

AZ-500 Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources

Get trained

Find documentation

Links to learning and documentation

[Choose from self-paced learning paths and modules or take an instructor-led course](#)

[Azure documentation](#)

[Azure Active Directory \(AD\)](#)

[Azure Firewall documentation](#)

[Azure Firewall Manager documentation](#)

[Azure Application Gateway documentation](#)

[Azure Front Door and CDN Documentation](#)

[Web Application Firewall documentation](#)

[Azure Key Vault documentation](#)

[Azure virtual network service endpoint policies](#)

[Manage Azure Private Endpoints - Azure Private Link](#)

[Create a Private Link service by using the Azure portal](#)

[Azure DDoS Protection Standard documentation](#)

[Endpoint Protection on a Windows VM in Azure](#)

[Secure and use policies - Azure Virtual Machines](#)

[Security - Azure App Service](#)

[Azure Policy documentation](#)

[Overview of Microsoft Defender for Servers](#)

[Microsoft Defender for Cloud documentation](#)

[Microsoft Threat Modeling Tool overview](#)

[Azure Monitor documentation](#)

[Microsoft Sentinel documentation](#)

[Azure Storage documentation](#)

Study resources

Ask a question

Get community support

Follow Microsoft Learn

Find a video

Links to learning and documentation

[Azure Files documentation](#)

[Azure SQL documentation](#)

[Microsoft Q&A | Microsoft Docs](#)

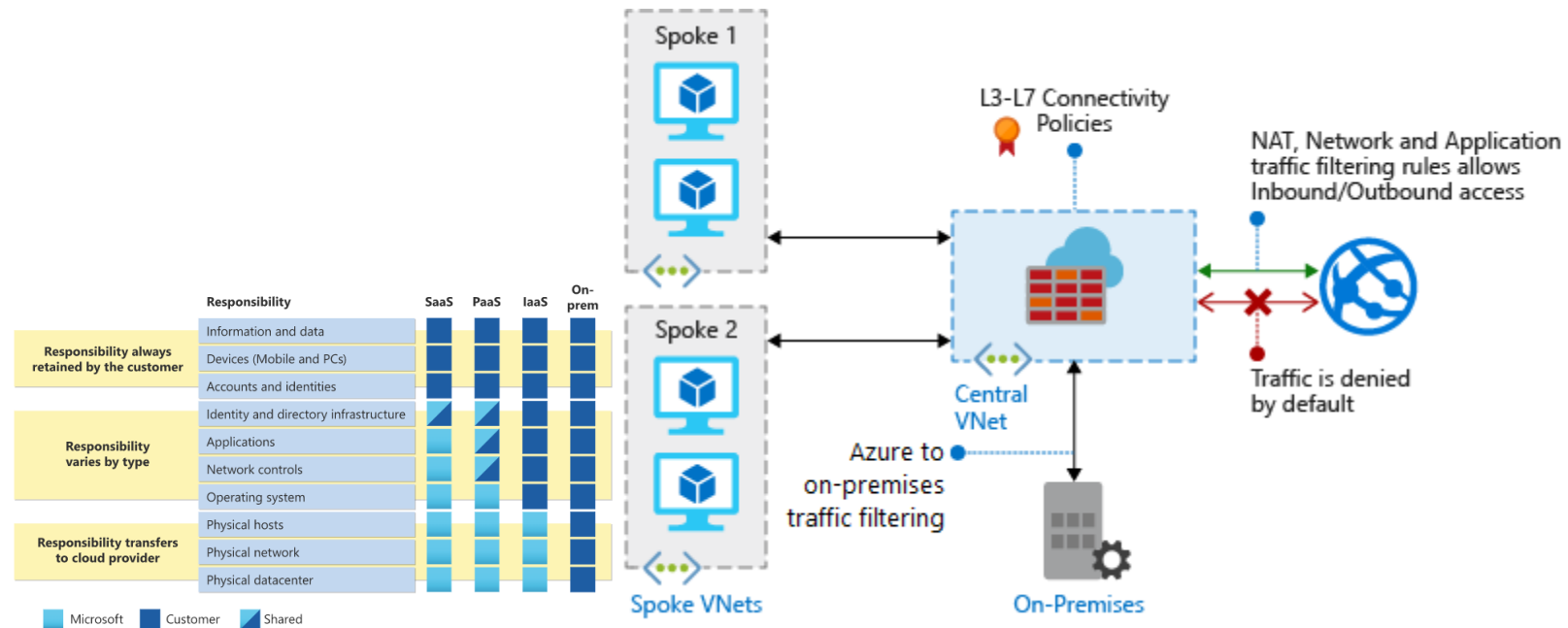
[Azure Community Support](#)

