-us/azure/active-directory/roles/manage-roles-portal

Configure and manage custom domains

To add, modify, or remove domains, you must be a Domain Name Administrator or Global Administrator of a business or enterprise plan. These changes affect the whole tenant; Customized administrators or regular users won't be able to make these changes.

Your company might need multiple domain names for different purposes. For example, you might want to add a different spelling of your company name because customers are already using it and their communications have failed to reach you.

In the Microsoft 365 admin center, choose **Setup**.

1. Under **Get your custom domain set up**, select **View** > **Manage** > **Add domain**.
2. Enter the new domain name that you want to add, and then select **Next**.
3. Sign in to your domain registrar, and then select **Next**.
4. Choose the services for your new domain.
5. Select **Next** > **Authorize** > **Next**, and then **Finish**. Your new domain has been added.

https://docs.microsoft.com/en-au/microsoft-365/admin/setup/add-domain?view=o365-worldwide

A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as yourbusiness.com or stateuniversity.edu.

Using a custom domain like "rob@contoso.com" with Microsoft 365 can help build credibility and recognition for your brand.

You can buy a domain in Microsoft 365 and we'll set it up automatically, or you can buy or bring one you already own from a domain registrar.

As a benefit of your Microsoft 365 Family or Microsoft 365 Personal subscription, you can create a personalized email address that's associated with your Outlook.com mailbox, for example, yourname@example.com. At the moment, we only support connecting domains managed by GoDaddy with Outlook.com. For more information, see Get a personalized email address in Microsoft 365.

https://docs.microsoft.com/en-au/microsoft-365/admin/setup/domains-faq?view=o365-worldwide

Set or change the default domain in Microsoft 365

You must have at least one custom domain that you've added to Microsoft 365 before you can choose a default domain.

1. In the admin center, go to the Settings > Domains page.
2. On the Domains page, select the domain you want to set as the default for new email addresses.
3. Select Set as default.

You cannot change the name of your initial .onmicrosoft.com domain.

Add custom subdomains or multiple domains to Microsoft 365?

o add subdomains, you must manage your own DNS settings at your registrar's website. If you are letting Microsoft manage your DNS settings with NS records, or if you bought the domain from Microsoft, you can't add subdomains.

Typically, you can add up to 900 domains to your Microsoft 365 subscription.

For example, you could add the domains contoso.com and contosomarketing.com, and then add the subdomains www.contoso.com, www.partners.contoso.com, www.marketing.partners.contoso.com, and so on.

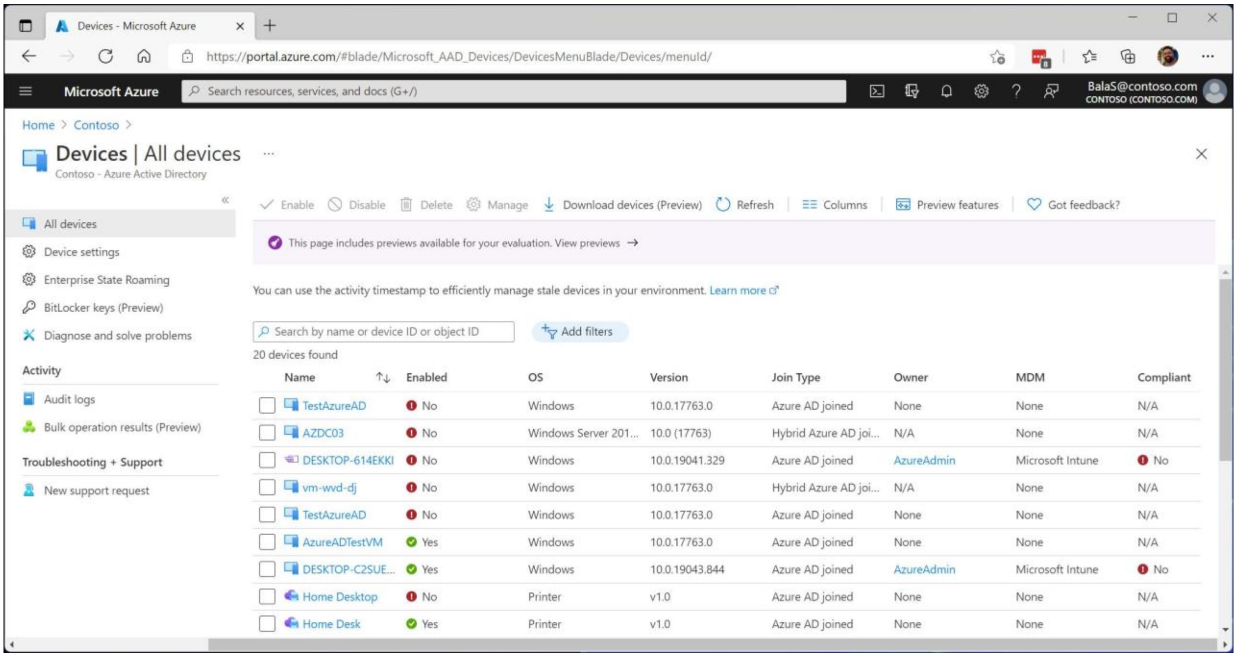
When you add a subdomain, it is automatically verified based on the parent domain that is being verified.

When you add multiple domains to Microsoft 365, you can host any of the services (like email) on any of the domains you've added. *When you change your email to Microsoft 365, by updating a domain's MX record, ALL email sent to that domain will start coming to Microsoft 365.*

https://docs.microsoft.com/en-au/microsoft-365/admin/setup/domains-faq?view=o365-worldwide

Configure and manage device registration options

A device identity is an object in Azure Active Directory (Azure AD). This device object is similar to users, groups, or applications. A device identity gives administrators information they can use when making access or configuration decisions.


Devices - Microsoft Azure
https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/Devices/menuId/
Microsoft Azure
Search resources, services, and docs (G+/)
BalaS@contoso.com
CONTOSO (CONTOSO.COM)
Home > Contoso >
Devices | All devices
Contoso - Azure Active Directory
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Enable
Disable
Delete
Manage
Download devices (Preview)
Refresh
Columns
Preview features
Got feedback?
Search by name or device ID or object ID
Add filters

This page includes previews available for your evaluation. View previews →

You can use the activity timestamp to efficiently manage stale devices in your environment. Learn more

20 devices found

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
TestAzureAD	No	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
AZDC03	No	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None	N/A
DESKTOP-614EKKI	No	Windows	10.0.19041.329	Azure AD joined	AzureAdmin	Microsoft Intune	No
vm-wvd-dj	No	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None	N/A
TestAzureAD	No	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
AzureADTestVM	Yes	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
DESKTOP-C2SUE...	Yes	Windows	10.0.19043.844	Azure AD joined	AzureAdmin	Microsoft Intune	No
Home Desktop	No	Printer	v1.0	Azure AD joined	None	None	N/A
Home Desk	Yes	Printer	v1.0	Azure AD joined	None	None	N/A

There are three ways to get a device identity:

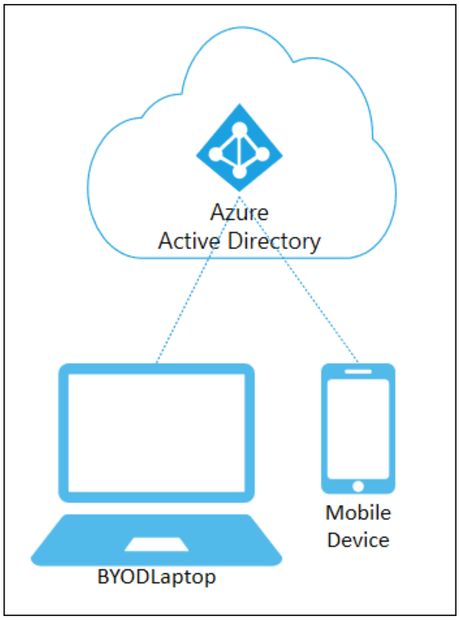
- Azure AD registration
- Azure AD join
- Hybrid Azure AD join

Device identities are a prerequisite for scenarios like device-based Conditional Access policies and Mobile Device Management with Microsoft Endpoint Manager.

https://docs.microsoft.com/en-us/azure/active-directory/devices/overview

Azure AD registered devices

The goal of Azure AD registered devices is to provide your users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization’s resources using a personal device.



Azure AD registered devices are signed in to using a local account like a Microsoft account on a Windows 10 or newer device. These devices have an Azure AD account for access to organizational resources. Access to resources in the organization can be limited based on that Azure AD account and Conditional Access policies applied to the device identity.

Administrators can secure and further control these Azure AD registered devices using Mobile Device Management (MDM) tools like Microsoft Intune. MDM provides a means to enforce organization-required configurations like requiring storage to be encrypted, password complexity, and security software kept updated.

Azure AD registration can be accomplished when accessing a work application for the first time or manually using the Windows 10 or Windows 11 Settings menu.

https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register

Configure delegation by using administrative units

An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. An administrative unit can contain only users, groups, or devices.

Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.

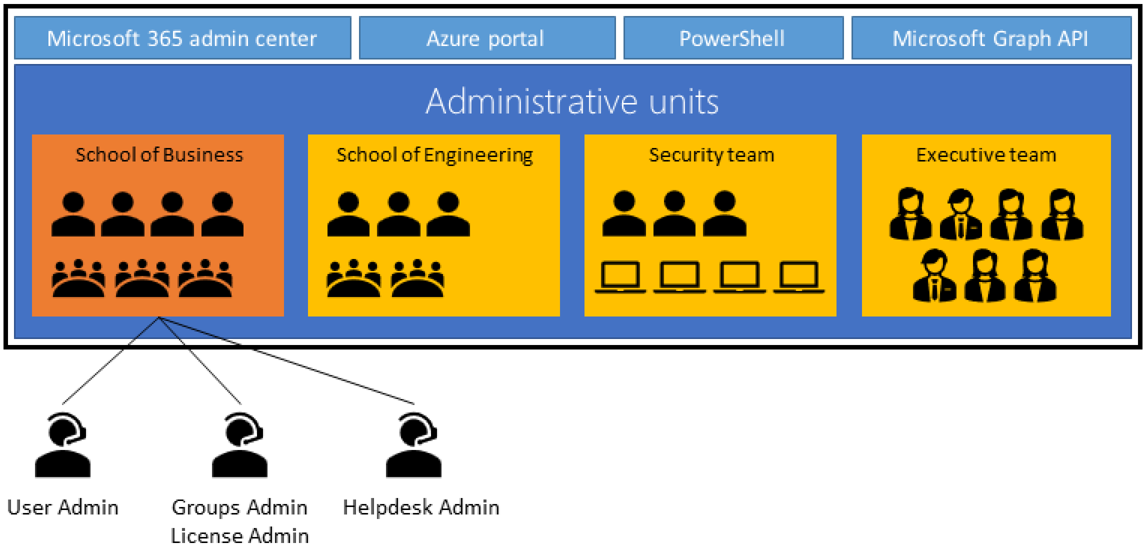
Deployment scenario

It can be useful to restrict administrative scope by using administrative units in organizations that are made up of independent divisions of any kind. Consider the example of a large university that's made up of many autonomous schools (School of Business, School of Engineering, and so on). Each school has a team of IT admins who control access, manage users, and set policies for their school.

A central administrator could:

- Create an administrative unit for the School of Business.
- Populate the administrative unit with only students and staff within the School of Business.
- Create a role with administrative permissions over only Azure AD users in the School of Business administrative unit.

Add the business school IT team to the role, along with its scope.



You can expect the creation of administrative units in the organization to go through the following stages:

1. **Initial adoption**: Your organization will start creating administrative units based on initial criteria, and the number of administrative units will increase as the criteria are refined.
2. **Pruning:** After the criteria are defined, administrative units that are no longer required will be deleted.

3.**Stabilization:** Your organizational structure is defined, and the number of administrative units isn't going to change significantly in the short term.

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

Configure tenant-wide settings

The Microsoft 365 admin center has two views: simplified view helps smaller organizations manage their most common tasks. Dashboard view includes more complex settings and tasks. You can switch between them from a button at the top of the admin center.

With the Microsoft 365 admin center, you can reset passwords, view your invoice, add or remove users, and much more all in one place.

Sign in to Office.com with your work account, and select the app launcher.

If you have permission to access the admin center, you'll see **Admin** in the list. Select it.

At the top of the admin center, review the top actions for you. You may see different actions depending on what you've already set up, such as creating new accounts, using Teams, setting up email, and installing Office apps.

Under **Your organization** on the **Users** tab is a list of people who can access apps and services, add new users, reset passwords, or use the three dots (more actions) menu. Select a person to view or edit their information and settings.

On the **Teams** tab, create a new team or manage existing teams. You can manage the members of a team or select the three dots (more actions) to change other Teams settings.

On the **Subscriptions** tab, add more products, add licenses, or use the three dots (more actions) menu to modify licenses or payment method.

On the **Learn** tab, browse videos and articles about the admin center and other Microsoft 365 features. To explore more advanced features of the admin center, open the navigation menu and expand the headings to see more. Select **Show all** to see everything in the navigation menu or use the search bar to quickly find what you're looking for.

https://docs.microsoft.com/en-us/microsoft-365/admin/multi-tenant/manage?view=o365-worldwide

Create, configure, and manage identities

Create, configure, and manage users

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

Add a new user

You can create a new user using the Azure Active Directory portal.
To add a new user, follow these steps:

1. Sign in to the Azure portal in the User Administrator role for the organization.
2. Search for and select *Azure Active Directory* from any page.
3. Select **Users**, and then select **New user**.
4. On the User page, enter information for this user:
5. Copy the autogenerated password provided in the Password box. You'll need to give this password to the user to sign in for the first time.
6. Select Create.

Add a new guest user

You can also invite new guest user to collaborate with your organization by selecting **Invite user** from the **New user** page. If your organization's external collaboration settings are configured such that you're allowed to invite guests, the user will be emailed an invitation they must accept in order to begin collaborating.

Add a consumer user

There might be scenarios in which you want to manually create consumer accounts in your Azure Active Directory B2C (Azure AD B2C) directory.

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.

Delete a user

You can delete an existing user using Azure Active Directory portal.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

Create, configure, and manage groups

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources. These resources include:

- A shared Outlook inbox
- A shared calendar
- A SharePoint document library
- A Planner
- A OneNote notebook
- Power BI
- Yammer (if the group was created from Yammer)
- A Team (if the group was created from Teams)
- Roadmap (if you have Project for the web)
- Stream

With a Microsoft 365 group, you don't have to manually assign permissions to each of these resources. Adding people to the group automatically gives them the permissions they need.

Any user can create a group unless you limit group creation to a specific set of people. If you limit group creation, users who cannot create groups will not be able to create SharePoint sites, Planners, teams, Outlook group calendars, Stream groups, Yammer groups, Shared libraries in OneDrive, or shared Power BI workspaces. These services require the people creating them to be able to create a group. Users can still participate in group activities, such as creating tasks in Planner or using Teams chat, provided they are a member of the group.

Groups have the following roles:

- **Owners** - Group owners can add or remove members and have unique permissions like the ability to delete conversations from the shared inbox or change different settings about the group. Group owners can rename the group, update the description or picture and more
- **Members** - Members can access everything in the group, but can't change group settings. By default group members can invite guests to join your group, though you can control that setting.
- **Guests** - Group guests are members who are from outside your organization.

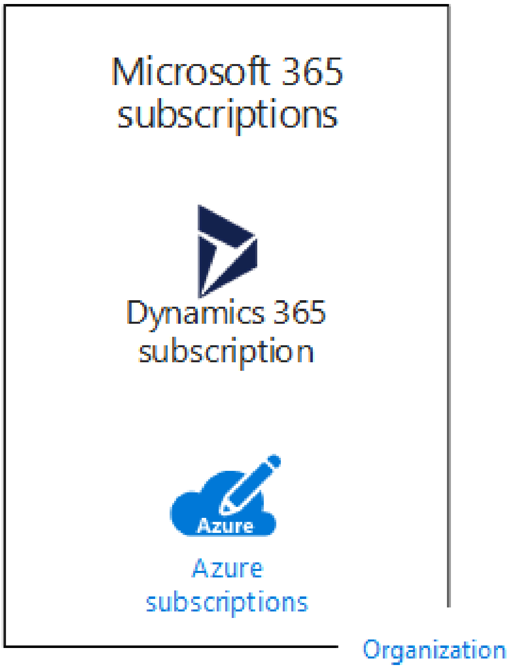
Only global admins, user admins, and groups admins can create and manage groups in the Microsoft 365 admin center. You can't be a delegated admin (for example, a consultant who is an admin on behalf of).

Manage licenses

Subscriptions
A subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based on either a per-user license fee or on cloud-based resource consumption.

- Microsoft's Software as a Service (SaaS)-based cloud offerings (Microsoft 365 and Dynamics 365) charge per-user license fees.
- Microsoft's Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud offerings (Azure) charge based on cloud resource consumption.

You can also use a trial subscription, but the subscription expires after a specific amount of time or consumption charges. You can convert a trial subscription to a paid subscription.



Organizations can have multiple subscriptions for Microsoft's cloud offerings. Figure 1 shows a single organization that has multiple Microsoft 365 subscriptions, a Dynamics 365 subscription, and multiple Azure subscriptions.

The figure is an example of multiple subscriptions for an organization

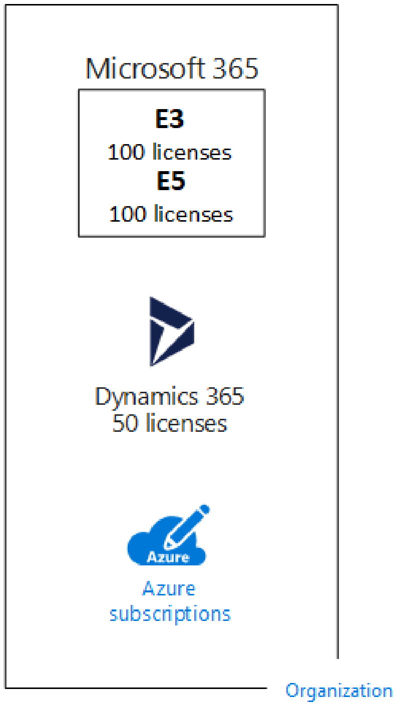
Licenses

For Microsoft's SaaS cloud offerings, a license allows a specific user account to use the services of the cloud offering. You are charged a fixed monthly fee as part of your subscription. Administrators assign licenses to individual user accounts in the subscription. For the example in Figure 2, the Contoso Corporation has a Microsoft 365 E5 subscription with 100 licenses, which allows to up to 100 individual user accounts to use Microsoft 365 E5 features and services.

Figure 2: Licenses within the SaaS-based subscriptions for an organization

For Azure PaaS-based cloud services, software licenses are built into the service pricing.

For Azure IaaS-based virtual machines, additional licenses to use the software or application installed on a virtual machine image might be required. Some virtual machine images have licensed versions of software installed and the cost is included in the per-minute rate for the server. Examples are the virtual machine images for SQL Server 2014 and SQL Server 2016.



Some virtual machine images have trial versions of applications installed and need additional software application licenses for use beyond the trial period. For example, the SharePoint Server 2016 Trial virtual machine image includes a trial version of SharePoint Server 2016 pre-installed. To continue using SharePoint Server 2016 after the trial expiration date, you must purchase a SharePoint Server 2016 license and client licenses from Microsoft. These charges are separate from the Azure subscription and the per-minute rate to run the virtual machine still applies.

An easy way to add subscriptions to your organization for Microsoft SaaS-based services is through the admin center:

1. Sign in to the Microsoft 365 admin center (https://admin.microsoft.com) with your **User Admin**, or **Global admin** account.
2. From the left navigation of the **Admin center** home page, click **Billing**, and then **Purchase services**.
3. On the **Purchase services** page, purchase your new subscriptions.

https://docs.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings

Implement and manage external identities

Manage external collaboration settings in Azure Active Directory

External collaboration settings let you specify what roles in your organization can invite external users for B2B collaboration. These settings also include options for allowing or blocking specific domains, and options for restricting what external guest users can see in your Azure AD directory. The following options are available:

- **Determine guest user access**: Azure AD allows you to restrict what external guest users can see in your Azure AD directory. For example, you can limit guest users' view of group memberships, or allow guests to view only their own profile information.

- **Specify who can invite guests**: By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration. If you want to limit the ability to send invitations, you can turn invitations on or off for everyone, or limit invitations to certain roles.

- **Enable guest self-service sign-up via user flows**: For applications you build, you can create user flows that allow a user to sign up for an app and create a new guest account. You can enable the feature in your external collaboration settings, and then add a self-service sign-up user flow to your app.

- **Allow or block domains**: You can use collaboration restrictions to allow or deny invitations to the domains you specify. For details, see Allow or block domains.
For B2B collaboration with other Azure AD organizations, you should also review your cross-tenant access settings to ensure your inbound and outbound B2B collaboration and scope access to specific users, groups, and applications.

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure

Invite external users (individually or in bulk)

You can invite anyone to collaborate with your organization by adding them to your directory as a guest user. Then you can either send an invitation email that contains a redemption link or send a direct link to an app you want to share. Guest users can sign in with their own work, school, or social identities. Along with this quickstart, you can learn more about adding guest users in the Azure portal, via PowerShell, or in bulk.

In this quickstart, you'll add a new guest user to your Azure AD directory via the Azure portal, send an invitation, and see what the guest user's invitation redemption process looks like.

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

Accept the invitation

Now sign in as the guest user to see the invitation.

1. Sign in to your test guest user's email account.
2. In your inbox, find the "You're invited" email.
3. In the email body, select **Get Started**. A **Review permissions** page opens in the browser.
4. Select **Accept**. The Access Panel opens, which lists the applications the guest user can access.

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

Add a guest user with PowerShell

There are many ways you can invite external partners to your apps and services with Azure Active Directory B2B collaboration. In the previous quickstart, you saw how to add guest users directly in the Azure Active Directory admin portal. You can also use PowerShell to add guest users, either one at a time or in bulk. In this quickstart, you’ll use the New-MgInvitation command to add one guest user to your Azure tenant.

You need a test email account that you can send the invitation to. The account must be from outside your organization. You can use any type of account, including a social account such as a gmail.com or outlook.com address.

Sign in to your tenant

Run the following command to connect to the tenant domain:

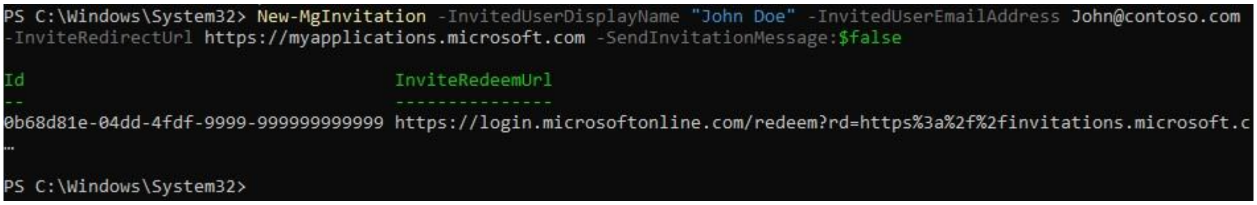
Connect-MgGraph -Scopes user.readwrite.all

Send an invitation

1. To send an invitation to your test email account, run the following PowerShell command (replace **"John Doe"** and **john@contoso.com** with your test email account name and email address):

New-MgInvitation -InvitedUserDisplayName "John Doe" -InvitedUserEmailAddress John@contoso.com -InviteRedirectUrl "https://myapplications.microsoft.com" -SendInvitationMessage:$true

The command sends an invitation to the email address specified. Check the output, which should look similar to the following example:



```
PS C:\Windows\System32> New-MgInvitation -InvitedUserDisplayName "John Doe" -InvitedUserEmailAddress John@contoso.com
-InviteRedirectUrl https://myapplications.microsoft.com -SendInvitationMessage:$false

Id                                   InviteRedeemUrl
--                                   ---------------
0b68d81e-04dd-4fdf-9999-999999999999 https://login.microsoftonline.com/redeem?rd=https%3a%2f%2finvitations.microsoft.c
…

PS C:\Windows\System32>
```

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-invite-powershell

Bulk invite Azure AD B2B collaboration users

If you use Azure Active Directory (Azure AD) B2B collaboration to work with external partners, you can invite multiple guest users to your organization at the same time. In this tutorial, you learn how to use the Azure portal to send bulk invitations to external users. Specifically, you'll follow these steps:

✓Use **Bulk invite users** to prepare a comma-separated value (.csv) file with the user information and invitation preferences
✓Upload the .csv file to Azure AD
✓Verify the users were added to the directory

Invite guest users in bulk

1. Sign in to the Azure portal with an account that is a global administrator in the organization.
2. In the navigation pane, select **Azure Active Directory**.
3. Under **Manage**, select **All Users**.
4. Select **Bulk operations** > **Bulk invite**.
5. On the **Bulk invite users** page, select **Download** to get a valid .csv template with invitation properties.
6. Open the .csv template and add a line for each guest user.
7. Save the file.
8. On the Bulk invite users page, under Upload your csv file, browse to the file. When you select the file, validation of the .csv file starts.
9. When the file contents are validated, you’ll see File uploaded successfully. If there are errors, you must fix them before you can submit the job.

10. When your file passes validation, select Submit to start the Azure bulk operation that adds the invitations.
11. To view the job status, select Click here to view the status of each operation. Or, you can select Bulk operation results in the Activity section. For details about each line item within the bulk operation, select the values under the # Success, # Failure, or Total Requests columns. If failures occurred, the reasons for failure will be listed.
12. When the job completes, you'll see a notification that the bulk operation succeeded.

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite

Manage external user accounts in Azure Active Directory

Traditionally, SharePoint permissions have been managed through a set of permissions groups within a site (Owners, Members, Visitors, etc.). In SharePoint in Microsoft 365, this remains true for some types of sites, but additional options are available and SharePoint is part of a much broader set of capabilities for secure collaboration with Microsoft 365.

The main types of sites in SharePoint are:

- **Team sites** - Team sites provide a collaboration environment for your teams and projects. Each team site, by default, is part of a Microsoft 365 group, which includes a mailbox, shared calendar, and other collaboration tools. Team sites may also be part of a team in Microsoft Teams. Permissions for team sites are best managed through the associated Microsoft 365 group or Teams team.
- **Channel sites** - Channel sites are team sites that are associated with a specific channel in a Teams team. Both private and shared channels create separate SharePoint sites just for the channel.
- **Communication sites** - Communication sites are for broadcasting news and status across the organization. Communication site permissions are managed by using the SharePoint Owners, Members, and Visitors groups for the site.
- **Hub sites** - Hub sites are team sites or communication sites that the administrator has configured as the center of a hub. They're designed to provide connection between related sites through shared navigation. Permissions for hub sites can be managed through the Owners, Members, and Visitors groups, or through the associated Microsoft 365 group if there is one. Special permissions are needed to associate sites to a hub.

https://docs.microsoft.com/en-us/sharepoint/modern-experience-sharing-permissions

Configure identity providers (social and SAML/WS-fed)

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

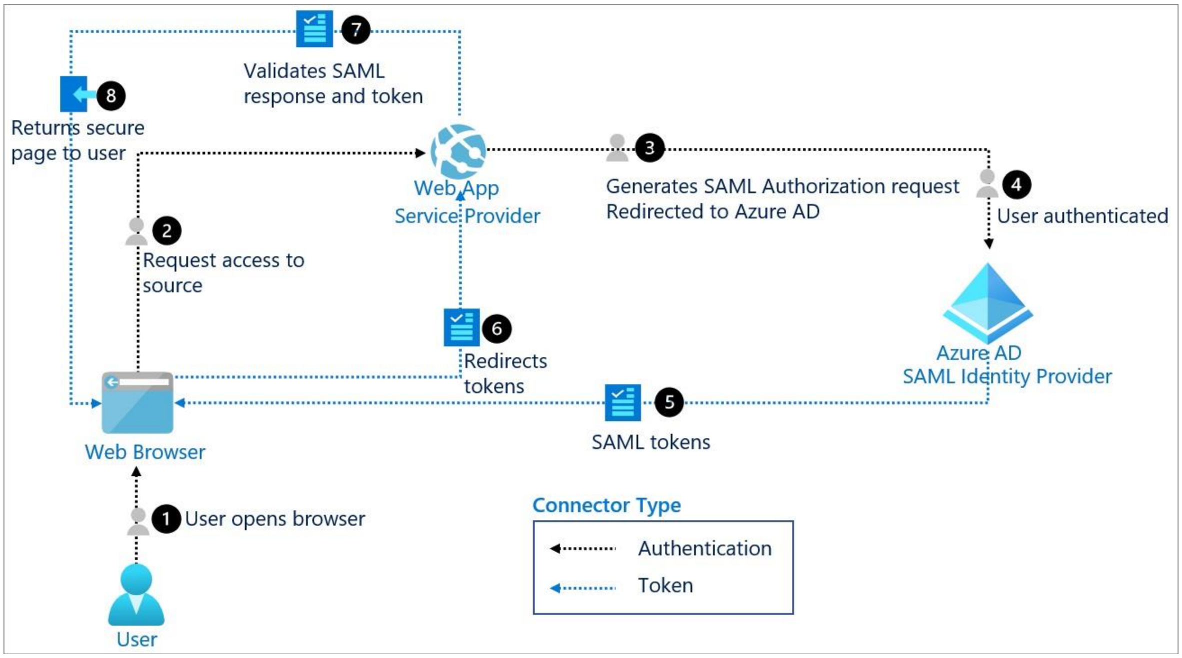
The SAML specification defines three roles:

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

Use When

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

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



https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-saml

Implement and manage hybrid identity

Implement and manage Azure Active Directory Connect (AADC)

Microsoft 365 uses an Azure Active Directory (Azure AD) tenant to store and manage identities for authentication and permissions to access cloud-based resources.

If you have an on-premises Active Directory Domain Services (AD DS) domain or forest, you can synchronize your AD DS user accounts, groups, and contacts with the Azure AD tenant of your Microsoft 365 subscription. This is hybrid identity for Microsoft 365. Here are its components.

Azure AD Connect runs on an on-premises server and synchronizes your AD DS with the Azure AD tenant. Along with directory synchronization, you can also specify these authentication options:

- Password hash synchronization (PHS)
- Azure AD performs the authentication itself.
- Pass-through authentication (PTA)
- Azure AD has AD DS perform the authentication.
- Federated authentication
- Azure AD refers the client computer requesting authentication to another identity provider.

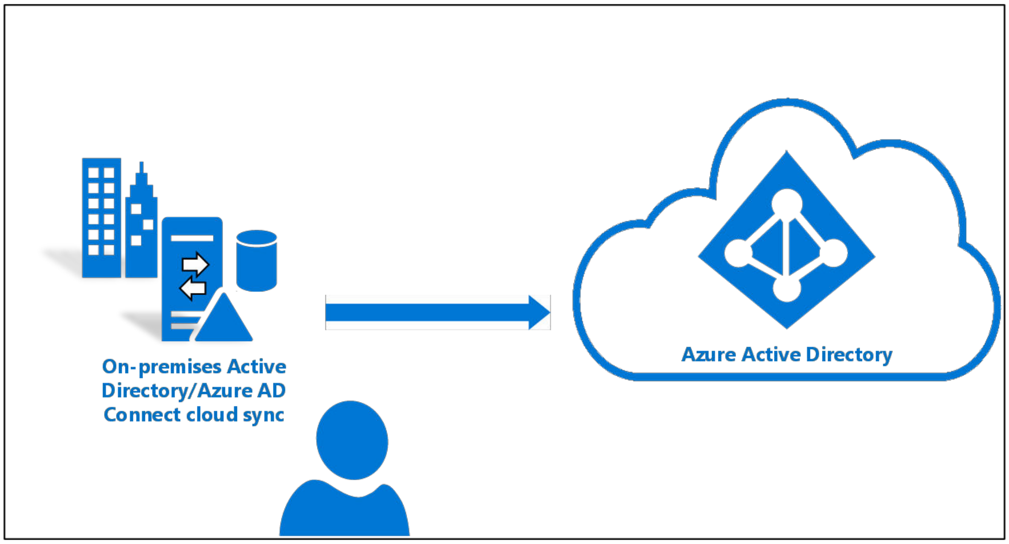
https://docs.microsoft.com/en-us/microsoft-365/enterprise/set-up-directory-synchronization?view=o365-worldwide

Implement and manage Azure AD Connect cloud sync

Azure AD Connect cloud sync is new offering from Microsoft designed to meet and accomplish your hybrid identity goals for synchronization of users, groups, and contacts to Azure AD. It accomplishes this by using the Azure AD cloud provisioning agent instead of the Azure AD Connect application. However, it can be used alongside Azure AD Connect sync and it provides the following benefits:

- Support for synchronizing to an Azure AD tenant from a multi-forest disconnected Active Directory forest environment: The common scenarios include merger & acquisition (where the acquired company's AD forests are isolated from the parent company's AD forests), and companies that have historically had multiple AD forests.

- Simplified installation with light-weight provisioning agents: The agents act as a bridge from AD to Azure AD, with all the sync configuration managed in the cloud.
- Multiple provisioning agents can be used to simplify high availability deployments, particularly critical for organizations relying upon password hash synchronization from AD to Azure AD.
- Support for large groups with up to 50,000 members. It's recommended to use only the OU scoping filter when synchronizing large groups.



https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/what-is-cloud-sync?

Cloud sync configuration

To configure provisioning, follow these steps.

1. In the Azure portal, select **Azure Active Directory**
2. Select **Azure AD Connect**.
3. Select **Manage cloud sync**.
4. Select New configuration.
5. On the configuration screen, select your domain and whether to enable password hash sync. Click Create.
6. The Edit provisioning configuration screen will open.
7. Enter a Notification email. This email will be notified when provisioning isn't healthy. It is recommended that you keep Prevent accidental deletion enabled and set the Accidental deletion threshold to a number that you wish to be notified about. For more information see accidental deletes below.
8. Move the selector to Enable, and select Save.

https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-configure

Implement and manage Password Hash Synchronization (PHS)

The Active Directory domain service stores passwords in the form of a hash value representation, of the actual user password. A hash value is a result of a one-way mathematical function (the *hashing algorithm*). There is no method to revert the result of a one-way function to the plain text version of a password.

To synchronize your password, Azure AD Connect sync extracts your password hash from the on-premises Active Directory instance. Extra security processing is applied to the password hash before it is synchronized to the Azure Active Directory authentication service. Passwords are synchronized on a per-user basis and in chronological order.

The actual data flow of the password hash synchronization process is similar to the synchronization of user data. However, passwords are synchronized more frequently than the standard directory synchronization window for other attributes. The password hash synchronization process runs every 2 minutes. You cannot modify the frequency of this process. When you synchronize a password, it overwrites the existing cloud password.

The first time you enable the password hash synchronization feature, it performs an initial synchronization of the passwords of all in-scope users. You cannot explicitly define a subset of user passwords that you want to synchronize. However, if there are multiple connectors, it is possible to disable password hash sync for some connectors but not others using the Set-ADSyncAADPasswordSyncConfiguration cmdlet.

When you change an on-premises password, the updated password is synchronized, most often in a matter of minutes. The password hash synchronization feature automatically retries failed synchronization attempts. If an error occurs during an attempt to synchronize a password, an error is logged in your event viewer.

The synchronization of a password has no impact on the user who is currently signed in. Your current cloud service session is not immediately affected by a synchronized password change that occurs, while you are signed in, to a cloud service. However, when the cloud service requires you to authenticate again, you need to provide your new password.

A user must enter their corporate credentials a second time to authenticate to Azure AD, regardless of whether they're signed in to their corporate network. This pattern can be minimized, however, if the user selects the Keep me signed in (KMSI) check box at sign-in. This selection sets a session cookie that bypasses authentication for 180 days. KMSI behavior can be enabled or disabled by the Azure AD administrator. In addition, you can reduce password prompts by turning on Seamless SSO, which automatically signs users in when they are on their corporate devices connected to your corporate network.

Enable password hash synchronization

When you install Azure AD Connect by using the **Express Settings** option, password hash synchronization is automatically enabled.

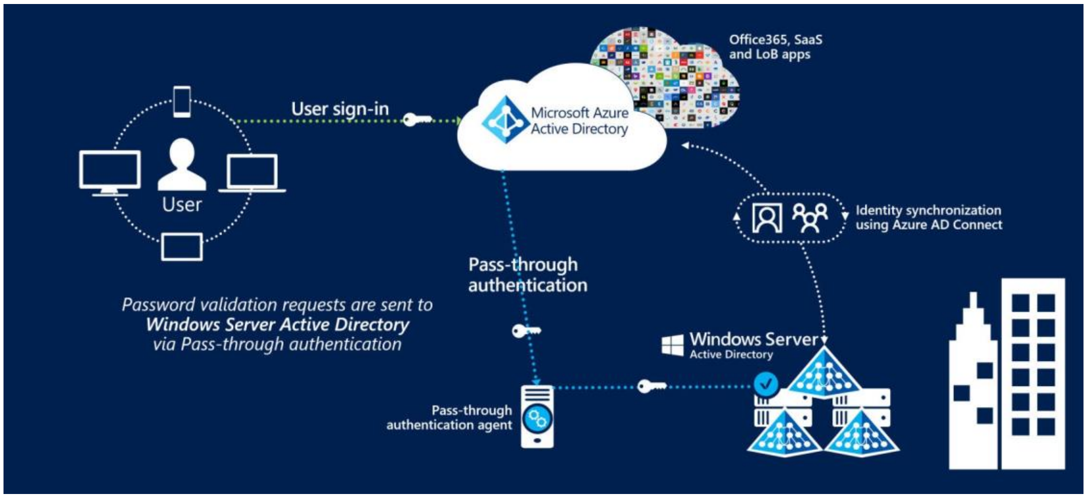
If you use custom settings when you install Azure AD Connect, password hash synchronization is available on the user sign-in page.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

Implement and manage Pass-Through Authentication (PTA)

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to 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 users sign in using Azure AD, this feature validates users' passwords directly against your on-premises Active Directory.

This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead. Review this guide for a comparison of the various Azure AD sign-in methods and how to choose the right sign-in method for your organization.


Office365, SaaS and LoB apps
User sign-in
Microsoft Azure Active Directory
User
Identity synchronization using Azure AD Connect
Pass-through authentication
Password validation requests are sent to Windows Server Active Directory via Pass-through authentication
Windows Server Active Directory
Pass-through authentication agent

You can combine Pass-through Authentication with the Seamless Single Sign-On feature. This way, when your users are accessing applications on their corporate machines inside your corporate network, they don't need to type in their passwords to sign in.

Key benefits of using Azure AD Pass-through Authentication

- *Great user experience*
- *Easy to deploy & administer*
- *Secure*
- *Highly available*

Feature highlights

- Supports user sign-in into all web browser-based applications and into Microsoft Office client applications that use modern authentication.
- Sign-in usernames can be either the on-premises default username (userPrincipalName) or another attribute configured in Azure AD Connect (known as Alternate ID).

The feature works seamlessly with Conditional Access features such as Multi-Factor Authentication (MFA) to help secure your users.

- Integrated with cloud-based self-service password management, including password write back to on-premises Active Directory and password protection by banning commonly used passwords.
- Multi-forest environments are supported if there are forest trusts between your AD forests and if name suffix routing is correctly configured.
- It is a free feature, and you don't need any paid editions of Azure AD to use it.

It can be enabled via Azure AD Connect.

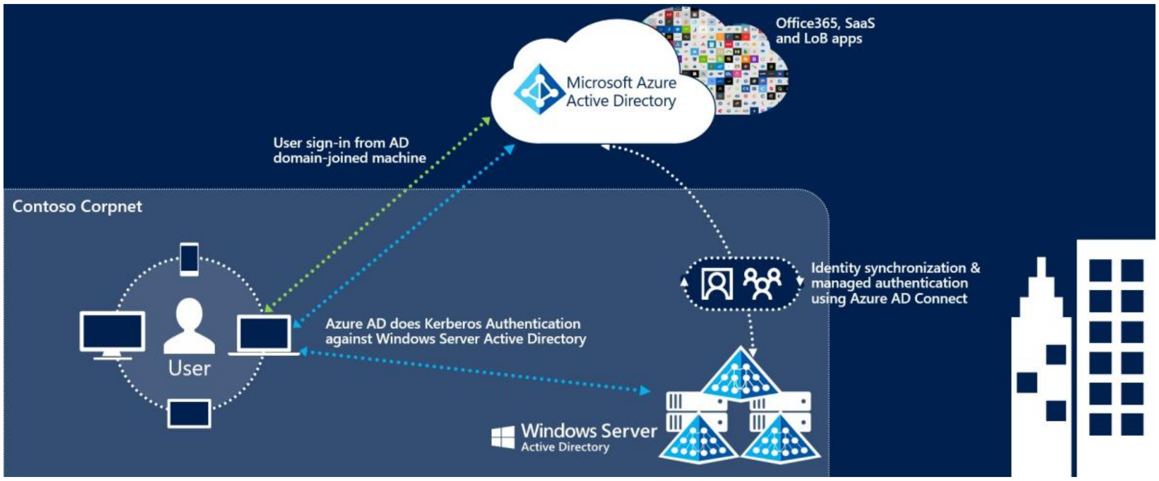
- It uses a lightweight on-premises agent that listens for and responds to password validation requests.
- Installing multiple agents provides high availability of sign-in requests.
- It protects your on-premises accounts against brute force password attacks in the cloud.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Implement and manage seamless Single Sign-On (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. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. Seamless SSO is not applicable to Active Directory Federation Services (ADFS).


Office365, SaaS and LoB apps
Microsoft Azure Active Directory
User sign-in from AD domain-joined machine
Contoso Corpnet
Identity synchronization & managed authentication using Azure AD Connect
User
Azure AD does Kerberos Authentication against Windows Server Active Directory
Windows Server Active Directory

Key benefits

- ***Great user experience***
  ◊ Users are automatically signed into both on-premises and cloud-based applications.
  ◊ Users don't have to enter their passwords repeatedly.

- ***Easy to deploy & administer***
  ◊No additional components needed on-premises to make this work.
  ◊Works with any method of cloud authentication - Password Hash Synchronization or Pass-through Authentication.
  ◊Can be rolled out to some or all your users using Group Policy.

◊ Register non-Windows 10 devices with Azure AD without the need for any AD FS infrastructure. This capability needs you to use version 2.1 or later of the workplace-join client.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

Implement and manage Federation excluding manual ADFS deployments

Manage AD FS

You can perform various AD FS-related tasks in Azure AD Connect with minimal user intervention by using the Azure AD Connect wizard. After you've finished installing Azure AD Connect by running the wizard, you can run the wizard again to perform additional tasks.