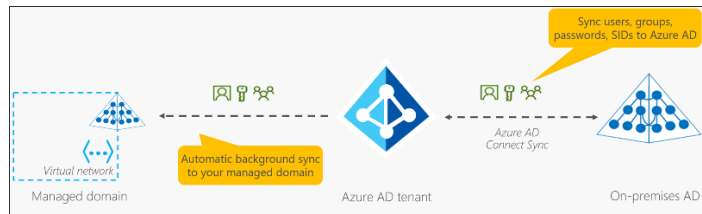
[Microsoft Learn - Microsoft Tech Community](#)

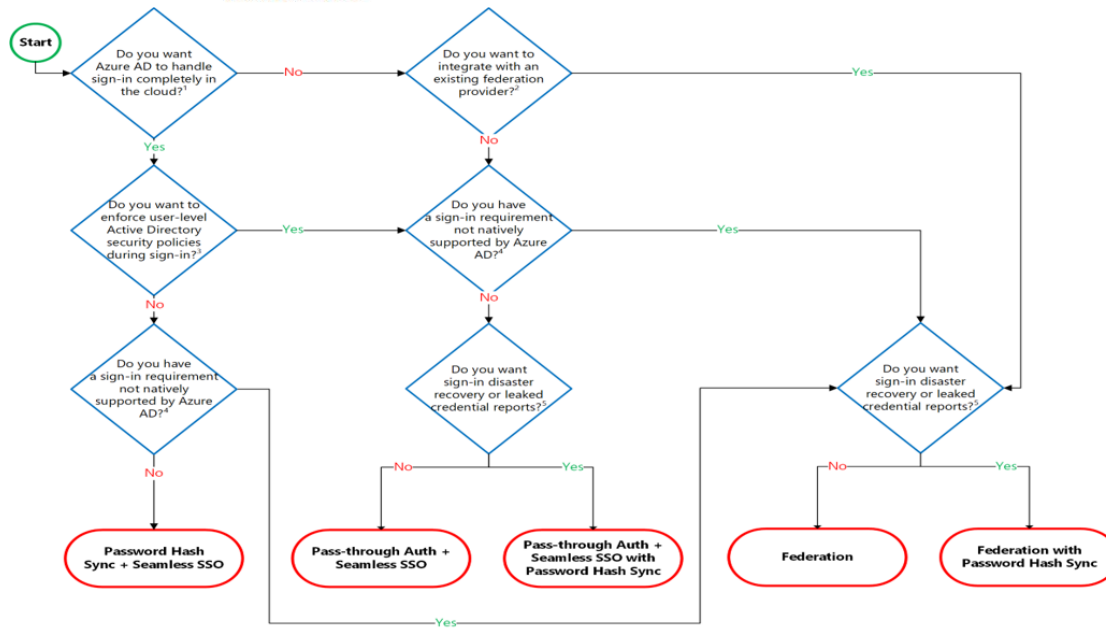
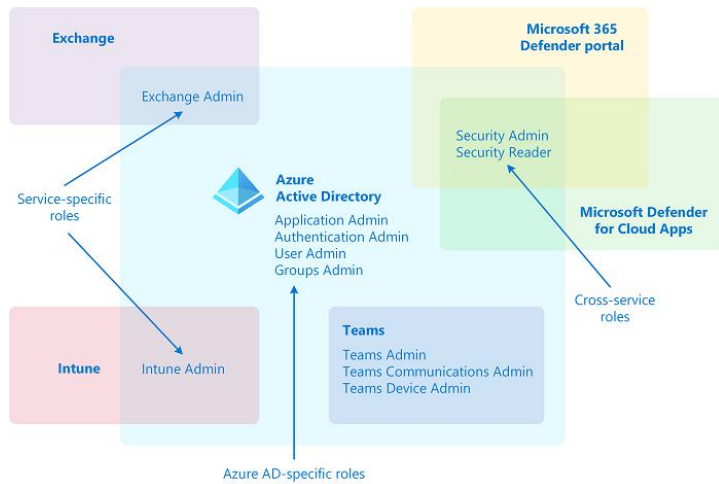
[Exam Readiness Zone](#)