Repair the trust

You can use Azure AD Connect to check the current health of the AD FS and Azure AD trust and take appropriate actions to repair the trust. Follow these steps to repair your Azure AD and AD FS trust.

1. Select **Repair AAD and ADFS Trust** from the list of additional tasks.
2. On the Connect to Azure AD page, provide your global administrator credentials for Azure AD, and click Next.
3. On the Remote access credentials page, enter the credentials for the domain administrator.
After you click Next, Azure AD Connect checks for certificate health and shows any issues. The Ready to configure page shows the list of actions that will be performed to repair the trust.
4. Click Install to repair the trust.

Federate with Azure AD using AlternateID

It is recommended that the on-premises User Principal Name(UPN) and the cloud User Principal Name are kept the same. If the on-premises UPN uses a non-routable domain (ex. Contoso.local) or cannot be changed due to local application dependencies, we recommend setting up alternate login ID. Alternate login ID allows you to configure a sign-in experience where users can sign in with an attribute other than their UPN, such as mail. The choice for User Principal Name in Azure AD Connect defaults to the userPrincipalName attribute in Active Directory. If you choose any other attribute for User Principal Name and are federating using AD FS, then Azure AD Connect will configure AD FS for alternate login ID.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-management

Implement and manage Azure Active Directory Connect Health

You can configure the Azure AD Connect Health service to send email notifications when alerts indicate that your identity infrastructure is not healthy. This occurs when an alert is generated, and when it is resolved.

To enable Azure AD Connect Health email notifications

1. In the Azure Portal, search for Azure AD Connect Health
2. Select **Sync errors**
3. Select **Notification Settings**.
4. At the email notification switch, select **ON**.
5. Select the check box if you want all global administrators to receive email notifications.
6. If you want to receive email notifications at any other email addresses, specify them in the **Additional Email Recipients** box. To remove an email address from this list, right-click the entry and select **Delete**.
7. To finalize the changes, click **Save**. Changes take effect only after you save.

Manage access with Azure RBAC

Azure role-based access control (Azure RBAC) for Azure AD Connect Health provides access to users and groups other than global administrators. Azure RBAC assigns roles to the intended users and groups, and provides a mechanism to limit the global administrators within your directory.

Azure AD Connect Health supports the following built-in roles:

Role	Permissions
Owner	Owners can *manage access* (for example, assign a role to a user or group), *view all information* (for example, view alerts) from the portal, and *change settings* (for example, email notifications) within Azure AD Connect Health. By default, Azure AD global administrators are assigned this role, and this cannot be changed.
Contributor	Contributors can *view all information* (for example, view alerts) from the portal, and *change settings* (for example, email notifications) within Azure AD Connect Health.
Reader	Readers can *view all information* (for example, view alerts) from the portal within Azure AD Connect Health.

All other roles (such as User Access Administrators or DevTest Labs Users) have no impact to access within Azure AD Connect Health, even if the roles are available in the portal experience.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations

Troubleshoot synchronization errors

Errors can occur when identity data is synced from Windows Server Active Directory to Azure Active Directory (Azure AD). This article provides an overview of different types of sync errors, some of the possible scenarios that cause those errors, and potential ways to fix the errors. This article includes common error types and might not cover all possible errors.

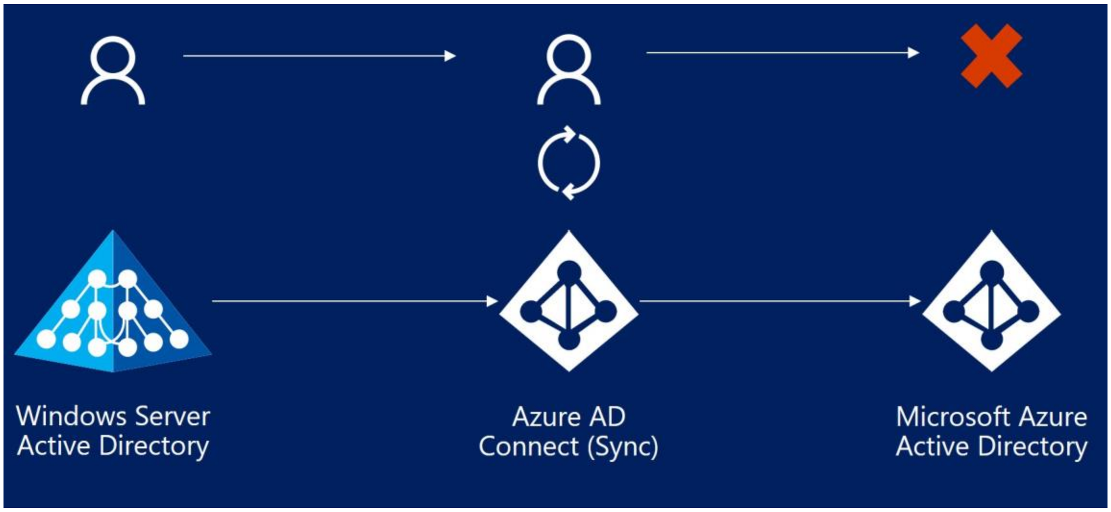
With the latest version of Azure AD Connect (August 2016 or higher), a Synchronization Errors Report is available in the Azure portal as part of Azure AD Connect Health for sync.

Starting September 1, 2016, Azure AD duplicate attribute resiliency is enabled by default for all the new Azure AD tenants. This feature is automatically enabled for existing tenants.

Azure AD Connect performs three types of operations from the directories it keeps in sync: Import, Synchronization, and Export. Errors can occur in all three operations. This article mainly focuses on errors during export to Azure AD.

Errors during export to Azure AD

The following section describes different types of synchronization errors that can occur during the export operation to Azure AD by using the Azure AD connector. You can identify this connector by the name format contoso.onmicrosoft.com. Errors during export to Azure AD indicate that an operation like add, update, or delete attempted by Azure AD Connect (sync engine) on Azure AD failed.



https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-sync-errors

Implement an authentication and access management solution (25-30%)

Plan and implement Azure Multifactor Authentication (MFA)

Plan Azure MFA deployment (excluding MFA Server)

In this world of mobility, with users accessing data and applications in the cloud and from any device, securing this information has become paramount. Every day there is a new headline about a security breach. Although, there is no guarantee against such breaches, multi-factor authentication, provides an additional layer of security to help prevent these breaches. Start by evaluating the organizations requirements for multi-factor authentication. That is, what is the organization trying to secure. This evaluation is important to define the technical requirements for setting up and enabling the organizations users for multi-factor authentication.

Make sure to answer the following:

- Is your company trying to secure Microsoft apps?
- How these apps are published?
- Does your company provide remote access to allow employees to access on-premises apps?

If yes, what type of remote access? You also need to evaluate where the users who are accessing these applications will be located. This evaluation is another important step to define the proper multi-factor authentication strategy. Make sure to answer the following questions:

- Where are the users going to be located?
- Can they be located anywhere?
- Does your company want to establish restrictions according to the user's location?

Once you understand these requirements, it is important to also evaluate the user's requirements for multi-factor authentication. This evaluation is important because it will define the requirements for rolling out multi-factor authentication. Make sure to answer the following questions:

- Are the users familiar with multi-factor authentication?

- Will some uses be required to provide additional authentication?
- If yes, all the time, when coming from external networks, or accessing specific applications, or under other conditions?
- Will the users require training on how to setup and implement multi-factor authentication?
- What are the key scenarios that your company wants to enable multi-factor authentication for their users?

After answering the previous questions, you will be able to understand if there are multi-factor authentication already implemented on-premises. This evaluation is important to define the technical requirements for setting up and enabling the organizations users for multi-factor authentication. Make sure to answer the following questions:

- Does your company need to protect privileged accounts with MFA?
- Does your company need to enable MFA for certain application for compliance reasons?
- Does your company need to enable MFA for all eligible users of these application or only administrators?
- Do you need have MFA always enabled or only when the users are logged outside of your corporate network?

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-hybrid-identity-design-considerations-multifactor-auth-requirements

Implement and manage Azure MFA settings

Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan. If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate.

Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

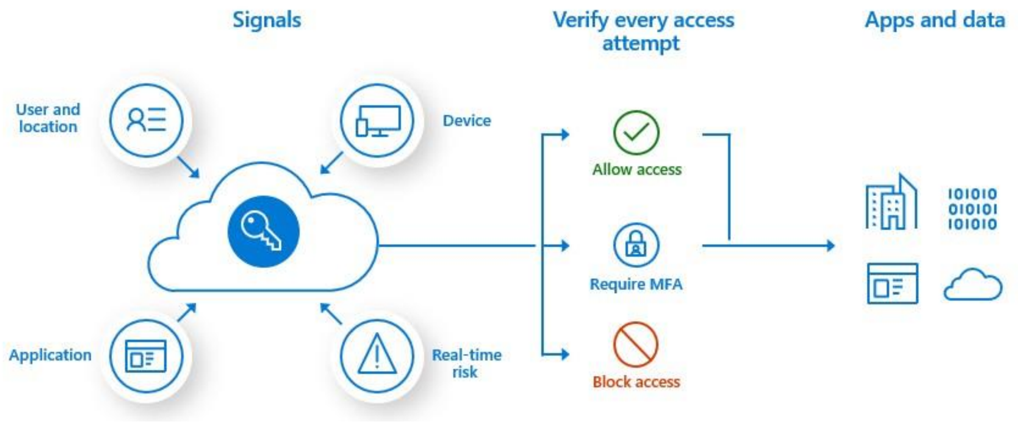
- Something you know, typically a password.
- Something you have, such as a trusted device that's not easily duplicated, like a phone or hardware key.
- Something you are - biometrics like a fingerprint or face scan.

Azure AD Multi-Factor Authentication can also further secure password reset. When users register themselves for Azure AD Multi-Factor Authentication, they can also register for self-service password reset in one step. Administrators can choose forms of secondary authentication and configure challenges for MFA based on configuration decisions.
You don't need to change apps and services to use Azure AD Multi-Factor Authentication. The verification prompts are part of the Azure AD sign-in, which automatically requests and processes the MFA challenge when needed.

How to enable and use Azure AD Multi-Factor Authentication

You can use security defaults in Azure AD tenants to quickly enable Microsoft Authenticator for all users. You can enable Azure AD Multi-Factor Authentication to prompt users and groups for additional verification during sign-in.

For more granular controls, you can use Conditional Access policies to define events or applications that require MFA. These policies can allow regular sign-in when the user is on the corporate network or a registered device but prompt for additional verification factors when the user is remote or on a personal device.



https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Manage MFA settings for users

Multi-factor authentication (MFA) is a process in which a user is prompted for additional forms of identification during a sign-in event. For example, the prompt could be to enter a code on their cellphone or to provide a fingerprint scan. When you require a second form of identification, security is increased because this additional factor isn't easy for an attacker to obtain or duplicate.

Azure AD Multi-Factor Authentication and Conditional Access policies give you the flexibility to require MFA from users for specific sign-in events.

Create a Conditional Access policy

The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.

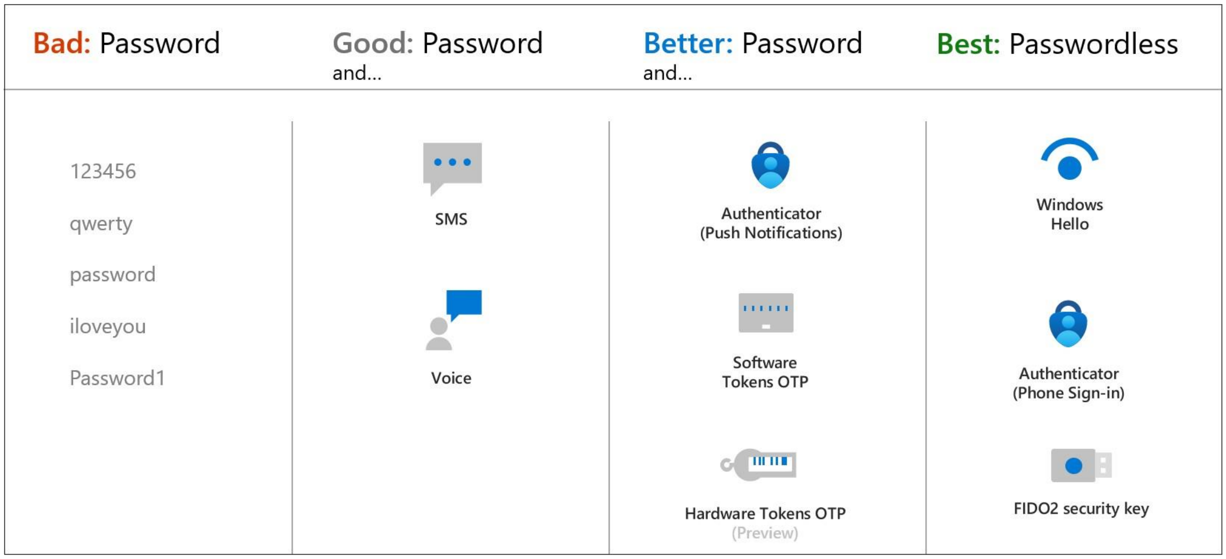
Conditional Access policies can be applied to specific users, groups, and apps. The goal is to protect your organization while also providing the right levels of access to the users who need it.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

Manage user authentication

Administer authentication methods (FIDO2 / Passwordless)

Microsoft recommends passwordless authentication methods such as Windows Hello, FIDO2 security keys, and the Microsoft Authenticator app because they provide the most secure sign-in experience. Although a user can sign-in using other common methods such as a username and password, passwords should be replaced with more secure authentication methods.



Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456 qwerty password iloveyou Password1	SMS Voice	Authenticator (Push Notifications) Software Tokens OTP Hardware Tokens OTP (Preview)	Windows Hello Authenticator (Phone Sign-in) FIDO2 security key

Azure AD Multi-Factor Authentication (MFA) adds additional security over only using a password when a user signs in. The user can be prompted for additional forms of authentication, such as to respond to a push notification, enter a code from a software or hardware token, or respond to an SMS or phone call.

To simplify the user on-boarding experience and register for both MFA and self-service password reset (SSPR), we recommend you enable combined security information registration. For resiliency, we recommend that you require users to register multiple authentication methods. When one method isn't available for a user during sign-in or SSPR, they can choose to authenticate with another method.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Implement an authentication solution based on Windows Hello for Business

Windows Hello for Business is the springboard to a world without passwords. It replaces username and password sign-in to Windows with strong user authentication based on an asymmetric key pair.

Windows Hello for Business has three deployment models: Azure **AD cloud only, hybrid, and on-premises**. Hybrid has three trust models: *Key trust*, *certificate trust*, and *cloud trust*. On-premises deployment models only support *Key trust* and *certificate trust*.

Hybrid deployments are for enterprises that use Azure Active Directory. On-premises deployments are for enterprises who exclusively use on-premises Active Directory. Remember that the environments that use Azure Active Directory must use the hybrid deployment model for all domains in that forest.

The trust model determines how you want users to authenticate to the on-premises Active Directory:

- **The key-trust model** is for enterprises who do not want to issue end-entity certificates to their users and have an adequate number of 2016 domain controllers in each site to support authentication. This still requires Active Directory Certificate Services for domain controller certificates.
- **The cloud-trust model** is also for hybrid enterprises who do not want to issue end-entity certificates to their users and have an adequate number of 2016 domain controllers in each site to support authentication. This trust model is simpler to deploy than key trust and does not require Active Directory Certificate Services. We recommend using cloud trust instead of key trust if the clients in your enterprise support it.

- **The certificate-trust** model is for enterprises that *do* want to issue end-entity certificates to their users and have the benefits of certificate expiration and renewal, similar to how smart cards work today.

The certificate trust model also supports enterprises which are not ready to deploy Windows Server 2016 Domain Controllers.

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-deployment-guide

Configure and deploy self-service password reset

Azure Active Directory (Azure AD) self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.

How does the password reset process work?

A user can reset or change their password using the SSPR portal. They must first have registered their desired authentication methods.

When a user selects the **Can't access your account** link from an application or page, or goes directly to https://aka.ms/sspr, the language used in the SSPR portal is based on the following options:

By default, the browser locale is used to display the SSPR in the appropriate language. The password reset experience is localized into the same languages that Microsoft 365 supports.

After the SSPR portal is displayed in the required language, the user is prompted to enter a user ID and pass a captcha. Azure AD now verifies that the user is able to use SSPR by doing the following checks:

- Checks that the user has SSPR enabled.
- Checks that the user has the right authentication methods defined on their account in accordance with administrator policy.
- Checks to see if the user's password is managed on-premises, such as if the Azure AD tenant is using federated, pass-through authentication, or password hash synchronization:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

Deploy and manage password protection

A lot of security guidance recommends that you don't use the same password in multiple places, to make it complex, and to avoid simple passwords like *Password123*. You can provide your users with guidance on how to choose passwords, but weak or insecure passwords are often still used. Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

You should use additional features like Azure AD Multi-Factor Authentication, not just rely on strong passwords enforced by Azure AD Password Protection.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

Implement and manage tenant restrictions

Large organizations that emphasize security want to move to cloud services like Microsoft 365, but need to know that their users only can access approved resources. Traditionally, companies restrict domain names or IP addresses when they want to manage access. This approach fails in a world where software as a service (or SaaS) apps are hosted in a public cloud, running on shared domain names like outlook.office.com and login.microsoftonline.com. Blocking these addresses would keep users from accessing Outlook on the web entirely, instead of merely restricting them to approved identities and resources.

The Azure Active Directory (Azure AD) solution to this challenge is a feature called tenant restrictions. With tenant restrictions, organizations can control access to SaaS cloud applications, based on the Azure AD tenant the applications use for single sign-on. For example, you may want to allow access to your organization's Microsoft 365 applications, while preventing access to other organizations' instances of these same applications.

With tenant restrictions, organizations can specify the list of tenants that users on their network are permitted to access. Azure AD then only grants access to these permitted tenants - all other tenants are blocked, even ones that your users may be guests in.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions

Configure smart lockout thresholds

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

By default, smart lockout locks the account from sign-in attempts for one minute after 10 failed attempts for Azure Public and Azure China 21Vianet tenants and 3 for Azure US Government tenants. The account locks again after each subsequent failed sign-in attempt, for one minute at first and longer in subsequent attempts. To minimize the ways an attacker could work around this behavior, we don't disclose the rate at which the lockout period grows over additional unsuccessful sign-in attempts.

Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password. If someone enters the same bad password multiple times, this behavior won't cause the account to lock out.

Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

Using smart lockout doesn't guarantee that a genuine user is never locked out. When smart lockout locks a user account, we try our best to not lock out the genuine user. The lockout service attempts to ensure that bad actors can't gain access to a genuine user account. The following considerations apply:

- Each Azure AD data center tracks lockout independently. A user has (*threshold_limit * datacenter_count*) number of attempts, if the user hits each data center.
- Smart Lockout uses familiar location vs unfamiliar location to differentiate between a bad actor and the genuine user. Unfamiliar and familiar locations both have separate lockout counters.

Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers. By setting smart lockout policies in Azure AD appropriately, attacks can be filtered out before they reach on-premises AD DS.

When using pass-through authentication, the following considerations apply:

- The Azure AD lockout threshold is **less** than the AD DS account lockout threshold. Set the values so that the AD DS account lockout threshold is at least two or three times greater than the Azure AD lockout threshold.

The Azure AD lockout duration must be set longer than the AD DS reset account lockout counter after duration. The Azure AD duration is set in seconds, while the AD duration is set in minutes.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

Plan, implement, and administer conditional access

Plan and implement security defaults

Managing security can be difficult with common identity-related attacks like password spray, replay, and phishing becoming more popular. Security defaults make it easier to help protect your organization from these attacks with preconfigured security settings:

- Requiring all users to register for Azure AD Multi-Factor Authentication.
- Requiring administrators to do multi-factor authentication.
- Blocking legacy authentication protocols.
- Requiring users to do multi-factor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.

Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You turn on security defaults in the Azure portal. If your tenant was created on or after October 22, 2019, security defaults may be enabled in your tenant. To protect all of our users, security defaults are being rolled out to new tenants at creation**.**

Who's it for?

- Organizations who want to increase their security posture, but don't know how or where to start.
- Organizations using the free tier of Azure Active Directory licensing.

Who should use Conditional Access?

- If you're an organization currently using Conditional Access policies, security defaults are probably not right for you.
- If you're an organization with Azure Active Directory Premium licenses, security defaults are probably not right for you.
- If your organization has complex security requirements, you should consider Conditional Access.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Plan conditional access policies

There are two types of conditional access with Intune: device-based conditional access and app-based conditional access. You need to configure the related compliance policies to drive conditional access compliance at your organization. Conditional access is commonly used to do things like allow or block access to Exchange, control access to the network, or integrate with a Mobile Threat Defense solution.

The information in this article can help you understand how to use the Intune mobile *device* compliance capabilities and the Intune mobile *application* management (MAM) capabilities.

Device-based Conditional Access

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services.

Intune provides device compliance policy capabilities that evaluate the compliance status of the devices. The compliance status is reported to Azure Active Directory that uses it to enforce the Conditional Access policy created in Azure Active Directory when the user tries to access company resources.

Device-based Conditional Access policies for Exchange online and other Microsoft 365 products are configured through the Microsoft Endpoint Manager admin center.

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use

Implement conditional access policy controls and assignments (targeting, applications, and conditions)

Before you can configure Conditional Access, verify the following configurations exist:

- Your Exchange version is **Exchange 2010 SP3 or later**. Exchange server Client Access Server (CAS) array is supported.
- You have installed and use the Exchange ActiveSync on-premises Exchange connector, which connects Intune to on-premises Exchange.

The connector for an on-premises Exchange organization can install on any machine as long as that machine can communicate with the Exchange server.

- The connector supports **Exchange CAS environment**. Intune supports installing the connector on the Exchange CAS server directly. We recommend you install it on a separate computer because of the additional load the connector puts on the server. When configuring the connector, you must set it up to communicate to one of the Exchange CAS servers.
- **Exchange ActiveSync** must be configured with certificate-based authentication, or user credential entry.
- When Conditional Access policies are configured and targeted to a user, before a user can connect to their email, the **device** they use must be:
    - ◊ Either **enrolled** with Intune or is a domain joined PC.
    - ◊ **Registered in Azure Active Directory**. Additionally, the client Exchange ActiveSync ID must be registered with Azure Active Directory.
- Azure AD Device Registration Service (DRS) is activated automatically for Intune and Microsoft 365 customers. Customers who have already deployed the ADFS Device Registration Service don't see registered devices in their on-premises Active Directory. **This does not apply to Windows PCs and devices**.
- **Compliant** with device compliance policies deployed to that device.
- If the device doesn't meet Conditional Access settings, the user is presented with one of the following messages when they sign in:
    - ◊ If the device isn't enrolled with Intune, or isn't registered in Azure Active Directory, a message displays with instructions about how to install the Company Portal app, enroll the device, and activate email. This process also associates the device's Exchange ActiveSync ID with the device record in Azure Active Directory.
    - ◊ If the device isn't compliant, a message displays that directs the user to the Intune Company Portal website, or the Company Portal app. From the company portal, they can find information about the problem and how to remediate it.

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-exchange-create

Testing and troubleshooting conditional access policies

To set up Conditional Access for Android Enterprise Personally-Owned Work Profile devices

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Deploy the Gmail or Nine Work app as **Required**.
3. Select **Devices** > **Configuration profiles** > **Create profile**, enter **Name** and **Description** for the profile.
4. Select **Android enterprise** in **Platform**, select **Email** in **Profile type**.
5. Configure the email profile settings
6. When you're done, select **OK** > **Create** to save your changes.
7. After you create the email profile, assign it to groups.

Set up device-based conditional access.

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-exchange-create

Implement application controls

Cloud apps, actions, and authentication context are key signals in a Conditional Access policy. Conditional Access policies allow administrators to assign controls to specific applications, actions, or authentication context.

- Administrators can choose from the list of applications that include built-in Microsoft applications and any Azure AD integrated applications including gallery, non-gallery, and applications published through Application Proxy.

- Administrators may choose to define policy not based on a cloud application but on a user action like **Register security information** or **Register or join devices**, allowing Conditional Access to enforce controls around those actions.

- Administrators can use authentication context to provide an extra layer of security in applications.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps

Implement session management

Conditional Access App Control uses a reverse proxy architecture and integrates with your IdP. When integrating with Azure AD Conditional Access, you can configure apps to work with Conditional Access App Control with just a few clicks, allowing you to easily and selectively enforce access and session controls on your organization's apps based on any condition in Conditional Access.

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to further refine filters and set actions to be taken on a user. With the access and session policies, you can:

- **Prevent data exfiltration**: You can block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices.
- **Require authentication context**: You can reevaluate Azure AD Conditional Access policies when a sensitive action occurs in the session. For example, require multi-factor authentication on download of a highly confidential file.
- **Protect on download**: Instead of blocking the download of sensitive documents, you can require documents to be labeled and encrypted when you integrate with Microsoft Information Protection. This action ensures the document is protected and user access is restricted in a potentially risky session.
- **Prevent upload of unlabeled files**: Before a sensitive file is uploaded, distributed, and used by others, it's important to make sure that the sensitive file has the label defined by your organization's policy. You can ensure that unlabeled files with sensitive content are blocked from being uploaded until the user classifies the content.
- **Block potential malware**: You can protect your environment from malware by blocking the upload of potentially malicious files. Any file that is uploaded or downloaded can be scanned against Microsoft threat intelligence and blocked instantaneously.
- **Monitor user sessions for compliance**: Risky users are monitored when they sign into apps and their actions are logged from within the session. You can investigate and analyze user behavior to understand where, and under what conditions, session policies should be applied in the future.
- **Block access**: You can granularly block access for specific apps and users depending on several risk factors. For example, you can block them if they're using client certificates as a form of device management.
- **Block custom activities**: Some apps have unique scenarios that carry risk, for example, sending messages with sensitive content in apps like Microsoft Teams or Slack. In these kinds of scenarios, you can scan messages for sensitive content and block them in real time.

How session control works

Creating a session policy with Conditional Access App Control enables you to control user sessions by redirecting the user through a reverse proxy instead of directly to the app. From then on, user requests and responses go through Defender for Cloud Apps rather than directly to the app.

When a session is protected by proxy, all the relevant URLs and cookies are replaced by Defender for Cloud Apps. For example, if the app returns a page with links whose domains end with myapp.com, the link's domain is suffixed with something like *.mcas.ms, as follows:

App URL	Replaced URL
`myapp.com`	`myapp.com.mcas.ms`

This method doesn't require you to install anything on the device making it ideal when monitoring or controlling sessions from unmanaged devices or partner users.

https://docs.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

Manage Azure AD Identity Protection

Implement and manage a user risk policy

Organizations must decide the level of risk they are willing to accept balancing user experience and security posture.

Microsoft's recommendation is to set the user risk policy threshold to **High** and the sign-in risk policy to **Medium and above** and allow self-remediation options. Choosing to block access rather than allowing self-remediation options, like password change and multi-factor authentication, will impact your users and administrators. Weigh this choice when configuring your policies.

Choosing a **High** threshold reduces the number of times a policy is triggered and minimizes the impact to users. However, it excludes **Low** and **Medium** risk detections from the policy, which may not block an attacker from exploiting a compromised identity. Selecting a **Low** threshold introduces more user interrupts.

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Risk remediation

Organizations can choose to block access when risk is detected. Blocking sometimes stops legitimate users from doing what they need to. A better solution is to allow self-remediation using Azure AD Multi-Factor Authentication (MFA) and self-service password reset (SSPR).

- When a user risk policy triggers:
- Administrators can require a secure password reset, requiring Azure AD MFA be done before the user creates a new password with SSPR, resetting the user risk.
- When a sign-in risk policy triggers:

Azure AD MFA can be triggered, allowing to user to prove it is them by using one of their registered authentication methods, resetting the sign-in risk.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection

Implement and manage sign-in risk policy

Sign in risk with Conditional Access

1. Sign in to the **Azure portal** as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to **Azure Active Directory** > **Security** > **Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users and groups**.
   a. Under **Include**, select **All users**.
   b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
   c. Select **Done**.
6. Under **Cloud apps or actions** > **Include**, select **All cloud apps**.
7. Under **Conditions** > **Sign-in risk**, set **Configure** to **Yes**. Under **Select the sign-in risk level this policy will apply to**.
   a. Select **High** and **Medium**.
   b. Select **Done**.

6. Under **Access controls** > **Grant**.
7. Select **Grant access**, **Require multi-factor authentication**.
8. Select **Select**.
9. Confirm your settings and set **Enable policy** to **On**.
10. Select **Create** to create to enable your policy.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection

Implement and manage MFA registration policy

We recommend that you require multifactor authentication (MFA or 2FA) for all your administrators. Multifactor authentication reduces the risk of an attack using a compromised password.

You can require that users complete a multifactor authentication challenge when they sign in. You can also require that users complete a multifactor authentication challenge when they activate a role in Azure Active Directory (Azure AD) Privileged Identity Management (PIM). This way, even if the user didn't complete multifactor authentication when they signed in, they'll be asked to do it by Privileged Identity Management.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-require-mfa

Monitor, investigate and remediate elevated risky users

Administrators may want to simulate risk in their environment in order to accomplish the following items:

- Populate data in the Identity Protection environment by simulating risk detections and vulnerabilities.
- Set up risk-based Conditional Access policies and test the impact of these policies.

This article provides you with steps for simulating the following risk detection types:

- Anonymous IP address (easy)
- Unfamiliar sign-in properties (moderate)
- Atypical travel (difficult)

Other risk detections cannot be simulated in a secure manner.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-simulate-risk

Implement Access Management for Apps (10-15%)

Plan, implement, and monitor the integration of Enterprise Apps for Single Sign-On (SSO)

Implement and configure consent settings

Manage consent to applications and evaluate consent requests Assign roles

Microsoft recommends that you restrict user consent to allow users to consent only for apps from verified publishers, and only for permissions that you select. For apps that don't meet these criteria, the decision-making process will be centralized with your organization's security and identity administrator team.

After you've disabled or restricted user consent, you have several important steps to take to help keep your organization secure as you continue to allow business-critical applications to be used. These steps are crucial to minimize impact on your organization's support team and IT administrators, and to help prevent the use of unmanaged accounts in third-party applications.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-consent-requests

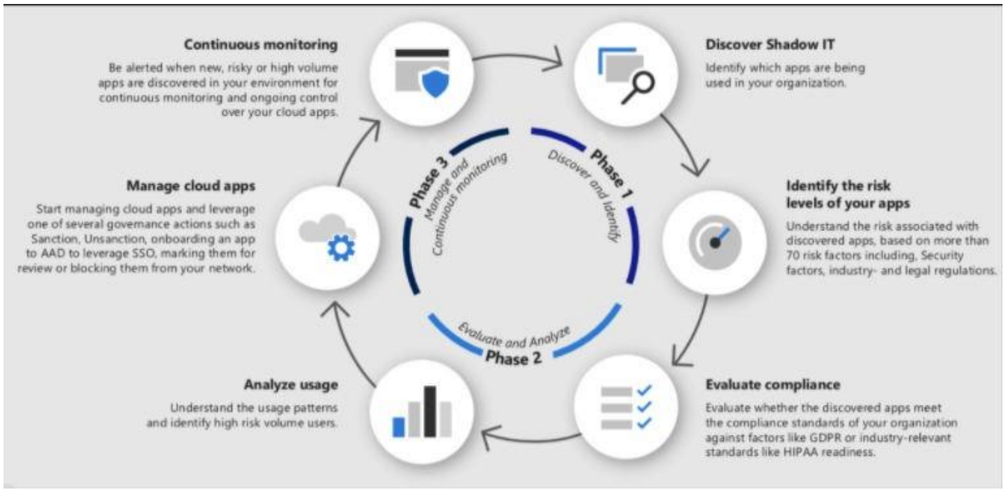
Discover apps by using MCAS or ADFS app report

Discover and manage shadow IT in your network

When IT admins are asked how many cloud apps they think their employees use, on average they say 30 or 40, when in reality, the average is over 1,000 separate apps being used by employees in your organization. Shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed, and may not be compliant with your security and compliance policies. And because your employees are able to access your resources and apps from outside your corporate network, it's no longer enough to have rules and policies on your firewalls.

- ✓ Discover and identify Shadow IT
- ✓ Evaluate and analyze
- ✓ Manage your apps
- ✓ Advanced Shadow IT discovery reporting
- ✓ Control sanctioned apps

Use this process to roll out Shadow IT Cloud Discovery in your organization.



Continuous monitoring

Be alerted when new, risky or high volume apps are discovered in your environment for continuous monitoring and ongoing control over your cloud apps.

Discover Shadow IT

Identify which apps are being used in your organization.

Manage cloud apps

Start managing cloud apps and leverage one of several governance actions such as Sanction, Unsanction, onboarding an app to AAD to leverage SSO, marking them for review or blocking them from your network.

Identify the risk levels of your apps

Understand the risk associated with discovered apps, based on more than 70 risk factors including, Security factors, industry- and legal regulations.

Analyze usage

Understand the usage patterns and identify high risk volume users.

Evaluate compliance

Evaluate whether the discovered apps meet the compliance standards of your organization against factors like GDPR or industry-relevant standards like HIPAA readiness.

https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-shadow-it

Discovered apps with Cloud App Security

Working with discovered apps

The Cloud Discovery dashboard is designed to give you more insight into how cloud apps are being used in your organization. It provides an at-a-glance overview of what kinds of apps are being used, your open alerts, and the risk levels of apps in your organization. It also shows you who your top app users are and provides an App Headquarter location map. The Cloud Discovery Dashboard has many options for filtering the data. Filtering allows you to generate specific views depending on what you're most interested in using easy-to-understand graphics to give you the full picture at a glance.

Review the Cloud Discovery Dashboard

The first thing you should do to get a general picture of your Cloud Discovery apps is review the following information in the Cloud Discovery Dashboard:

1. First look at the overall cloud app use in your organization in the High-level usage overview.

2. Then, dive one level deeper to see which are the top categories used in your org for each of the different use parameters. You can see how much of this usage is by Sanction apps.
3. Go even deeper and see all the apps in a specific category in the Discovered apps tab.
4. You can see the top users and source IP addresses to identify which users are the most dominant users of cloud apps in your organization.
5. Check how the discovered apps spread according to geographic location (according to their HQ) in the App Headquarters map.
6. Finally, don't forget to review the risk score of the discovered app in the App risk overview. Check the discovery alerts status to see how many open alerts should you investigate.

Deep dive into Discovered apps

If you want to deep dive into the data Cloud Discovery provides, use the filters to review which apps are risky and which are commonly used.

For example, if you want to identify commonly used risky cloud storage and collaboration apps, you can use the Discovered apps page to filter for the apps you want. Then you can unsanction or block them as follows:

1. In the Discovered apps page, under Browse by category select both Cloud storage and Collaboration.
2. Then, use the Advanced filters and set Compliance risk factor to SOC 2 equals False
3. For Usage, set Users to greater than 50 users and Usage for Transactions to greater than 100.
4. Set the Security risk factor for Data at rest encryption equals Not supported. Then set Risk score equals 6 or lower.

After the results are filtered, you can unsanction and block them by using the bulk action checkbox to unsanction them all in one action. After they're unsanctioned, you can use a blocking script to block them from being used in your environment.

Cloud Discovery enables you to dive even deeper into your organization's cloud usage. You can identify specific instances that are in use by investigating the discovered subdomains.

For example, you can differentiate between different SharePoint sites.

This is supported only in firewalls and proxies that contain target URL data. For more information, see the list of supported appliances in Supported firewalls and proxies.

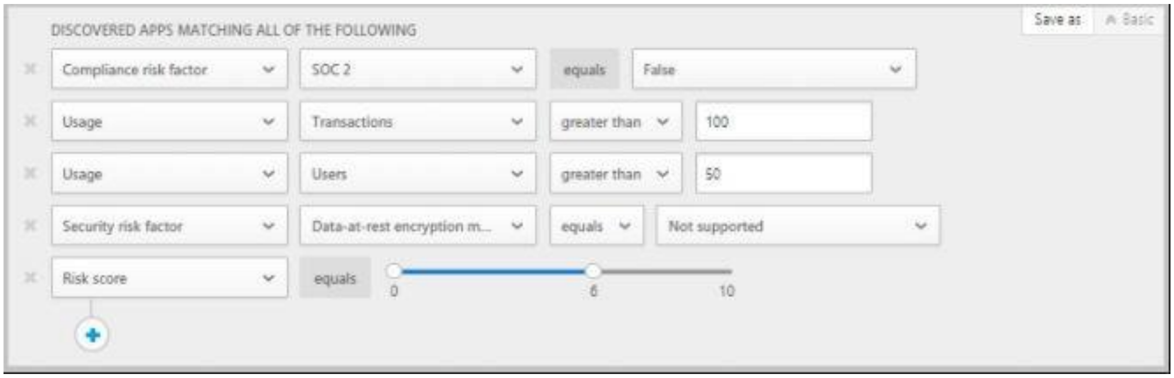
https://docs.microsoft.com/en-us/defender-cloud-apps/discovered-apps

Design and implement access management for apps

App access options

Ongoing access management, usage evaluation, and reporting continue to be a challenge after an app is integrated into your organization's identity system. In many cases, IT Administrators or help desk have to take an ongoing active role in managing access to your apps. Sometimes, assignment is performed by a general or divisional IT team. Often, the assignment decision is intended to be delegated to the business decision maker, requiring their approval before IT makes the assignment.

Other organizations invest in integration with an existing automated identity and access management system, like Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). Both the integration and rule development tend to be specialized and expensive. Monitoring or reporting on either management approach is its own separate, costly, and complex investment.



DISCOVERED APPS MATCHING ALL OF THE FOLLOWING

Compliance risk factor | SOC 2 | equals | False

Usage | Transactions | greater than | 100

Usage | Users | greater than | 50

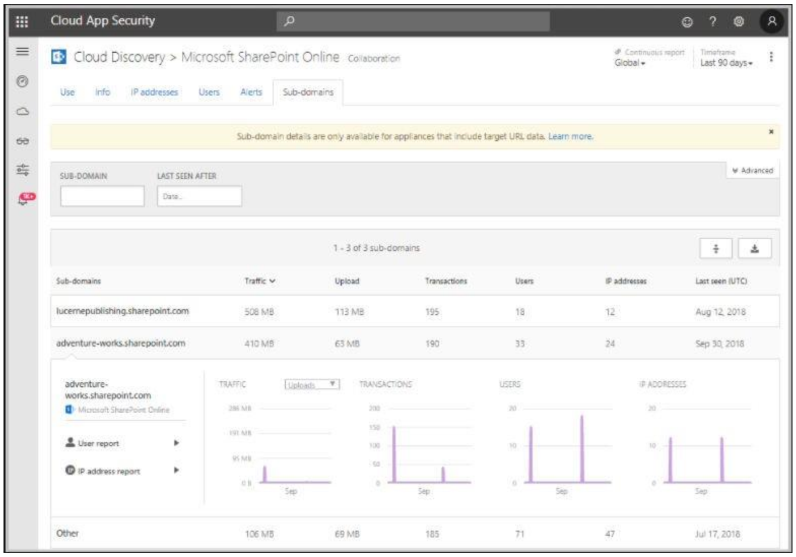
Security risk factor | Data-at-rest encryption m... | equals | Not supported

Risk score | equals | 0 – 6 (0 to 10)

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-access-management

Design and implement app management roles

Enterprise application permissions for custom roles in Azure Active Directory



Sub-domain details are only available for appliances that include target URL data. Learn more.

1 - 3 of 3 sub-domains

Sub-domains	Traffic	Upload	Transactions	Users	IP addresses	Last seen (UTC)
lucernepublishing.sharepoint.com	508 MB	113 MB	195	18	12	Aug 12, 2018
adventure-works.sharepoint.com	410 MB	63 MB	190	33	24	Sep 30, 2018
Other	106 MB	69 MB	185	71	47	Jul 17, 2018

This article contains the currently available enterprise application permissions for custom role definitions in Azure Active Directory (Azure AD). In this article, you'll find permission lists for some common scenarios and the full list of enterprise app permissions.

https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-app-permissions

Monitor and audit access / Sign-ins to Azure Active Directory integrated enterprise applications

Sign-in logs

As an IT administrator, you want to know how your IT environment is doing. The information about your system's health enables you to assess whether and how you need to respond to potential issues.

To support you with this goal, the Azure Active Directory portal gives you access to three activity logs:

Sign-ins – Information about sign-ins and how your resources are used by your users.
Audit – Information about changes applied to your tenant such as users and group management or updates applied to your tenant's resources.
Provisioning – Activities performed by the provisioning service, such as the creation of a group in ServiceNow or a user imported from Workday.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Integrate on-premises apps by using Azure AD application proxy

Application Proxy

Remote access to on-premises applications through Azure AD Application Proxy

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal. For example, Application Proxy can provide remote access and single sign-on to Remote Desktop, SharePoint, Teams, Tableau, Qlik, and line of business (LOB) applications.

Azure AD Application Proxy is:

- **Simple to use**. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don't need to change or update your applications to work with Application Proxy.

- **Secure**. On-premises applications can use Azure's authorization controls and security analytics. For example, on-premises applications can use Conditional Access and two-step verification. Application Proxy doesn't require you to open inbound connections through your firewall.

- **Cost-effective**. On-premises solutions typically require you to set up and maintain demilitarized zones (DMZs), edge servers, or other complex infrastructures. Application Proxy runs in the cloud, which makes it easy to use. To use Application Proxy, you don't need to change the network infrastructure or install additional appliances in your on-premises environment.

What is Application Proxy?

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. Azure AD, the Application Proxy service, and the Application Proxy connector work together to securely pass the user sign-on token from Azure AD to the web application.

Application Proxy works with:

- Web applications that use Integrated Windows authentication for authentication
- Web applications that use form-based or header-based access
- Web APIs that you want to expose to rich applications on different devices

- Applications hosted behind a Remote Desktop Gateway
- Rich client apps that are integrated with the Microsoft Authentication Library (MSAL)

Application Proxy supports single sign-on. For more information on supported methods, see Choosing a single sign-on method.

Application Proxy is recommended for giving remote users access to internal resources. Application Proxy replaces the need for a VPN or reverse proxy. It is not intended for internal users on the corporate network. These users who unnecessarily use Application Proxy can introduce unexpected and undesirable performance issues.