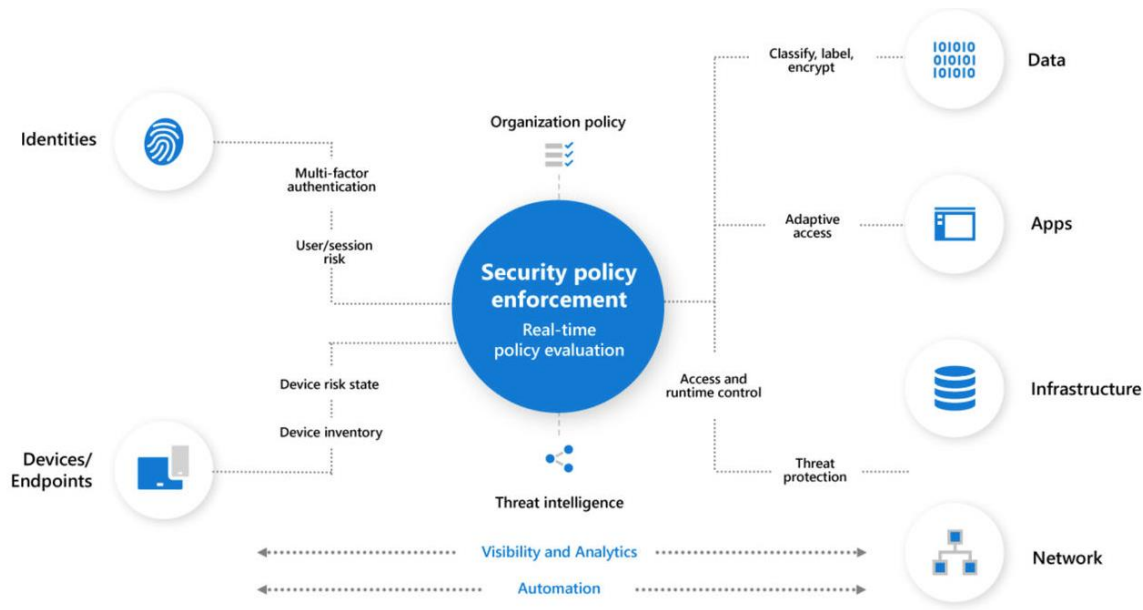
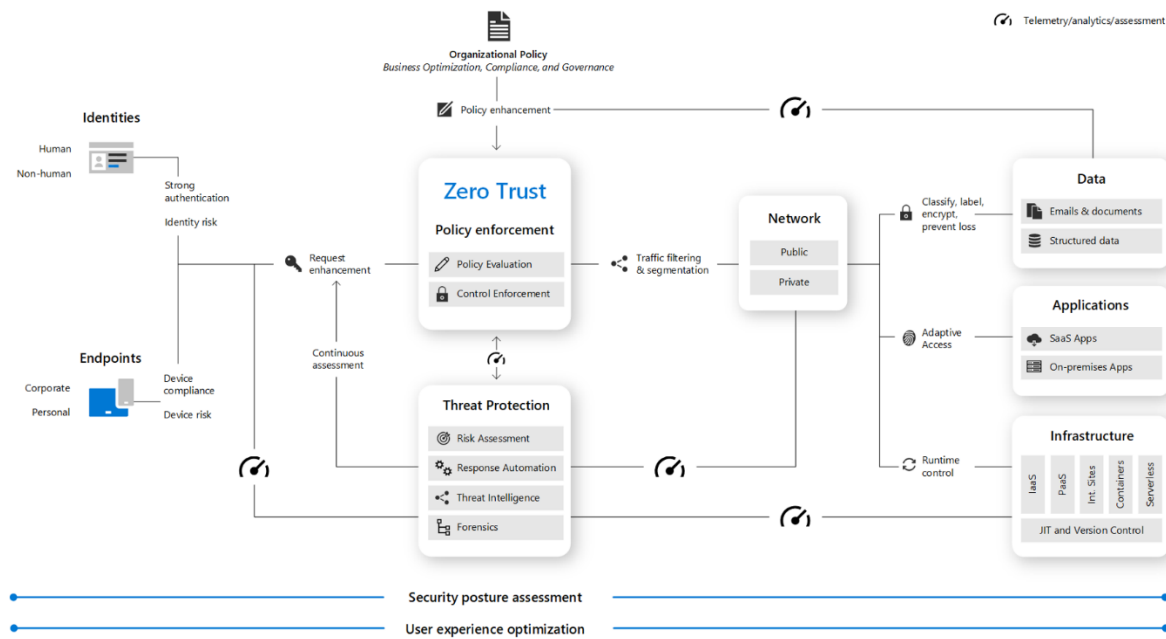
[Azure Fridays](#)