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

Integrate custom SaaS apps for SSO

Add an app

Quickstart: Add an enterprise application

In this quickstart, you use the Azure Active Directory Admin Center to add an enterprise application to your Azure Active Directory (Azure AD) tenant. Azure AD has a gallery that contains thousands of enterprise applications that have been pre-integrated. Many of the applications your organization uses are probably already in the gallery. This quickstart uses the application named Azure AD SAML Toolkit as an example, but the concepts apply for most enterprise applications in the gallery.

It is recommended that you use a non-production environment to test the steps in this quickstart.

Prerequisites

To add an enterprise application to your Azure AD tenant, you need:

An Azure AD user account. If you don't already have one, you can Create an account for free. One of the following roles: Global Administrator, Cloud Application Administrator, or Application Administrator.

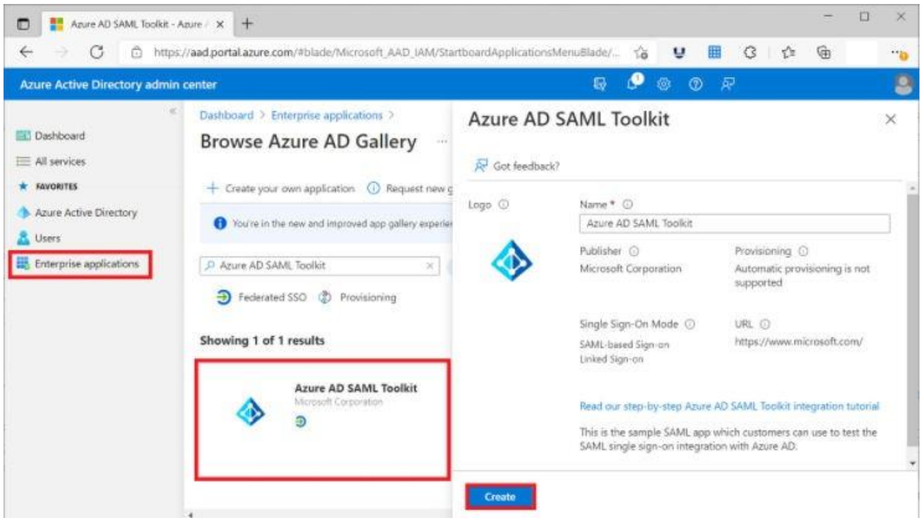
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal

Configure pre-integrated (gallery) SaaS apps

Add an enterprise application

To add an enterprise application to your tenant:

1. Go to the Azure Active Directory Admin Center and sign in using one of the roles listed in the prerequisites.
2. In the left menu, select Enterprise applications. The All applications pane opens and displays a list of the applications in your Azure AD tenant.
3. In the Enterprise applications pane, select New application.
4. The Browse Azure AD Gallery pane opens and displays tiles for cloud platforms, on-premises applications, and featured applications. Applications listed in the Featured applications section have icons indicating whether they support federated single sign-on (SSO) and provisioning. Search for and select the application. In this quickstart, Azure AD SAML Toolkit is being used.


Azure AD SAML Toolkit - Azure
https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/...
Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Enterprise applications >
Browse Azure AD Gallery
Create your own application
Request new g
You're in the new and improved app gallery experie
Federated SSO
Provisioning
Azure AD SAML Toolkit
Microsoft Corporation
Got feedback?
Create

Search: Azure AD SAML Toolkit

Showing 1 of 1 results

Azure AD SAML Toolkit

Logo

Name *: Azure AD SAML Toolkit

Publisher: Microsoft Corporation

Provisioning: Automatic provisioning is not supported

Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: https://www.microsoft.com/

Read our step-by-step Azure AD SAML Toolkit integration tutorial

This is the sample SAML app which customers can use to test the SAML single sign-on integration with Azure AD.

5.Enter a name that you want to use to recognize the instance of the application. For example, Azure AD SAML Toolkit 1.

6.Select **Create**.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal

Implement application user provisioning

SaaS application tutorials

Tutorials for integrating SaaS applications with Azure Active Directory
To help integrate your cloud-enabled software as a service (SaaS) applications with Azure Active Directory, we have developed a collection of tutorials that walk you through configuration.

For a list of all SaaS apps that have been pre-integrated into Azure AD, see the Active Directory Marketplace.

Use the application network portal to request a SCIM enabled application to be added to the gallery for automatic provisioning or a SAML / OIDC enabled application to be added to the gallery for SSO.

https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/tutorial-list

Implement app registrations

Plan your line of business application registration strategy

Register app or web API

Register an application with the Microsoft identity platform

Get started with the Microsoft identity platform by registering an application in the Azure portal.

The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Whether it's a client application like a web or mobile app, or it's a web API that backs a client app, registering it establishes a trust relationship between your application and the identity provider, the Microsoft identity platform.

Prerequisites

- An Azure account that has an active subscription. Create an account for free.
- The Azure account must have permission to manage applications in Azure Active Directory

(Azure AD). Any of the following Azure AD roles include the required permissions:

- ∗ Application administrator
- ∗ Application developer
- ∗ Cloud application administrator
- Completion of the Set up a tenant quickstart.

Register an application

Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around.

Follow these steps to create the app registration:

1.Sign in to the Azure portal.

2.If you have access to multiple tenants, use the Directories + subscriptions filter in the top menu to switch to the tenant in which you want to register the application.

3.Search for and select Azure Active Directory.

4.Under Manage, select App registrations > New registration.

5.Enter a display **Name** for your application. Users of your application might see the display name when they use the app, for example during sign-in. You can change the display name at any time and multiple app registrations can share the same name. The app registration's automatically generated Application (client) ID, not its display name, uniquely identifies your app within the identity platform.

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

7.Don't enter anything for Redirect URI (optional). You'll configure a redirect URI in the next section.

Select Register to complete the initial app registration.

When registration finishes, the Azure portal displays the app registration's Overview pane. You see the Application (client) ID. Also called the *client ID*, this value uniquely identifies your application in the Microsoft identity platform.

Your application's code, or more typically an authentication library used in your application, also uses the client ID. The ID is used as part of validating the security tokens it receives from the identity platform.

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Implement application registrations

App scenarios and authentication flows

The Microsoft identity platform supports authentication for different kinds of modern application architectures. All of the architectures are based on the industry-standard protocols OAuth 2.0 and OpenID Connect. By using the authentication libraries for the Microsoft identity platform, applications authenticate identities and acquire tokens to access protected APIs.

This article describes authentication flows and the application scenarios that they're used in.

Application scenarios

The Microsoft identity platform supports authentication for these app architectures:

- Single-page apps
- Web apps
- Web APIs
- Mobile apps
- Native apps
- Daemon apps
- Server-side apps

Applications use the different authentication flows to sign in users and get tokens to call protected APIs.

Scenarios and supported authentication flows

You use authentication flows to implement the application scenarios that are requesting tokens. There isn't a one-to-one mapping between application scenarios and authentication flows.

Scenarios that involve acquiring tokens also map to OAuth 2.0 authentication flows. For more information, see OAuth 2.0 and OpenID Connect protocols on the Microsoft identity platform.

https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-flows- app-scenarios

Configure application permissions

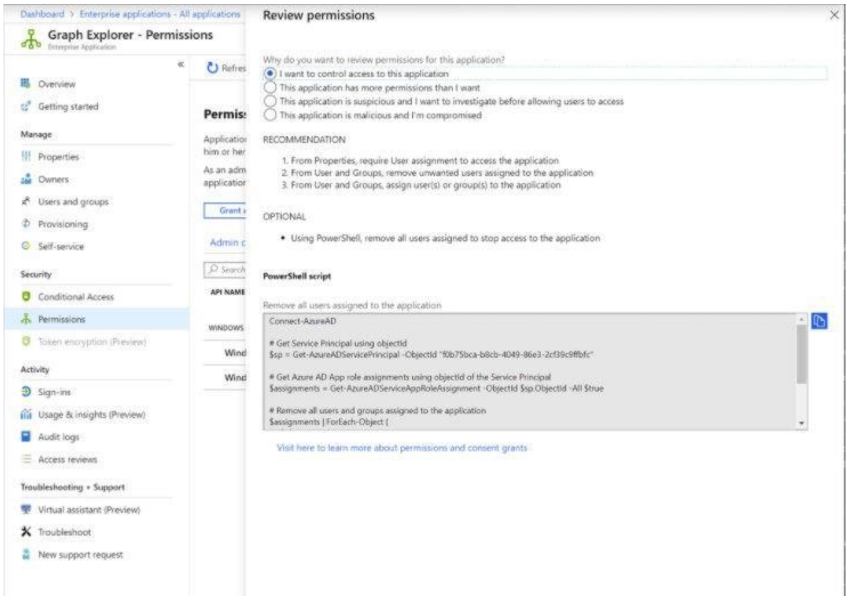
Review permissions granted to apps

In this article you'll learn how to review permissions granted to applications in your Azure Active Directory (Azure AD) tenant. You may need to review permissions when you have detected a malicious application or the application has been granted more permissions than is necessary.

The steps in this article apply to all applications that were added to your Azure Active Directory (Azure AD) tenant via user or admin consent. For more information on consenting to applications, see Azure Active Directory consent framework.

To review application permissions:

1. Sign in to the Azure portal using one of the roles listed in the prerequisites section.
2. Select Azure Active Directory, and then select Enterprise applications.
3. Select the application that you want to restrict access to.
4. Select Permissions. In the command bar, select Review permissions.



Review permissions

Why do you want to review permissions for this application?

● I want to control access to this application
○ This application has more permissions than I want
○ This application is suspicious and I want to investigate before allowing users to access
○ This application is malicious and I'm compromised

RECOMMENDATION

1. From Properties, require User assignment to access the application
2. From User and Groups, remove unwanted users assigned to the application
3. From User and Groups, assign user(s) or group(s) to the application

OPTIONAL

- Using PowerShell, remove all users assigned to stop access to the application

PowerShell script

Remove all users assigned to the application

```
Connect-AzureAD

# Get Service Principal using objectId
$sp = Get-AzureADServicePrincipal -ObjectId "f0b75bca-b8cb-4049-86e3-2cf39c9ffbfc"

# Get Azure AD App role assignments using objectId of the Service Principal
$assignments = Get-AzureADServiceAppRoleAssignment -ObjectId $sp.ObjectId -All $true

# Remove all users and groups assigned to the application
$assignments | ForEach-Object {
```

Visit here to learn more about permissions and consent grants

5. Give a reason for why you want to review permissions for the application by selecting any of the options listed after the question , Why do you want to review permissions for this application?

Each option generates PowerShell scripts that enable you to control user access to the application and to review permissions granted to the application. For information about how to control user access to an application, see How to remove a user's access to an application.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-application-permissions

Implement application authorization

Authentication vs. authorization

This article defines authentication and authorization. It also briefly covers how you can use the Microsoft identity platform to authenticate and authorize users in your web apps, web APIs, or apps that call protected web APIs. If you see a term you aren't familiar with, try our glossary or our Microsoft identity platform videos, which cover basic concepts.

Authentication

Authentication is the process of proving that you are who you say you are. It's sometimes shortened to *AuthN*. The Microsoft identity platform uses the OpenID Connect protocol for handling authentication.

Authorization

A*uthorization* is the act of granting an authenticated party permission to do something. It specifies what data you're allowed to access and what you can do with that data. Authorization is sometimes shortened to *AuthZ*. The Microsoft identity platform uses the OAuth 2.0 protocol for handling authorization.

Authentication and authorization using the Microsoft identity platform

Creating apps that each maintain their own username and password information incurs a high administrative burden when adding or removing users across multiple apps. Instead, your apps can delegate that responsibility to a centralized identity provider.

Azure Active Directory (Azure AD) is a centralized identity provider in the cloud. Delegating authentication and authorization to it enables scenarios such as:

- Conditional Access policies that require a user to be in a specific location.
- The use of multi-factor authentication, which is sometimes called two-factor authentication or 2FA.
- Enabling a user to sign in once and then be automatically signed in to all of the web apps that share the same centralized directory. This capability is called *single sign-on (SSO)*.

The Microsoft identity platform simplifies authorization and authentication for application developers by providing identity as a service. It supports industry-standard protocols and open -source libraries for different platforms to help you start coding quickly. It allows developers to build applications that sign in all Microsoft identities, get tokens to call Microsoft Graph, access Microsoft APIs, or access other APIs that developers have built.

Here's a comparison of the protocols that the Microsoft identity platform uses:

- **OAuth versus OpenID Connect**: The platform uses OAuth for authorization and OpenID Connect (OIDC) for authentication. OpenID Connect is built on top of OAuth 2.0, so the terminology and flow are similar between the two. You can even both authenticate a user (through OpenID Connect) and get authorization to access a protected resource that the user owns (through OAuth 2.0) in one request. For more information, see OAuth 2.0 and OpenID Connect protocols and OpenID Connect protocol.

- **OAuth versus SAML**: The platform uses OAuth 2.0 for authorization and SAML for authentication. For more information on how to use these protocols together to both authenticate a user and get authorization to access a protected resource, see Microsoft identity platform and OAuth 2.0 SAML bearer assertion flow.

- **OpenID Connect versus SAML**: The platform uses both OpenID Connect and SAML to authenticate a user and enable single sign-on. SAML authentication is commonly used with identity providers such as Active Directory Federation Services (AD FS) federated to Azure AD, so it's often used in enterprise applications. OpenID Connect is commonly used for apps that are purely in the cloud, such as mobile apps, websites, and web APIs.

https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization

Plan and configure multi-tier application permissions

Single tenant and multi-tenant apps

Tenancy in Azure Active Directory

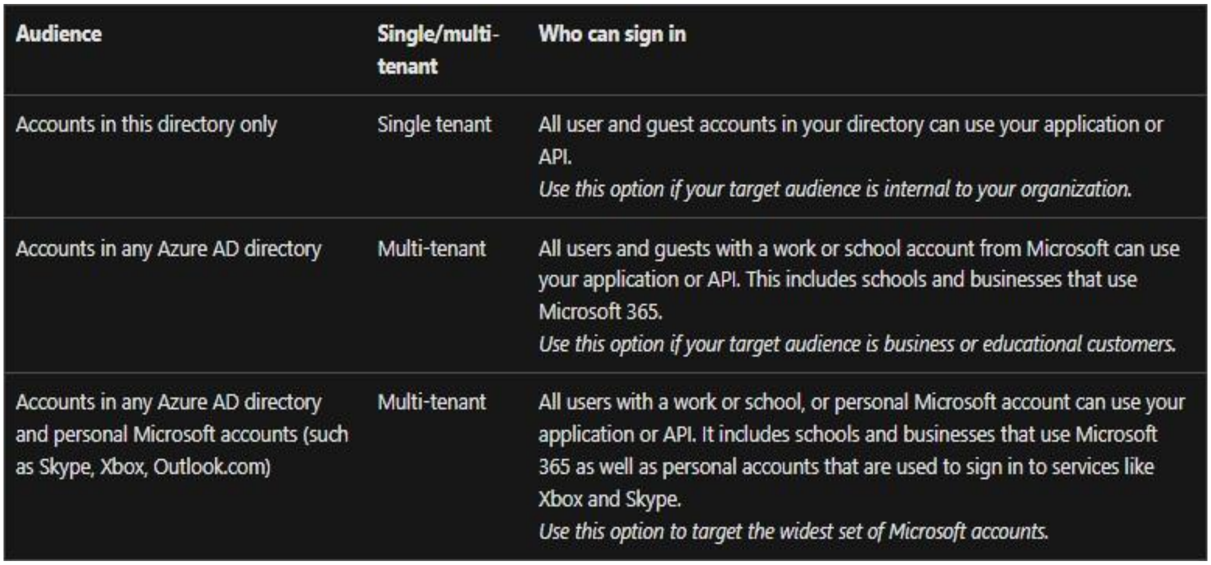
Azure Active Directory (Azure AD) organizes objects like users and apps into groups called *tenants*. Tenants allow an administrator to set policies on the users within the organization and the apps that the organization owns to meet their security and operational policies.

Who can sign in to your app?

When it comes to developing apps, developers can choose to configure their app to be either single-tenant or multi-tenant during app registration in the Azure portal.

- Single-tenant apps are only available in the tenant they were registered in, also known as their home tenant.
- Multi-tenant apps are available to users in both their home tenant and other tenants.

In the Azure portal, you can configure your app to be single-tenant or multi-tenant by setting the audience as follows.



Audience	Single/multi-tenant	Who can sign in
Accounts in this directory only	Single tenant	All user and guest accounts in your directory can use your application or API. *Use this option if your target audience is internal to your organization.*
Accounts in any Azure AD directory	Multi-tenant	All users and guests with a work or school account from Microsoft can use your application or API. This includes schools and businesses that use Microsoft 365. *Use this option if your target audience is business or educational customers.*
Accounts in any Azure AD directory and personal Microsoft accounts (such as Skype, Xbox, Outlook.com)	Multi-tenant	All users with a work or school, or personal Microsoft account can use your application or API. It includes schools and businesses that use Microsoft 365 as well as personal accounts that are used to sign in to services like Xbox and Skype. *Use this option to target the widest set of Microsoft accounts.*

Best practices for multi-tenant apps

Building great multi-tenant apps can be challenging because of the number of different policies that IT administrators can set in their tenants. If you choose to build a multi-tenant app, follow these best practices:

- Test your app in a tenant that has configured Conditional Access policies.
- Follow the principle of least user access to ensure that your app only requests permissions it actually needs.
- Provide appropriate names and descriptions for any permissions you expose as part of your app. This helps users and admins know what they're agreeing to when they attempt to use your app's APIs. For more information, see the best practices section in the permissions guide.

https://docs.microsoft.com/en-us/azure/active-directory/develop/single-and-multi-tenant-apps

Plan and implement an Identity Governance Strategy (25-30)

Plan and implement entitlement management

Define catalogs

Create and manage a catalog of resources in Azure AD entitlement management.

This article shows you how to create and manage a catalog of resources and access packages in Azure Active Directory (Azure AD) entitlement management.

Create a catalog

A catalog is a container of resources and access packages. You create a catalog when you want to group related resources and access packages. Whoever creates the catalog becomes the first catalog owner. A catalog owner can add more catalog owners.

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-catalog-create

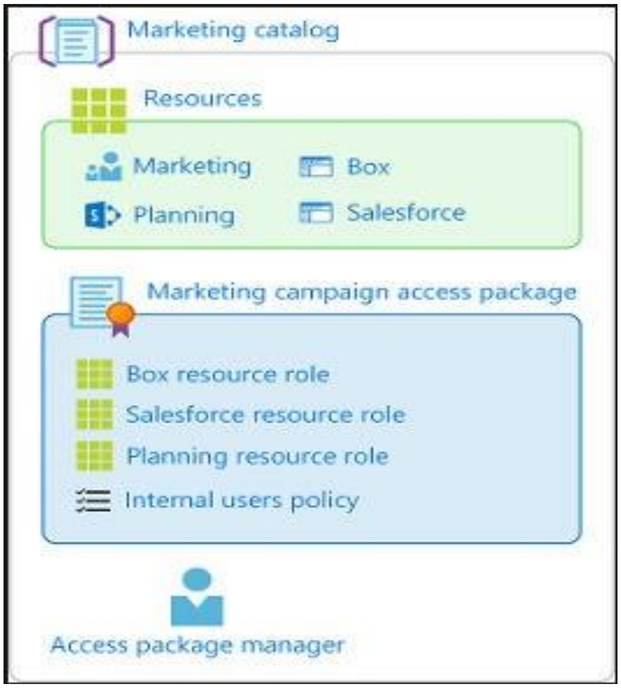
Define access packages

An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package. This article describes how to create a new access package.

All access packages must be put in a container called a catalog. A catalog defines what resources you can add to your access package. If you don't specify a catalog, your access package will be put into the General catalog. Currently, you can't move an existing access package to a different catalog.

If you are an access package manager, you cannot add resources you own to a catalog. You are restricted to using the resources available in the catalog. If you need to add resources to a catalog, you can ask the catalog owner.

All access packages must have at least one policy. Policies specify who can request the access package and also approval and lifecycle settings. When you create a new access package, you can create an initial policy for users in your directory, for users not in your directory, for administrator direct assignments only, or you can choose to create the policy later.



https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

Plan, implement and manage entitlements

Common scenarios in Azure AD entitlement management

There are several ways that you can configure entitlement management for your organization. However, if you're just getting started, it's helpful to understand the common scenarios for administrators, catalog owners, access package managers, approvers, and requestors.

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-scenarios

Implement and manage terms of use

Require terms of use

Azure AD terms of use policies provide a simple method that organizations can use to present information to end users. This presentation ensures users see relevant disclaimers for legal or compliance requirements.

What can I do with terms of use?

- Require employees or guests to accept your terms of use policy before getting access.
- Require employees or guests to accept your terms of use policy on every device before getting access.
- Require employees or guests to accept your terms of use policy on a recurring schedule.
- Require employees or guests to accept your terms of use policy before registering security information in Azure AD Multi-Factor Authentication (MFA).
- Require employees to accept your terms of use policy before registering security information in Azure AD self-service password reset (SSPR).
- Present a general terms of use policy for all users in your organization.
- Present specific terms of use policies based on a user attributes (such as doctors versus nurses, or domestic versus international employees) by using dynamic groups).
- Present specific terms of use policies when accessing high business impact applications, like Salesforce.
- Present terms of use policies in different languages.
- List who has or hasn't accepted to your terms of use policies.
- Help meeting privacy regulations.
- Display a log of terms of use policy activity for compliance and audit.
- Create and manage terms of use policies using Microsoft Graph APIs.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

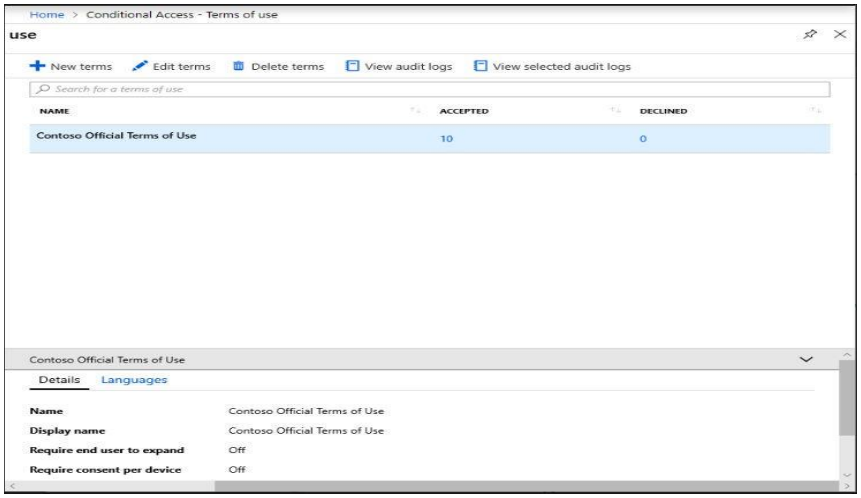
Manage the lifecycle of external users in Azure AD Identity Governance settings

Review and remove users from external organizations

View report of who has accepted and declined

The Terms of use blade shows a count of the users who have accepted and declined. These counts and who accepted/declined are stored for the life of the terms of use policy.

1. Sign in to Azure and navigate to **Terms of use** at https://aka.ms/catou.

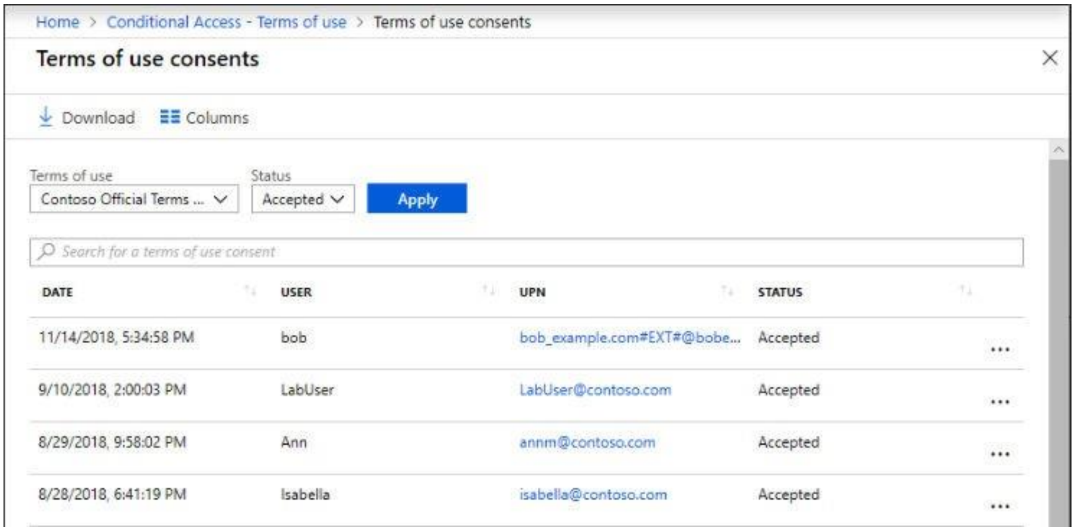

Home > Conditional Access - Terms of use
use
New terms
Edit terms
Delete terms
View audit logs
View selected audit logs
Search for a terms of use

NAME	ACCEPTED	DECLINED
Contoso Official Terms of Use	10	0

Contoso Official Terms of Use
Details
Languages

Name	Contoso Official Terms of Use
Display name	Contoso Official Terms of Use
Require end user to expand	Off
Require consent per device	Off

2. For a terms of use policy, click the numbers under **Accepted** or **Declined** to view the current state for users.

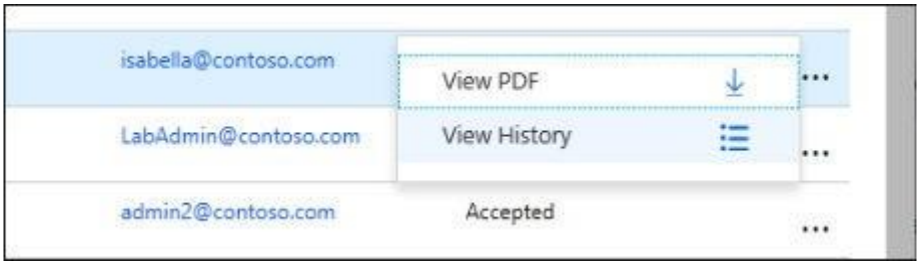

Home > Conditional Access - Terms of use > Terms of use consents
Terms of use consents
Download
Columns

Terms of use: Contoso Official Terms ...
Status: Accepted

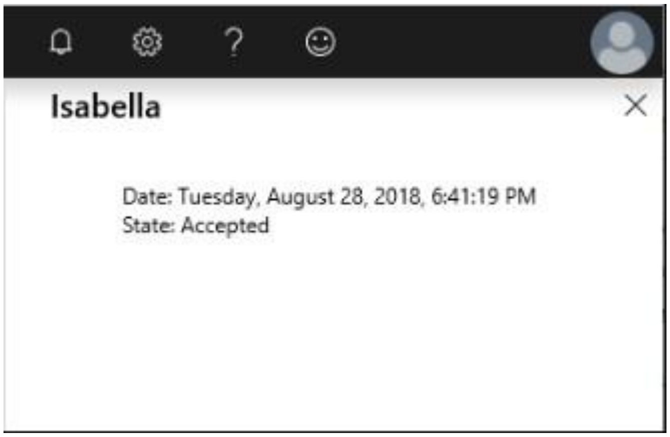
Apply
Search for a terms of use consent

DATE	USER	UPN	STATUS
11/14/2018, 5:34:58 PM	bob	bob_example.com#EXT#@bobe...	Accepted
9/10/2018, 2:00:03 PM	LabUser	LabUser@contoso.com	Accepted
8/29/2018, 9:58:02 PM	Ann	annm@contoso.com	Accepted
8/28/2018, 6:41:19 PM	Isabella	isabella@contoso.com	Accepted

3. To view the history for an individual user, click the ellipsis (**...**) and then View History.



In the view history pane, you see a history of all the accepts, declines, and expirations.


Isabella

Date: Tuesday, August 28, 2018, 6:41:19 PM
State: Accepted

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

Plan, implement, and manage access reviews

Plan for access reviews

Plan an Azure Active Directory access reviews deployment

Azure Active Directory (Azure AD) access reviews help your organization keep the network more secure by managing its resource access lifecycle. With access reviews, you can:

- Schedule regular reviews or do ad-hoc reviews to see who has access to specific resources, such as applications and groups.
- Track reviews for insights, compliance, or policy reasons.
- Delegate reviews to specific admins, business owners, or users who can self-attest to the need for continued access.
- Use the insights to efficiently determine if users should continue to have access.
- Automate review outcomes, such as removing users' access to resources.

Access reviews are an Azure AD Identity Governance capability. The other capabilities are entitlement management, Privileged Identity Management (PIM), and terms of use. Together, they help you address these four questions:

- Which users should have access to which resources?
- What are those users doing with that access?
- Is there effective organizational control for managing access?
- Can auditors verify that the controls are working?

Planning your access reviews deployment is essential to make sure you achieve your desired governance strategy for users in your organization.

https://docs.microsoft.com/en-us/azure/active-directory/governance/deploy-access- reviews

Create access reviews for groups and apps

Create an access review of an access package in Azure AD entitlement management

To reduce the risk of stale access, you should enable periodic reviews of users who have active assignments to an access package in Azure AD entitlement management. You can enable reviews when you create a new access package or edit an existing access package. This article describes how to enable access reviews of access packages.

Create an access review of an access package

You can enable access reviews when creating a new access package or editing an existing access package policy. Follow these steps to enable access reviews of an access package:

1. Open the Lifecycle tab for an access package to specify when a user's assignment to the access package expires. You can also specify whether users can extend their assignments.
2. In the Expiration section, set Access package assignments expires to On date, Number of days, Number of hours, or Never.

For On date, select an expiration date in the future.

For Number of days, specify a number between 0 and 3660 days.

For Number of hours, specify a number of hours.

Based on your selection, a user's assignment to the access package expires on a certain date, a certain number of days after they are approved, or never.

3. Click Show advanced expiration settings to show additional settings.

4. To allow user to extend their assignments, set Allow users to extend access to Yes.

5. To require approval to grant an extension, set Require approval to grant extension to Yes. The same approval settings that were specified on the Requests tab will be used.

6. Next, move the Require access reviews toggle to Yes.

7. Specify the date the reviews will start next to Starting on.

8. Next, set the Review frequency to Annually, Bi-annually, Quarterly or Monthly. This setting determines how often access reviews will occur.

9. Set the Duration to define how many days each review of the recurring series will be open for input from reviewers. For example, you might schedule an annual review that starts on January 1st and is open for review for 30 days so that reviewers have until the end of the month to respond.

10. Next to Reviewers, select Self-review if you want users to perform their own access review or select Specific reviewer(s) if you want to designate a reviewer. You can also select Manager if you want to designate the reviewee’s manager to be the reviewer. If you select this option, you need to add a fallback to forward the review to in case the manager cannot be found in the system.

11. If you selected Specific reviewer(s), specify which users will do the access review

12. If you selected Manager, specify the fallback reviewer

13. There are other advanced settings you can configure. To configure other advanced access review settings, click Show advanced access review settings

14. Click Review + Create or click next if you are creating a new access package. Click Update if you are editing an access package, at the bottom of the page.

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-reviews-create

Monitor access review findings

Review access

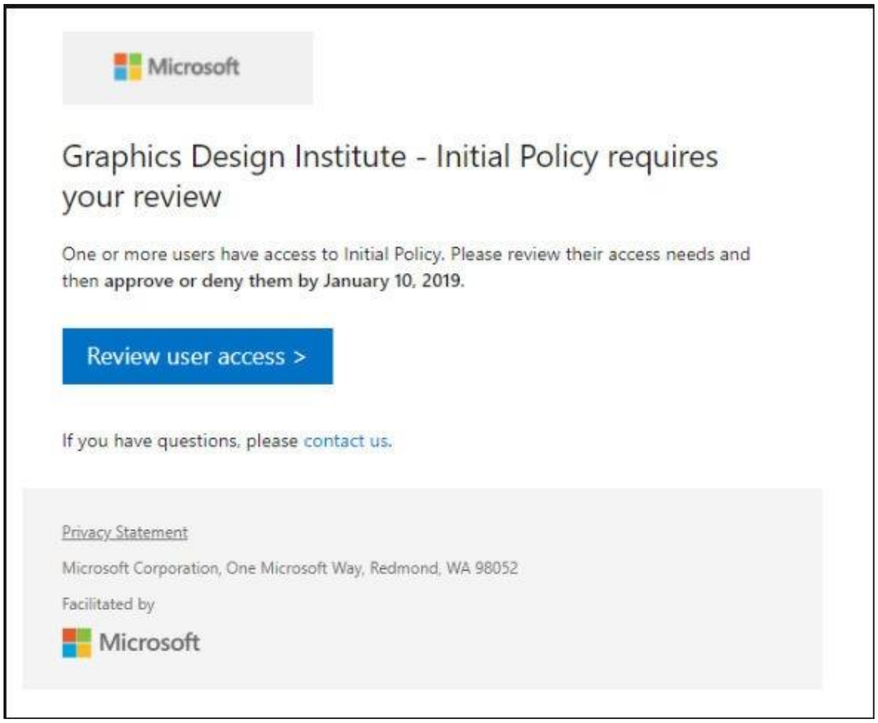
Review access of an access package in Azure AD entitlement management

Azure AD entitlement management simplifies how enterprises manage access to groups, applications, and SharePoint sites. This article describes how to perform access reviews for other users that are assigned to an access package as a designated reviewer.

Open the access review

Use the following steps to find and open the access review:

1. You may receive an email from Microsoft that asks you to review access. Locate the email to open the access review. Here is an example email to review access:



Microsoft

Graphics Design Institute - Initial Policy requires your review

One or more users have access to Initial Policy. Please review their access needs and then **approve or deny them by January 10, 2019.**

Review user access >

If you have questions, please contact us.

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

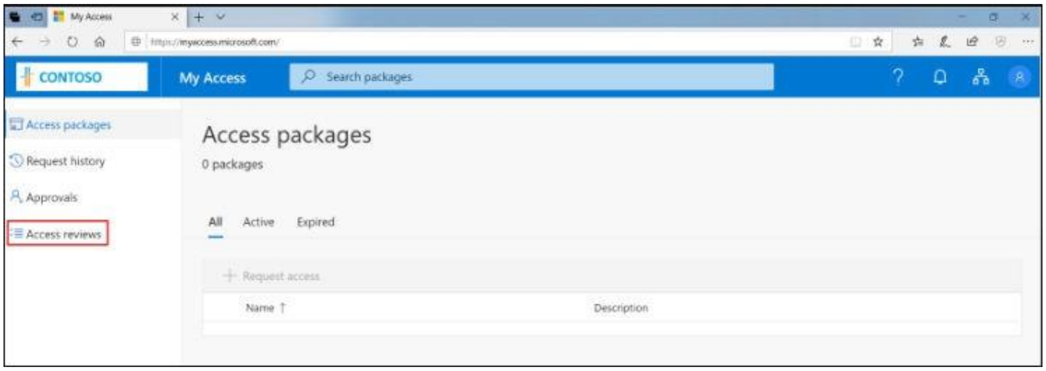
Facilitated by

Microsoft

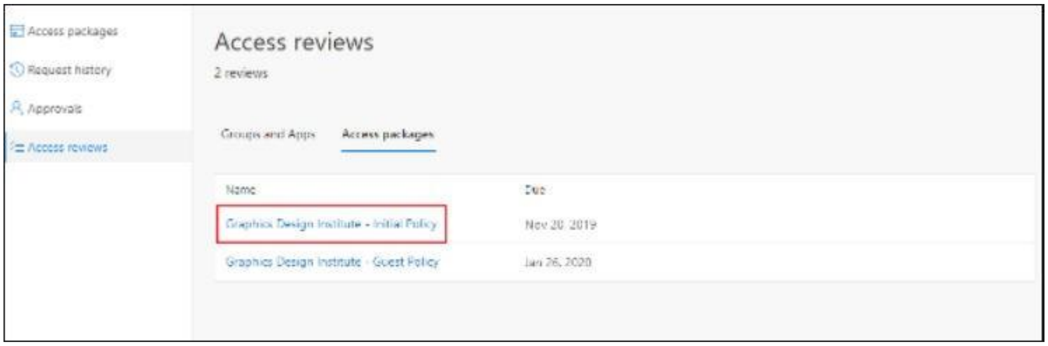
2. Click the Review user access link to open the access review.

3. If you don't have the email, you can find your pending access reviews by navigating directly to https://myaccess.microsoft.com. (For US Government, use https://myaccess.microsoft.us instead.)

4. Click Access reviews on the left navigation bar to see a list of pending access reviews assigned to you.



5. Click the review that you'd like to begin.



Name	Due
Graphics Design Institute - Initial Policy	Nov 20, 2019
Graphics Design Institute - Guest Policy	Jan 26, 2020

Perform the access review

Once you open the access review, you will see the names of users for which you need to review. There are two ways that you can approve or deny access:

- You can manually approve or deny access for one or more users
- You can accept the system recommendations

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-reviews-review-access?WT.mc_id=ES-MVP-4039827

Manage licenses for access reviews

License requirements

Using this feature requires an Azure AD Premium P2 license. To find the right license for your requirements, see Compare generally available features of Azure AD.

How many licenses must you have?

Your directory needs at least as many Azure AD Premium P2 licenses as the number of employees who will be performing the following tasks:

- Member users who are assigned as reviewers
- Member users who perform a self-review
- Member users as group owners who perform an access review
- Member users as application owners who perform an access review

For guest users, licensing needs will depend on the licensing model you're using. However, the below guest users' activities are considered Azure AD Premium P2 usage:

- Guest users who are assigned as reviewers
- Guest users who perform a self-review
- Guest users as group owners who perform an access review
- Guest users as application owners who perform an access review

Azure AD Premium P2 licenses are not required for users with the Global Administrator or User Administrator roles who set up access reviews, configure settings, or apply the decisions from the reviews.

Azure AD guest user access is based on a monthly active users (MAU) billing model, which replaces the 1:5 ratio billing model. For more information, see Azure AD External Identities pricing.

For more information about licenses, see Assign or remove licenses using the Azure Active Directory portal.

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Automate access review management tasks

Access reviews

Azure AD access reviews

Use Azure AD access reviews to configure one-time or recurring access reviews for attestation of users' rights to access Azure AD resources. These Azure AD resources include groups, service principals, access packages, and privileged roles.

Typical customer scenarios for access reviews include:

- Customers can review and certify guest user access to groups through group memberships. Reviewers can use the insights that are provided to efficiently decide whether guests should have continued access.
- Customers can review and certify employee access to Azure AD resources.
- Customers can review and audit assignments to Azure AD privileged roles. This supports organizations in the management of privileged access.

Note that the access reviews feature, including the API, is included in Azure AD Premium P2. The tenant where an access review is being created must have a valid purchased or trial Azure AD Premium P2 or EMS E5 subscription. For more information about the license requirements, see Access reviews license requirements.

https://docs.microsoft.com/en-us/graph/api/resources/accessreviewsv2-overview?view=graph-rest-beta

Configure recurring access reviews

Automate actions based on Access Reviews

You can choose to have access removal automated by setting the Auto apply results to resource option to Enable.

After the review is finished and has ended, users who weren't approved by the reviewer will be automatically removed from the resource or kept with continued access. Options could mean removing their group membership or their application assignment or revoking their right to elevate to a privileged role.

https://docs.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews

Plan and implement privileged access

Define a privileged access strategy for administrative users (resources, roles, approvals, thresholds)

Deploy PIM

Plan a Privileged Identity Management deployment

Privileged Identity Management (PIM) provides a time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions to important resources. These resources include resources in Azure Active Directory (Azure AD), Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

PIM enables you to allow a specific set of actions at a particular scope. Key features include:

- Provide just-in-time privileged access to resources
- Assign eligibility for membership or ownership of privileged access groups
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multifactor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit

To gain the most from this deployment plan, it’s important that you get a complete overview of What is Privileged Identity Management.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

Configure Privileged Identity Management for Azure AD roles

Management capabilities for Azure AD roles in Privileged Identity Management

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. The following video introduces you to important PIM concepts and features.

Who can do what?

For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged Role

Administrator or Global Administrator role can manage assignments for other administrators. Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.

For Azure resource roles in Privileged Identity Management, only a subscription administrator, a resource Owner, or a resource User Access administrator can manage assignments for other administrators. Users who are Privileged Role Administrators, Security Administrators, or Security Readers do not by default have access to view assignments to Azure resource roles in Privileged Identity Management.

What does it do?

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit
- Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments

Managing privileged access Azure AD groups (preview)

In Privileged Identity Management (PIM), you can now assign eligibility for membership or ownership of privileged access groups. Starting with this preview, you can assign Azure Active Directory (Azure AD) built-in roles to cloud groups and use PIM to manage group member and owner eligibility and activation. For more information about role-assignable groups in Azure AD, see Use Azure AD groups to manage role assignments.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Configure Privileged Identity Management for Azure resources

Discover Azure resources

Discover Azure resources to manage in Privileged Identity Management

Using Azure Active Directory (Azure AD) Privileged Identity Management (PIM), you can improve the protection of your Azure resources. This is helpful to:

- Organizations that already use Privileged Identity Management to protect Azure AD roles
- Management group and subscription owners who are trying to secure production resources

When you first set up Privileged Identity Management for Azure resources, you need to discover and select the resources you want to protect with Privileged Identity Management. When you discover resources through Privileged Identity Management, PIM creates the PIM service principal (MS-PIM) assigned as User Access Administrator on the resource. There's no limit to the number of resources that you can manage with Privileged Identity Management. However, we recommend starting with your most critical production resources.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-discover-resources

Assign roles

Assign Azure AD roles in Privileged Identity Management

With Azure Active Directory (Azure AD), a Global administrator can make permanent Azure AD admin role assignments. These role assignments can be created using the Azure portal or using PowerShell commands.

The Azure AD Privileged Identity Management (PIM) service also allows Privileged role administrators to make permanent admin role assignments. Additionally, Privileged role administrators can make users eligible for Azure AD admin roles. An eligible administrator can activate the role when they need it, and then their permissions expire once they're done.

Privileged Identity Management support both built-in and custom Azure AD roles. .