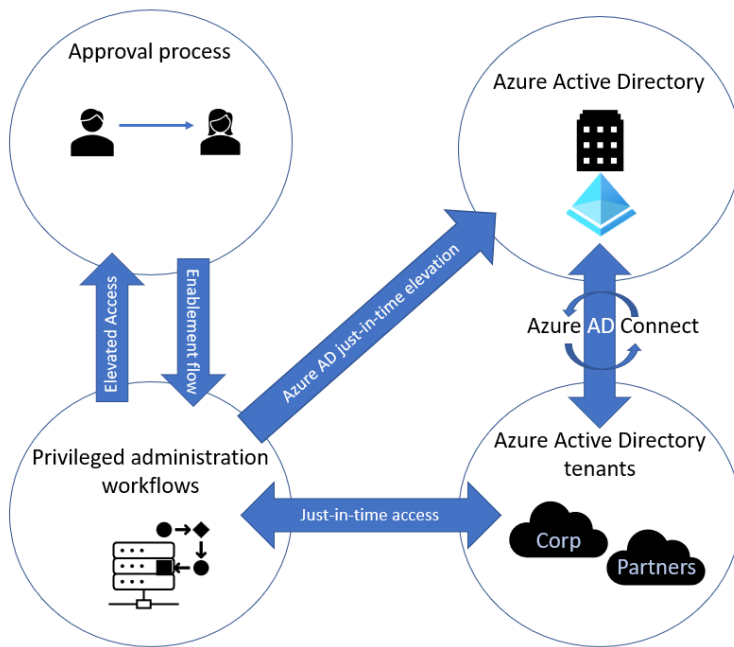
[Browse other Microsoft Learn shows](#)











Category

Azure AD-specific roles

Role

Application Administrator
 Application Developer
 Authentication Administrator
 Business to consumer (B2C) Identity Experience Framework (IEF) Keyset Administrator
 Business to consumer (B2C) Identity Experience Framework (IEF) Policy Administrator
 Cloud Application Administrator
 Cloud Device Administrator
 Conditional Access Administrator
 Device Administrators
 Directory Readers
 Directory Synchronization Accounts
 Directory Writers
 External ID User Flow Administrator
 External ID User Flow Attribute Administrator
 External Identity Provider Administrator
 Groups Administrator
 Guest Inviter
 Helpdesk Administrator

Category	Role
Cross-service roles	Hybrid Identity Administrator
	License Administrator
	Partner Tier1 Support
	Partner Tier2 Support
	Password Administrator
	Privileged Authentication Administrator
	Privileged Role Administrator
	Reports Reader
	User Administrator
	Global Administrator
Service-specific roles	Compliance Administrator
	Compliance Data Administrator
	Global Reader
	Security Administrator
	Security Operator
	Security Reader
	Service Support Administrator
	Azure DevOps Administrator
	Azure Information Protection Administrator
	Billing Administrator
	Customer relationship management (CRM) Service Administrator
	Customer Lockbox Access Approver
	Desktop Analytics Administrator
	Exchange Service Administrator
	Insights Administrator
	Insights Business Leader
	Intune Service Administrator
	Kaizala Administrator
	Lync Service Administrator
	Message Center Privacy Reader
	Message Center Reader
	Modern Commerce User
	Network Administrator
	Office Apps Administrator
	Power BI Service Administrator
	Power Platform Administrator
	Printer Administrator
	Printer Technician
	Search Administrator
	Search Editor
	SharePoint Service Administrator
	Teams Communications Administrator

Category**Role**

Teams Communications Support Engineer
Teams Communications Support Specialist
Teams Devices Administrator
Teams Administrator

All Roles**Role****Description****Application Administrator**

Users in this role can create and manage all aspects of enterprise applications, application registrations, and application proxy settings. Users assigned to this role aren't added as owners when creating new application registrations or enterprise applications. This role also grants the ability to consent for delegated permissions and application permissions, except for application permissions for Microsoft Graph.