When a role is assigned, the assignment:

- Can't be asigned for a duration of less than five minutes
- Can't be removed within five minutes of it being assigned

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

Assign Azure resource roles in Privileged Identity Management

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) can manage the built-in Azure resource roles, as well as custom roles, including (but not limited to):

- Owner
- User Access Administrator
- Contributor
- Security Admin
- Security Manager

Users or members of a group assigned to the Owner or User Access Administrator subscription roles, and Azure AD Global administrators that enable subscription management in Azure AD have Resource administrator permissions by default. These administrators can assign roles, configure role settings, and review access using Privileged Identity Management for Azure resources. A user can't manage Privileged Identity Management for Resources without Resource administrator permissions. View the list of Azure built-in roles.

Privileged Identity Management support both built-in and custom Azure roles. For more information on Azure custom roles, see Azure custom roles.

Role assignment conditions

You can use the Azure attribute-based access control (Azure ABAC) preview to place resource conditions on eligible role assignments using Privileged Identity Management (PIM). With PIM, your end users must activate an eligible role assignment to get permission to perform certain actions. Using Azure attribute-based access control conditions in PIM enables you not only to limit a user’s role permissions to a resource using fine-grained conditions, but also to use PIM to secure the role assignment with a time-bound setting, approval workflow, audit trail, and so on. For more information, see Azure attribute-based access control public preview.

When a role is assigned, the assignment:

- Can't be assign for a duration of less than five minutes
- Can't be removed within five minutes of it being assigned

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

Manage PIM requests

Approve or deny requests for Azure AD roles in Privileged Identity Management

With Azure Active Directory (Azure AD) Privileged Identity Management (PIM), you can configure roles to require approval for activation, and choose one or multiple users or groups as delegated approvers. Delegated approvers have 24 hours to approve requests. If a request is not approved within 24 hours, then the eligible user must re-submit a new request. The 24 hour approval time window is not configurable.

View pending requests

As a delegated approver, you'll receive an email notification when an Azure AD role request is pending your approval. You can view these pending requests in Privileged Identity Management.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

Approve or deny requests for Azure resource roles in Privileged Identity Management

With Privileged Identity Management (PIM) in Azure Active Directory (Azure AD), you can configure roles to require approval for activation, and choose users or groups from your Azure AD organization as delegated approvers. We recommend selecting two or more approvers for each role to reduce workload for the privileged role administrator. Delegated approvers have 24 hours to approve requests. If a request is not approved within 24 hours, then the eligible user must re-submit a new request. The 24 hour approval time window is not configurable.

Follow the steps in this article to approve or deny requests for Azure resource roles.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-approval-workflow

Analyze PIM audit history and reports

View audit history for Azure AD roles in Privileged Identity Management

You can use the Privileged Identity Management (PIM) audit history to see all role assignments and activations within the past 30 days for all privileged roles. If you want to retain audit data for longer than the default retention period, you can use Azure Monitor to route it to an Azure storage account. .

View activity and audit history for Azure resource roles in Privileged Identity Management

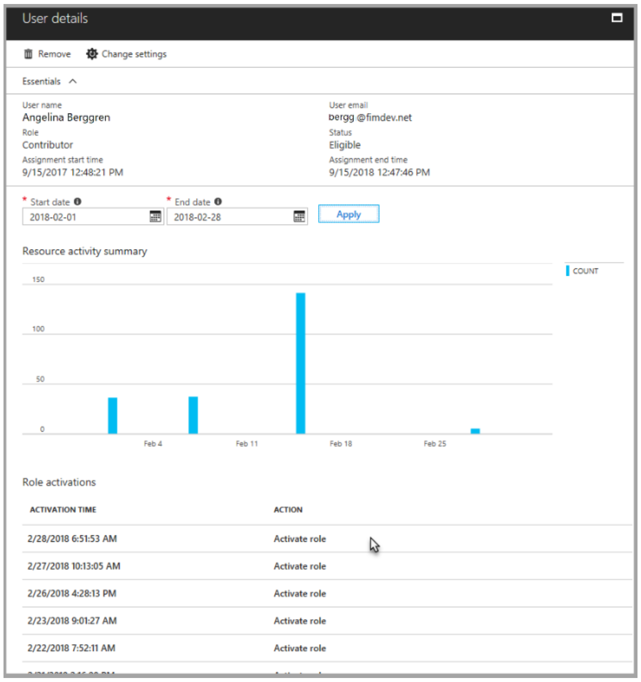
With Azure Active Directory (Azure AD) Privileged Identity Management (PIM), you can view activity, activations, and audit history for Azure resources roles within your organization. This includes subscriptions, resource groups, and even virtual machines. Any resource within the Azure portal that leverages the Azure role-based access control functionality can take advantage of the security and lifecycle management capabilities in Privileged Identity Management. If you want to retain audit data for longer than the default retention period, you can use Azure Monitor to route it to an Azure storage account. For more information, see Archive Azure AD logs to an Azure storage account.

View activity and activations

To see what actions a specific user took in various resources, you can view the Azure resource activity that's associated with a given activation period.

1. Open Azure AD Privileged Identity Management.
2. Select Azure resources.
3. Select the resource you want to view activity and activations for.
4. Select Roles or Members.
5. Select a user.

You see a summary of the user's actions in Azure resources by date. It also shows the recent role activations over that same time period.



User name
Angelina Berggren

User email
bergg @fimdev.net

Role
Contributor

Status
Eligible

Assignment start time
9/15/2017 12:48:21 PM

Assignment end time
9/15/2018 12:47:46 PM

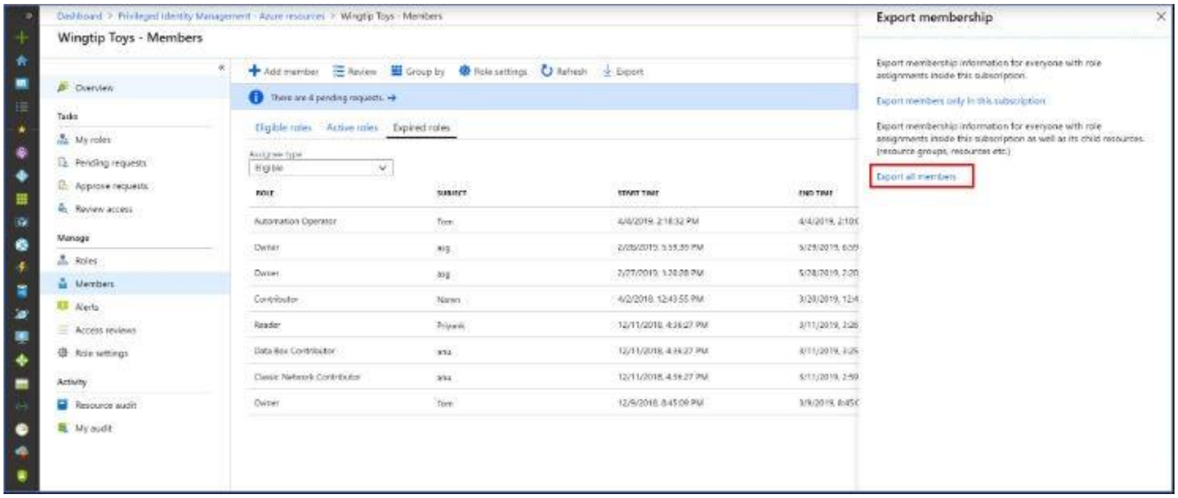
* Start date 2018-02-01

* End date 2018-02-28

Role activations

ACTIVATION TIME	ACTION
2/28/2018 6:51:53 AM	Activate role
2/27/2018 10:13:05 AM	Activate role
2/26/2018 4:28:13 PM	Activate role
2/23/2018 9:01:27 AM	Activate role
2/22/2018 7:52:11 AM	Activate role

6. Select a specific role activation to see details and corresponding Azure resource activity that occurred while that user was active.



There are 4 pending requests. →

ROLE	SUBJECT	START TIME	END TIME
Automation Operator	Tom	4/4/2019, 2:18:32 PM	4/4/2019, 2:10(
Owner	aig	2/28/2019, 5:55:39 PM	5/29/2019, 6:59
Owner	aig	2/27/2019, 1:20:28 PM	5/28/2019, 2:20
Contributor	Naren	4/2/2018, 12:43:55 PM	3/20/2019, 12:4
Reader	Priyank	12/11/2018, 4:36:27 PM	3/11/2019, 3:26
Data Box Contributor	ana	12/11/2018, 4:36:27 PM	3/11/2019, 3:25
Classic Network Contributor	ana	12/11/2018, 4:59:27 PM	5/11/2019, 2:59
Owner	Tom	12/9/2018, 8:45:09 PM	3/9/2019, 8:45(

Export membership

Export membership information for everyone with role assignments inside this subscription.

Export members only in this subscription

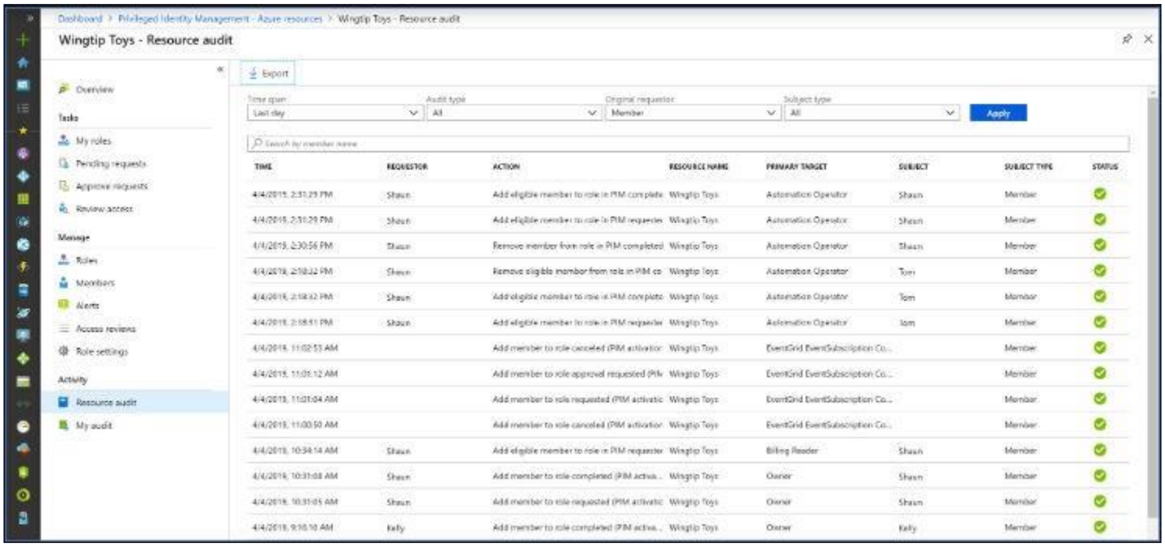
Export membership information for everyone with role assignments inside this subscription as well as its child resources. (resource groups, resources etc.)

Export all members

View resource audit history

Resource audit gives you a view of all role activity for a resource.

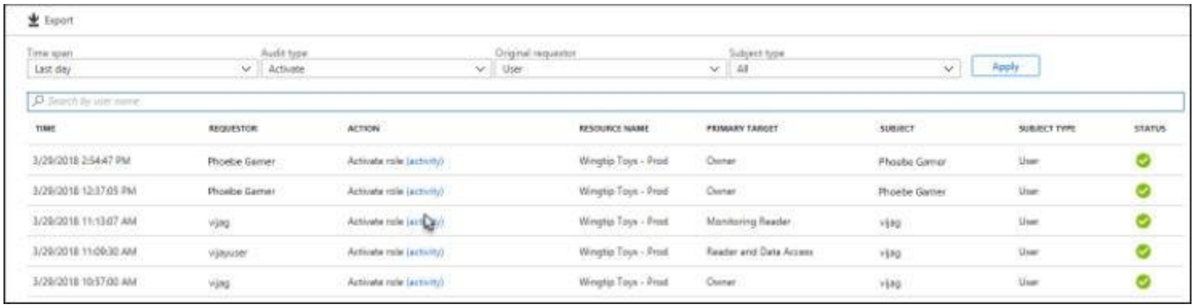
1. Open Azure AD Privileged Identity Management.
2. Select Azure resources.
3. Select the resource you want to view audit history for.
4. Select Resource audit.
5. Filter the history using a predefined date or custom range.



Time span: Last day
Audit type: All
Original requestor: Member
Subject type: All

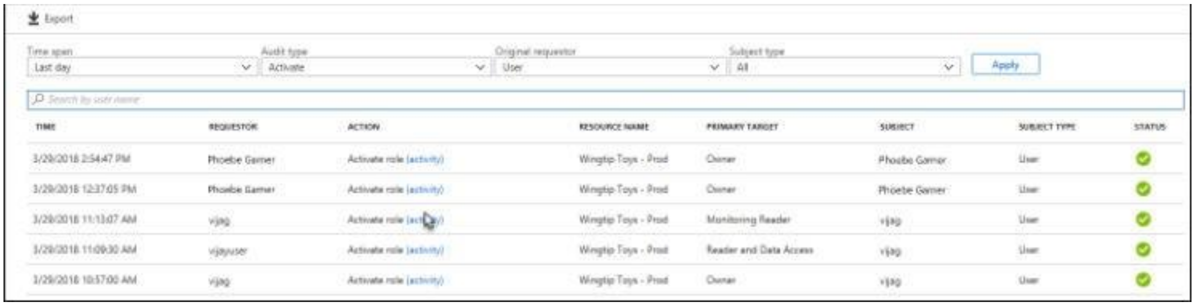
TIME	REQUESTOR	ACTION	RESOURCE NAME	PRIMARY TARGET	SUBJECT	SUBJECT TYPE	STATUS
4/4/2019, 2:31:29 PM	Shaun	Add eligible member to role in PIM complete	Wingtip Toys	Automation Operator	Shaun	Member	✓
4/4/2019, 2:31:29 PM	Shaun	Add eligible member to role in PIM requested	Wingtip Toys	Automation Operator	Shaun	Member	✓
4/4/2019, 2:30:56 PM	Shaun	Remove member from role in PIM completed	Wingtip Toys	Automation Operator	Shaun	Member	✓
4/4/2019, 2:18:32 PM	Shaun	Remove eligible member from role in PIM co	Wingtip Toys	Automation Operator	Tom	Member	✓
4/4/2019, 2:18:32 PM	Shaun	Add eligible member to role in PIM complete	Wingtip Toys	Automation Operator	Tom	Member	✓
4/4/2019, 2:18:31 PM	Shaun	Add eligible member to role in PIM requested	Wingtip Toys	Automation Operator	Tom	Member	✓
4/4/2019, 11:02:53 AM		Add member to role canceled (PIM activation	Wingtip Toys	EventGrid EventSubscription Co...		Member	✓
4/4/2019, 11:01:12 AM		Add member to role approval requested (PIM	Wingtip Toys	EventGrid EventSubscription Co...		Member	✓
4/4/2019, 11:01:04 AM		Add member to role requested (PIM activatic	Wingtip Toys	EventGrid EventSubscription Co...		Member	✓
4/4/2019, 11:00:50 AM		Add member to role canceled (PIM activation	Wingtip Toys	EventGrid EventSubscription Co...		Member	✓
4/4/2019, 10:34:14 AM	Shaun	Add eligible member to role in PIM requester	Wingtip Toys	Billing Reader	Shaun	Member	✓
4/4/2019, 10:31:08 AM	Shaun	Add member to role completed (PIM activa...	Wingtip Toys	Owner	Shaun	Member	✓
4/4/2019, 10:31:05 AM	Shaun	Add member to role requested (PIM activatic	Wingtip Toys	Owner	Shaun	Member	✓
4/4/2019, 9:10:10 AM	Kelly	Add member to role completed (PIM activa...	Wingtip Toys	Owner	Kelly	Member	✓

6. For Audit type, select Activate (Assigned + Activated).



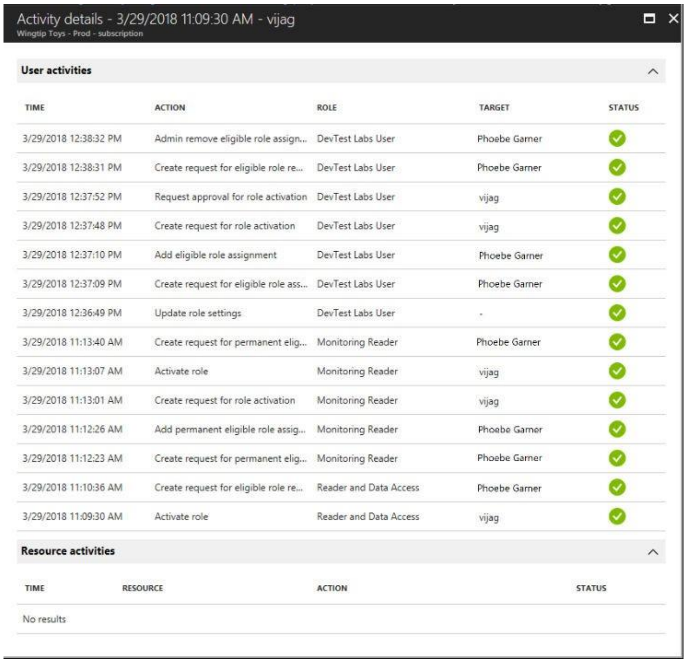
Time span: Last day
Audit type: Activate
Original requestor: User
Subject type: All

TIME	REQUESTOR	ACTION	RESOURCE NAME	PRIMARY TARGET	SUBJECT	SUBJECT TYPE	STATUS
3/29/2018 2:54:47 PM	Phoebe Garner	Activate role (activity)	Wingtip Toys - Prod	Owner	Phoebe Garner	User	✓
3/29/2018 12:37:05 PM	Phoebe Garner	Activate role (activity)	Wingtip Toys - Prod	Owner	Phoebe Garner	User	✓
3/29/2018 11:13:07 AM	vijag	Activate role (activity)	Wingtip Toys - Prod	Monitoring Reader	vijag	User	✓
3/29/2018 11:09:30 AM	vijayuser	Activate role (activity)	Wingtip Toys - Prod	Reader and Data Access	vijag	User	✓
3/29/2018 10:57:00 AM	vijag	Activate role (activity)	Wingtip Toys - Prod	Owner	vijag	User	✓


Time span: Last day
Audit type: Activate
Original requestor: User
Subject type: All

TIME	REQUESTOR	ACTION	RESOURCE NAME	PRIMARY TARGET	SUBJECT	SUBJECT TYPE	STATUS
3/29/2018 2:54:47 PM	Phoebe Garner	Activate role (activity)	Wingtip Toys - Prod	Owner	Phoebe Garner	User	✓
3/29/2018 12:37:05 PM	Phoebe Garner	Activate role (activity)	Wingtip Toys - Prod	Owner	Phoebe Garner	User	✓
3/29/2018 11:13:07 AM	vijag	Activate role (activity)	Wingtip Toys - Prod	Monitoring Reader	vijag	User	✓
3/29/2018 11:09:30 AM	vijayuser	Activate role (activity)	Wingtip Toys - Prod	Reader and Data Access	vijag	User	✓
3/29/2018 10:57:00 AM	vijag	Activate role (activity)	Wingtip Toys - Prod	Owner	vijag	User	✓

7. Under Action, click (activity) for a user to see that user's activity detail in Azure resources.



Activity details - 3/29/2018 11:09:30 AM - vijag
Wingtip Toys - Prod - subscription

User activities

TIME	ACTION	ROLE	TARGET	STATUS
3/29/2018 12:38:32 PM	Admin remove eligible role assign...	DevTest Labs User	Phoebe Garner	✓
3/29/2018 12:38:31 PM	Create request for eligible role re...	DevTest Labs User	Phoebe Garner	✓
3/29/2018 12:37:52 PM	Request approval for role activation	DevTest Labs User	vijag	✓
3/29/2018 12:37:48 PM	Create request for role activation	DevTest Labs User	vijag	✓
3/29/2018 12:37:10 PM	Add eligible role assignment	DevTest Labs User	Phoebe Garner	✓
3/29/2018 12:37:09 PM	Create request for eligible role ass...	DevTest Labs User	Phoebe Garner	✓
3/29/2018 12:36:49 PM	Update role settings	DevTest Labs User	-	✓
3/29/2018 11:13:40 AM	Create request for permanent elig...	Monitoring Reader	Phoebe Garner	✓
3/29/2018 11:13:07 AM	Activate role	Monitoring Reader	vijag	✓
3/29/2018 11:13:01 AM	Create request for role activation	Monitoring Reader	vijag	✓
3/29/2018 11:12:26 AM	Add permanent eligible role assig...	Monitoring Reader	Phoebe Garner	✓
3/29/2018 11:12:23 AM	Create request for permanent elig...	Monitoring Reader	Phoebe Garner	✓
3/29/2018 11:10:36 AM	Create request for eligible role re...	Reader and Data Access	Phoebe Garner	✓
3/29/2018 11:09:30 AM	Activate role	Reader and Data Access	vijag	✓

Resource activities

TIME	RESOURCE	ACTION	STATUS
No results			

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-pim-resource-rbac

Create and manage break-glass accounts

Create emergency accounts

Manage emergency access accounts in Azure AD

It is important that you prevent being accidentally locked out of your Azure Active Directory (Azure AD) organization because you can't sign in or activate another user's account as an administrator. You can mitigate the impact of accidental lack of administrative access by creating two or more *emergency access accounts* in your organization.

Emergency access accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or "break glass"' scenarios where normal administrative accounts can't be used. We recommend that you maintain a goal of restricting emergency account use to only the times when it is absolutely necessary.

This article provides guidelines for managing emergency access accounts in Azure AD.