Application Developer

Can create application registrations independent of the Users can register applications setting.

Attack Payload Author

Users in this role can create attack payloads but not actually launch or schedule them. Attack payloads are then available to all administrators in the tenant, who can use them to create a simulation.

Attack Simulation Administrator

Users in this role can create and manage all aspects of attack simulation creation, launch/scheduling of a simulation, and the review of simulation results. Members of this role have this access for all simulations in the tenant.

Attribute Assignment Administrator

Users with this role can assign and remove custom security attribute keys and values for supported Azure AD objects such as users, service principals, and devices. By default, Global Administrator and other administrator roles don't have permissions to read, define, or assign custom security attributes. To work with custom security attributes, you must be assigned one of the custom security attribute roles.

Attribute Assignment Reader

Users with this role can read custom security attribute keys and values for supported Azure AD objects. By default, Global Administrator and other administrator roles don't have permissions to read, define, or assign custom security attributes. You must be assigned one of the custom security attribute roles to work with custom security attributes.

Attribute Definition Administrator

Users with this role can define a valid set of custom security attributes that can be assigned to supported Azure AD objects. This role can also activate and deactivate custom security attributes. By default, Global Administrator and other administrator roles don't have permissions to read, define, or assign custom security attributes. To work with custom security attributes, you must be assigned one of the custom security attribute roles.

Authentication Administrator

Assign the Authentication Administrator role to users who need to do the following:

- Set or reset any authentication method (including passwords) for nonadministrators and some roles.
- Require users who are nonadministrators or assigned to some roles to re-register against existing nonpassword credentials (for example, **Multifactor authentication (MFA)** or **Fast ID Online (FIDO)**), and can also revoke remember MFA on the device, which prompts for MFA on the next sign-in.
- Perform sensitive actions for some users.
- Create and manage support tickets in Azure and the Microsoft 365 admin center.

Users with this role can't do the following tasks:

- Can't change the credentials or reset MFA for members and owners of a role-assignable group.

Role	Description
	-Can't manage MFA settings in the legacy MFA management portal or Hardware OATH tokens. The same functions can be accomplished using the Set-MsolUser commandlet Azure AD PowerShell module.
Authentication Policy Administrator	<p>Assign the Authentication Policy Administrator role to users who need to do the following:</p> <ul style="list-style-type: none"> -Configure the authentication methods policy, tenant-wide MFA settings, and password protection policy that determine which methods each user can register and use. -Manage Password Protection settings: smart lockout configurations and updating the custom banned passwords list. -Create and manage verifiable credentials. -Create and manage Azure support tickets. <p>Users with this role can't do the following tasks:</p> <ul style="list-style-type: none"> -Can't update sensitive properties. -Can't delete or restore users. -Can't manage MFA settings in the legacy MFA management portal or Hardware OATH tokens.
Azure AD Joined Device Local Administrator	This role is available for assignment only as another local administrator in Device settings. Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory. They don't have the ability to manage device objects in Azure Active Directory.
Azure DevOps Administrator	<p>Users with this role can manage all enterprise Azure DevOps policies applicable to all Azure DevOps organizations backed by the Azure AD.</p> <p>Users in this role can manage these policies by navigating to any Azure DevOps organization that is backed by the company's Azure AD.</p> <p>Users in this role can claim ownership of orphaned Azure DevOps organizations. This role grants no other Azure DevOps-specific permissions (for example, Project Collection Administrators) inside any of the Azure DevOps organizations backed by the company's Azure AD organization.</p>
Azure Information Protection Administrator	Users with this role have all permissions in the Azure Information Protection service. This role allows configuring labels for the Azure Information Protection policy, managing protection templates, and activating protection. This role doesn't grant any permissions in Identity Protection Center, Privileged Identity Management, Monitor Microsoft 365 Service Health, or Office 365 Security and compliance center.
Business-to-Consumer (B2C) Identity Experience Framework (IEF) Keyset Administrator	<p>Users can create and manage policy keys and secrets for token encryption, token signatures, and claim encryption/decryption.</p> <p>By adding new keys to existing key containers, this limited administrator can roll over secrets as needed without impacting existing applications.</p> <p>This user can see the full content of these secrets and their expiration dates even after their creation.</p>
Business-to-Consumer (B2C) Identity Experience Framework (IEF) Policy Administrator	Users in this role have the ability to create, read, update, and delete all custom policies in Azure AD B2C and therefore have full control over the Identity Experience Framework in the relevant Azure AD B2C organization. By editing policies, this user can establish direct federation with external identity providers, change the directory schema, change all user-facing content HyperText Markup Language (HTML), Cascading Style Sheets (CSS), JavaScript), change the requirements to complete authentication, create new users, send user data to external systems including full migrations, and edit all user information including sensitive fields like passwords and phone numbers. Conversely, this role can't change the encryption keys or edit the secrets used for federation in the organization.
Billing Administrator	Makes purchases, manages subscriptions, manages support tickets, and monitors service health.