Create emergency access accounts

Create two or more emergency access accounts. These accounts should be cloud-only accounts that use the *.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment.

How to create an emergency access account

1.Sign in to the Azure portal or Azure AD admin center as an existing Global Administrator.

2.Select Azure Active Directory > Users.

3.Select New user.

4.Select Create user.

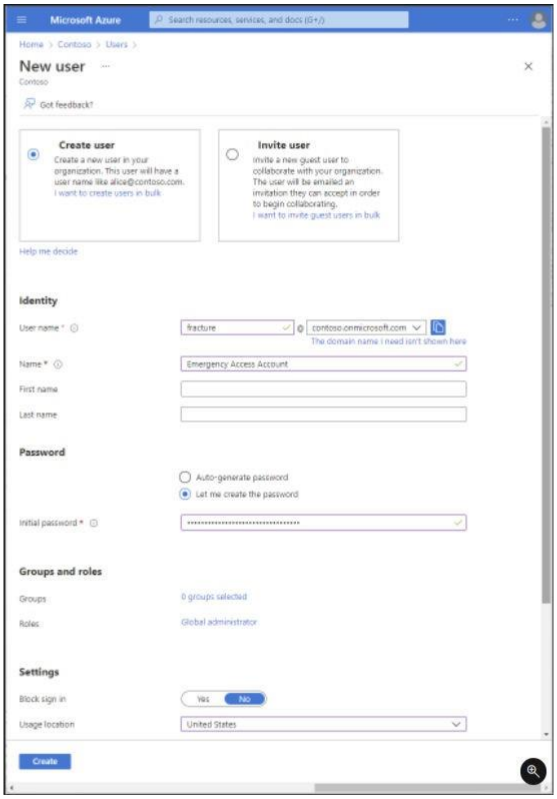
5.Give the account a User name.

6.Give the account a Name.

7.Create a long and complex password for the account.

8.Under Roles, assign the Global Administrator role.

9.Under Usage location, select the appropriate location.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso > Users >
Got feedback?
Help me decide
The domain name I need isn't shown here
Create

New user

Contoso

● Create user
Create a new user in your organization. This user will have a user name like alice@contoso.com.
I want to create users in bulk

○ Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk

Identity

User name * : fracture @ contoso.onmicrosoft.com

Name * : Emergency Access Account

First name :

Last name :

Password

○ Auto-generate password
● Let me create the password

Initial password * : ••••••••••••••••••••••••••••••••

Groups and roles

Groups : 0 groups selected

Roles : Global administrator

Settings

Block sign in : Yes [✓ No]

Usage location : United States

10.Select Create.

11.Store account credentials safely.

12.Monitor sign-in and audit logs.

13.Validate accounts regularly.

When configuring these accounts, the following requirements must be met:

- The emergency access accounts should not be associated with any individual user in the organization. Make sure that your accounts are not connected with any employee-supplied mobile phones, hardware tokens that travel with individual employees, or other employee-specific credentials. This precaution covers instances where an individual employee is unreachable when the credential is needed. It is important to ensure that any registered devices are kept in a known, secure location that has multiple means of communicating with Azure AD.
- Use strong authentication for your emergency access accounts and make sure it doesn't use the same authentication methods as your other administrative accounts. For example, if your normal administrator account uses the Microsoft Authenticator app for strong authentication, use a FIDO2 security key for your emergency accounts. Consider the dependencies of various authentication methods, to avoid adding external

requirements into the authentication process.

- The device or credential must not expire or be in scope of automated cleanup due to lack of use.
- In Azure AD Privileged Identity Management, you should make the Global Administrator role assignment permanent rather than eligible for your emergency access accounts.

https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

Monitor and maintain Azure Active Directory

Analyze and investigate sign-in logs to troubleshoot access issues

Sign-in logs

Sign-in logs in Azure Active Directory

As an IT administrator, you want to know how your IT environment is doing. The information about your system's health enables you to assess whether and how you need to respond to potential issues.

To support you with this goal, the Azure Active Directory portal gives you access to three activity logs:

- Sign-ins – Information about sign-ins and how your resources are used by your users.

- Audit – Information about changes applied to your tenant such as users and group management or updates applied to your tenant's resources.

- Provisioning – Activities performed by the provisioning service, such as the creation of a group in ServiceNow or a user imported from Workday.

This article gives you an overview of the sign-ins report.

Filter sign-in activities

You can filter the data in a log to narrow it down to a level that works for you:

Request ID - The ID of the request you care about.

User - The name or the user principal name (UPN) of the user you care about.

Application - The name of the target application.

Status - The sign-in status you care about:

- Success
- Failure
- Interrupted

IP address - The IP address of the device used to connect to your tenant.

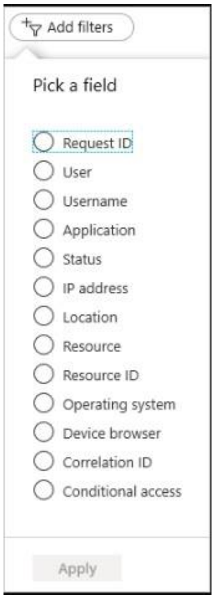
The Location - The location the connection was initiated from:

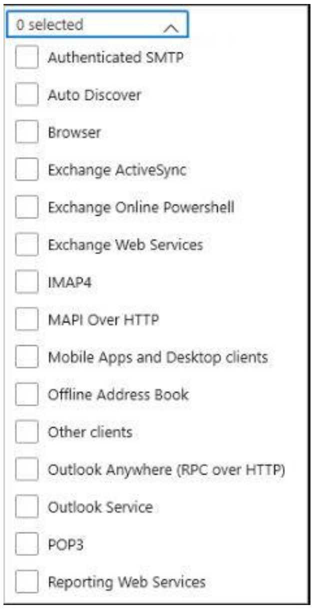
- City
- State / Province
- Country/Region

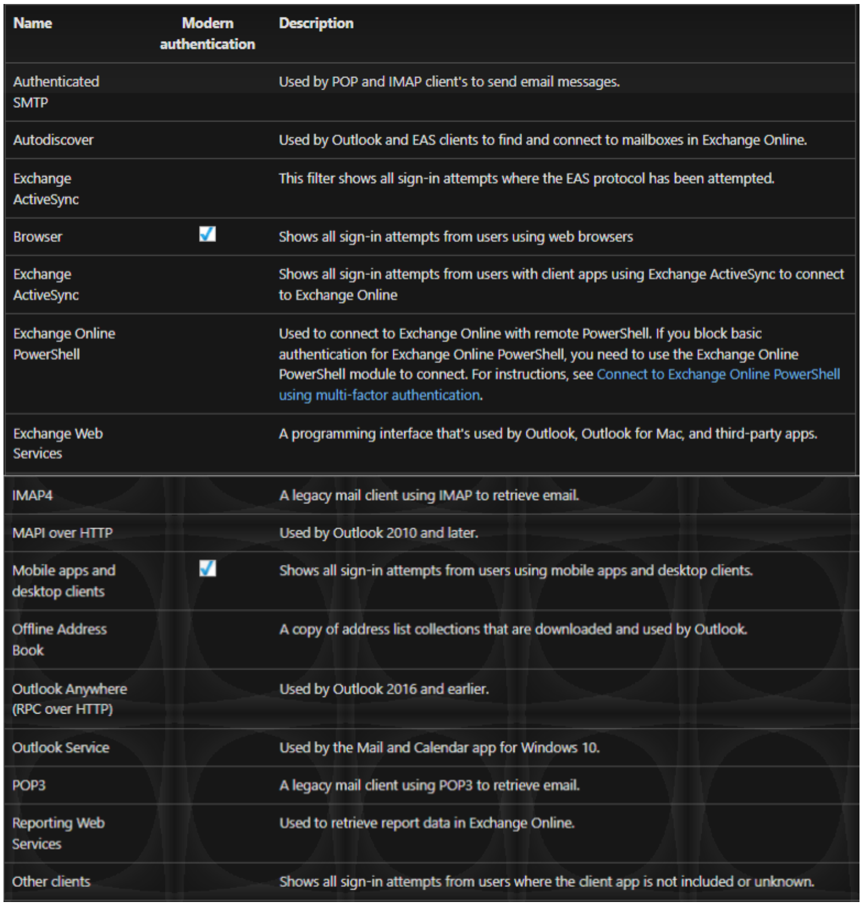
Resource - The name of the service used for the sign-in.

Resource ID - The ID of the service used for the sign-in.

Client app - The type of the client app used to connect to your tenant:







Name	Modern authentication	Description
Authenticated SMTP		Used by POP and IMAP client's to send email messages.
Autodiscover		Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.
Exchange ActiveSync		This filter shows all sign-in attempts where the EAS protocol has been attempted.
Browser	☑	Shows all sign-in attempts from users using web browsers
Exchange ActiveSync		Shows all sign-in attempts from users with client apps using Exchange ActiveSync to connect to Exchange Online
Exchange Online PowerShell		Used to connect to Exchange Online with remote PowerShell. If you block basic authentication for Exchange Online PowerShell, you need to use the Exchange Online PowerShell module to connect. For instructions, see Connect to Exchange Online PowerShell using multi-factor authentication.
Exchange Web Services		A programming interface that's used by Outlook, Outlook for Mac, and third-party apps.
IMAP4		A legacy mail client using IMAP to retrieve email.
MAPI over HTTP		Used by Outlook 2010 and later.
Mobile apps and desktop clients	☑	Shows all sign-in attempts from users using mobile apps and desktop clients.
Offline Address Book		A copy of address list collections that are downloaded and used by Outlook.
Outlook Anywhere (RPC over HTTP)		Used by Outlook 2016 and earlier.
Outlook Service		Used by the Mail and Calendar app for Windows 10.
POP3		A legacy mail client using POP3 to retrieve email.
Reporting Web Services		Used to retrieve report data in Exchange Online.
Other clients		Shows all sign-in attempts from users where the client app is not included or unknown.

Operating system - The operating system running on the device used sign-on to your tenant.

Device browser - If the connection was initiated from a browser, this field enables you to filter by browser name.

Correlation ID - The correlation ID of the activity.

Conditional access - The status of the applied conditional access rules

- **Not applied**: No policy applied to the user and application during sign-in.
- **Success**: One or more conditional access policies applied to the user and application (but not necessarily the other conditions) during sign-in.
- **Failure**: The sign-in satisfied the user and application condition of at least one Conditional Access policy and grant controls are either not satisfied or set to block access.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Review and monitor Azure AD audit logs

Audit logs

Audit logs in Azure Active Directory

As an IT administrator, you want to know how your IT environment is doing. The information about your system's health enables you to assess whether and how you need to respond to potential issues.

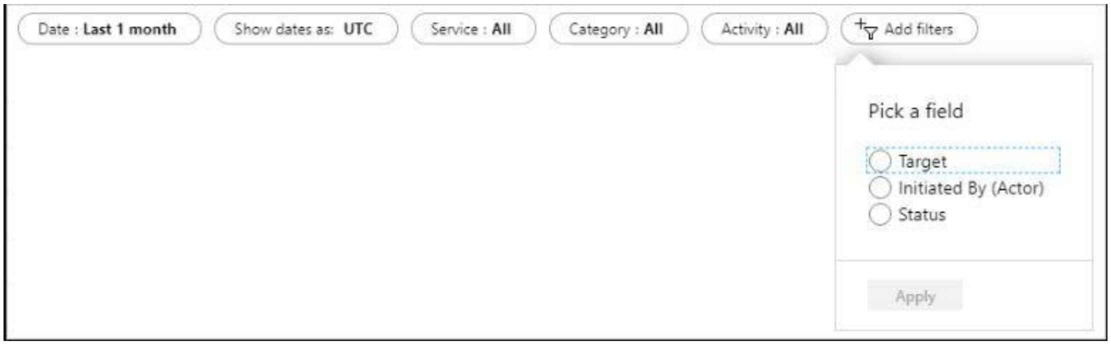
To support you with this goal, the Azure Active Directory portal gives you access to three activity logs:

- Sign-ins – Information about sign-ins and how your resources are used by your users.
- Audit – Information about changes applied to your tenant such as users and group management or updates applied to your tenant's resources.
- Provisioning – Activities performed by the provisioning service, such as the creation of a group in ServiceNow or a user imported from Workday.

Filtering audit logs

You can filter the audit data on the following fields:

- Service
- Category
- Activity
- Status
- Target
- Initiated by (Actor)
- Date range



The **Service** filter allows you to select from a drop-down list of the following services:

- All
- AAD Management UX
- Access Reviews
- Account Provisioning
- Application Proxy
- Authentication Methods
- B2C
- Conditional Access
- Core Directory
- Entitlement Management
- Hybrid Authentication
- Identity Protection
- Invited Users
- MIM Service
- MyApps
- PIM
- Self-service Group Management
- Self-service Password Management
- Terms of Use

The **Category** filter enables you to select one of the following filters:

- All
- AdministrativeUnit
- ApplicationManagement
- Authentication
- Authorization
- Contact
- Device
- DeviceConfiguration
- DirectoryManagement
- EntitlementManagement
- GroupManagement
- KerberosDomain
- KeyManagement
- Label
- Other
- PermissionGrantPolicy

- Policy
- ResourceManagement
- RoleManagement
- UserManagement

The Activity filter is based on the category and activity resource type selection you make. You can select a specific activity you want to see or choose all.

You can get the list of all Audit Activities using the Graph API: https://graph.windows.net/<tenantdomain>/activities/auditActivityTypesV2?api-version=beta

The Status filter allows you to filter based on the status of an audit operation. The status can be one of the following:

- All
- Success
- Failure

The Target filter allows you to search for a particular target by the starting of the name or user principal name (UPN). The target name and UPN are case-sensitive.

The Initiated by filter enables you to define what an actor's name or a universal principal name (UPN) starts with. The name and UPN are case-sensitive.

The Date range filter enables to you to define a timeframe for the returned data.
Possible values are:

- 7 days
- 24 hours
- Custom

When you select a custom timeframe, you can configure a start time and an end time.

You can also choose to download the filtered data, up to 250,000 records, by selecting the **Download** button. You can download the logs in either CSV or JSON format. The number of records you can download is constrained by the Azure Active Directory report retention policies.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

Enable and integrate Azure AD diagnostic logs with Log Analytics / Azure Sentinel

Log analytics wizard

Configure a workspace

This procedure outlines how to configure a log analytics workspace for your audit and sign-in logs. Configuring a log analytics workspace consists of two main steps:

1. Creating a log analytics workspace
2. Setting diagnostic settings
3. On the log analytics workspaces page, click Add.
4. On the Create Log Analytics workspace page, perform the following steps:

a. Select your subscription.
b. Select a resource group.
c. In the **Name** textbox, type a name (e.g.: MytestWorkspace1).
d. Select your region.

5. Click Review + Create.
6. Click Create and wait for the deployment to be succeeded. You may need to refresh the page to see the new workspace.
7. Search for Azure Active Directory.
8. In Monitoring section, click Diagnostic setting.
9. On the Diagnostic settings page, click Add diagnostic setting.
10. On the Diagnostic setting page, perform the following steps:

a. Under Category details, select AuditLogs and SigninLogs.
b. Under Destination details, select Send to Log Analytics, and then select your new log analytics workspace.
c. Click Save.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

Export sign-in and audit logs to a third-party SIEM

Stream logs to event hub

In this tutorial, you learn how to set up Azure Monitor diagnostics settings to stream Azure Active Directory (Azure AD) logs to an Azure event hub. Use this mechanism to integrate your logs with third-party Security Information and Event Management (SIEM) tools, such as Splunk and QRadar.

Stream logs to an event hub

1. Sign in to the Azure portal.
2. Select Azure Active Directory > Audit logs.
3. Select Export Data Settings.
4. In the Diagnostics settings pane, do either of the following:

- To change existing settings, select Edit setting.
- To add new settings, select Add diagnostics setting.You can have up to three settings.

5. Select the Stream to an event hub check box, and then select Event Hub/Configure.

a. Select the Azure subscription and Event Hubs namespace that you want to route the logs to.The subscription and Event Hubs namespace must both be associated with the Azure AD tenant that the logs stream from. You can also specify an event hub within the Event Hubs namespace to which logs should be sent. If no event hub is specified, an event hub is created in the namespace with the default name insights-logs-audit.
b. Select any combination of the following items:

- To send audit logs to the event hub, select the AuditLogs check box.
- To send interactive user sign-in logs to the event hub, select the SignInLogs check box.
- To send non-interactive user sign-in logs to the event hub, select the NonInteractiveUserSignInLogs check box.
- To send service principal sign-in logs to the event hub, select the ServicePrincipalSignInLogs check box.
- To send managed identity sign-in logs to the event hub, select the ManagedIdentitySignInLogs check box.
- To send provisioning logs to the event hub, select the ProvisioningLogs check box.
- To send sign-ins sent to Azure AD by an AD FS Connect Health agent, select the ADFSSignInLogs check box.
- To send risky user information, select the RiskyUsers check box.
- To send user risk events information, select the UserRiskEvents check box.

c. Select Save to save the setting.

6. After about 15 minutes, verify that events are displayed in your event hub. To do so, go to the event hub from the portal and verify that the **incoming messages** count is greater than zero.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub

Review Azure AD activity by using Log Analytics / Azure Sentinel, excluding KQL use

Connect Azure Active Directory data to Azure Sentinel

You can use Microsoft Sentinel's built-in connector to collect data from Azure Active Directory and stream it into Microsoft Sentinel. The connector allows you to stream the following log types:

- Sign-in logs, which contain information about interactive user sign-ins where a user provides an authentication factor.

  The Azure AD connector now includes the following three additional categories of sign-in logs, all currently in PREVIEW:

◊ Non-interactive user sign-in logs, which contain information about sign-ins performed by a client on behalf of a user without any interaction or authentication factor from the user.
◊ Service principal sign-in logs, which contain information about sign-ins by apps and service principals that do not involve any user. In these sign-ins, the app or service provides a credential on its own behalf to authenticate or access resources.
◊ Managed Identity sign-in logs, which contain information about sign-ins by Azure resources that have secrets managed by Azure. For more information, see What are managed identities for Azure resources?

- Audit logs, which contain information about system activity relating to user and group management, managed applications, and directory activities.
- Provisioning logs (also in PREVIEW), which contain system activity information about users, groups, and roles provisioned by the Azure AD provisioning service.

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-active-directory

Install and use the log analytics views for Azure AD

The Azure Active Directory log analytics views helps you analyze and search the Azure AD activity logs in your Azure AD tenant. Azure AD activity logs include:

- Audit logs: The audit logs activity report gives you access to the history of every task that's performed in your tenant.
- Sign-in logs: With the sign-in activity report, you can determine who performed the tasks that are reported in the audit logs.

Install the log analytics views

1. Navigate to your Log Analytics workspace. To do this, first navigate to the Azure portal and select All services. Type Log Analytics in the text box, and select Log Analytics workspaces. Select the workspace you routed the activity logs to, as part of the prerequisites.
2. Select View Designer, select Import and then select Choose File to import the views from your local computer.
3. Select the views you downloaded from the prerequisites and select Save to save the import. Do this for the Azure AD Account Provisioning Events view and the Sign-ins Events view.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-install-use-log-analytics-views

Analyze Azure Active Directory workbooks / reporting

How to use Azure AD workbooks

In order to optimize the underlying queries in this workbook, please click on "Edit", click on Settings icon and select the workspace where you want to run these queries. Workbooks by default will select all workspaces where you are routing your Azure AD logs.

Do you want to:

- Understand the effect of your Conditional Access policies on your users' sign-in experience?
- Troubleshoot sign-in failures to get a better view of your organization's sign-in health and

to resolve issues quickly?

- Understand risky users and risk detections trends in your tenant?
- Know who's using legacy authentications to sign in to your environment? (By blocking legacy authentication, you can improve your tenant's protection.)
- Do you need to understand the impact of Conditional Access policies in your tenant?
- Would you like the ability to review: sign-in log queries, with a workbook that reports how many users were granted or denied access, as well as how many users bypassed Conditional Access policies when accessing resources?
- Interested in developing a deeper understanding of conditional access, with a workbook details per condition so that the impact of a policy can be contextualized per condition, including device platform, device state, client app, sign-in risk, location, and application?
- Archive and report on more than one year of historical application role and access package assignment activity?

To help you to address these questions, Azure Active Directory provides workbooks for monitoring. Azure Monitor workbooks combine text, analytics queries, metrics, and parameters into rich interactive reports.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-use-azure-monitor-workbooks

Configure notifications

Alert on an activity log event

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. You create these alerts for Azure resources by using an Azure Resource Manager template. You can also create, update, or delete these alerts in the Azure portal.

Typically, you create activity log alerts to receive notifications when specific changes occur to resources in your Azure subscription. Alerts are often scoped to particular resource groups or resources. For example, you might want to be notified when any virtual machine in the sample resource group myProductionResourceGroup is deleted. Or, you might want to get notified if any new roles are assigned to a user in your subscription.

When you create alert rules, make sure that:

- The subscription in the scope isn't different from the subscription where the alert is created.
- The criteria must be the level, status, caller, resource group, resource ID, or resource type event category on which the alert is configured.
- There's no anyOf condition or nested conditions in the alert configuration JSON. Only one allOf condition is allowed, with no further allOf or anyOf conditions.
- When the category is administrative, you must specify at least one of the preceding criteria in your alert. You can't create an alert that activates every time an event is created in the activity logs.
- Alerts can't be created for events in the alert category of the activity log.

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-activity-log