Role	Description
Cloud App Security Administrator	Users with this role have full permissions in Defender for Cloud Apps. They can add administrators, add Microsoft Defender for Cloud Apps policies and settings, upload logs, and perform governance actions.
Cloud Application Administrator	Users in this role have the same permissions as the Application Administrator role, excluding the ability to manage application proxy. This role grants the ability to create and manage all aspects of enterprise applications and application registrations. Users assigned to this role aren't added as owners when creating new application registrations or enterprise applications. This role also grants the ability to consent for delegated permissions and application permissions, except for application permissions for Microsoft Graph.
Cloud Device Administrator	Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role doesn't grant permissions to manage any other properties on the device.
Compliance Administrator	Users with this role have permissions to manage compliance-related features in the Microsoft Purview compliance portal, Microsoft 365 admin center, Azure, and Office 365 Security and compliance center. Assignees can also manage all features within the Exchange admin center and create support tickets for Azure and Microsoft 365.
Compliance Data Administrator	Users with this role have permissions to track data in the Microsoft Purview compliance portal, Microsoft 365 admin center, and Azure. Users can also track compliance data within the Exchange admin center, Compliance Manager, and Teams and Skype for Business admin center and create support tickets for Azure and Microsoft 365.
Conditional Access Administrator	Users with this role have the ability to manage Azure Active Directory Conditional Access settings.
Customer Lockbox Access Approver	Manages Microsoft Purview Customer Lockbox requests in your organization. They receive email notifications for Customer Lockbox requests and can approve and deny requests from the Microsoft 365 admin center. They can also turn the Customer Lockbox feature on or off. Only Global Administrators can reset the passwords of people assigned to this role.
Desktop Analytics Administrator	Users in this role can manage the Desktop Analytics service, including viewing asset inventory, creating deployment plans, and viewing deployment and health status.
Directory Readers	<p>Users in this role can read basic directory information. This role should be used for:</p> <ul style="list-style-type: none"> -Granting a specific set of guest users read access instead of granting it to all guest users. -Granting a specific set of nonadmin users access to the Azure portal when "Restrict access to Azure AD portal to admins only" is set to "Yes". -Granting service principals access to the directory where Directory.Read.All isn't an option.
Directory Synchronization Accounts	Don't use. This role is automatically assigned to the Azure AD Connect service and isn't intended or supported for any other use.
Directory Writers	Users in this role can read and update basic information of users, groups, and service principals.
Domain Name Administrator	Users with this role can manage (read, add, verify, update, and delete) domain names. They can also read directory information about users, groups, and applications, as these objects possess domain dependencies. For on-premises environments, users with this role can configure domain names for federation so that associated users are always authenticated on-premises. These users can then sign into Azure AD-based services with their on-premises passwords via single sign-on. Federation settings need to be synced via Azure AD Connect so users also have permissions to manage Azure AD Connect.

Role	Description
Dynamics 365 Administrator	Users with this role have global permissions within Microsoft Dynamics 365 Online when the service is present, and the ability to manage support tickets and monitor service health.
Edge Administrator	Users in this role can create and manage the enterprise site list required for Internet Explorer mode on Microsoft Edge. This role grants permissions to create, edit, and publish the site list and additionally allows access to manage support tickets.
Exchange Administrator	Users with this role have global permissions within Microsoft Exchange Online, when the service is present. Also has the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.
Exchange Recipient Administrator	Users with this role have read access to recipients and write access to the attributes of those recipients in Exchange Online.
External ID User Flow Administrator	Users with this role can create and manage user flows (also called " built-in " policies) in the Azure portal. These users can customize HTML/CSS/JavaScript content, change MFA requirements, select claims in the token, manage API connectors and their credentials, and configure session settings for all user flows in the Azure AD organization. On the other hand, this role doesn't include the ability to review user data or make changes to the attributes that are included in the organization schema. Changes to Identity Experience Framework policies (also known as custom policies) are also outside the scope of this role.
External ID User Flow Attribute Administrator	<p>Users with this role add or delete custom attributes available to all user flows in the Azure AD organization.</p> <p>Users with this role can change or add new elements to the end-user schema and impact the behavior of all user flows, and indirectly result in changes to what data may be asked of end users and ultimately sent as claims to applications. This role can't edit user flows.</p>
External Identity Provider Administrator	<p>This administrator manages federation between Azure AD organizations and external identity providers. With this role, users can add new identity providers and configure all available settings (for example, authentication path, service ID, assigned key containers). This user can enable the Azure AD organization to trust authentications from external identity providers. The resulting impact on end-user experiences depends on the type of organization:</p> <ul style="list-style-type: none"> -Azure AD organizations for employees and partners: The addition of a federation (for example, with Gmail) immediately impacts all guest invitations not yet redeemed. See Adding Google as an identity provider for B2B guest users. -Azure Active Directory B2C organizations: The addition of a federation (for example, with Facebook, or with another Azure AD organization) doesn't immediately impact end-user flows until the identity provider is added as an option in a user flow (also called a built-in policy).
Global Administrator	Users with this role have access to all administrative features in Azure Active Directory, and services that use Azure Active Directory identities like the Microsoft 365 Defender portal, the Microsoft Purview compliance portal, Exchange Online, SharePoint Online, and Skype for Business Online. Furthermore, Global Administrators can elevate their access to manage all Azure subscriptions and management groups. This allows Global Administrators to get full access to all Azure resources using the respective Azure AD Tenant. The person who signs up for the Azure AD organization becomes a Global Administrator. There can be more than one Global Administrator at your company. Global Administrators can reset the password for any user and all other administrators.
Global Administrator	As a best practice, Microsoft recommends that you assign the Global Administrator role to fewer than five people in your organization.
Global Reader	Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions. Global Reader is the read-only counterpart to Global Administrator. Assign Global Reader instead of Global Administrator for planning, audits, or investigations. Use Global Reader in combination with other limited admin roles like Exchange Administrator to make it easier to get work done without the assigning the Global Administrator role. Global Reader works with Microsoft 365 admin center, Exchange admin center, SharePoint admin center, Teams admin center, Security center, compliance center, Azure AD admin center, and Device Management admin center.

Role	Description
	<p>Users with this role can't do the following tasks:</p> <ul style="list-style-type: none"> -Can't access the Purchase Services area in the Microsoft 365 admin center.
Groups Administrator	<p>Users in this role can create/manage groups and its settings like naming and expiration policies. It's important to understand that assigning a user to this role gives them the ability to manage all groups in the organization across various workloads like Teams, SharePoint, Yammer in addition to Outlook. Also the user is able to manage the various groups settings across various admin portals like Microsoft admin center, Azure portal, and workload specific ones like Teams and SharePoint admin centers.</p>
Guest Inviter	<p>Users in this role can manage Azure Active Directory B2B guest user invitations when the Members can invite user setting is set to No.</p>
Helpdesk Administrator	<p>Users with this role can change passwords, invalidate refresh tokens, create and manage support requests with Microsoft for Azure and Microsoft 365 services, and monitor service health. Invalidating a refresh token forces the user to sign in again. Whether a Helpdesk Administrator can reset a user's password and invalidate refresh tokens depends on the role the user is assigned.</p> <p>Users with this role can't do the following:</p> <ul style="list-style-type: none"> -Can't change the credentials or reset MFA for members and owners of a role-assignable group.
Hybrid Identity Administrator	<p>Users in this role can create, manage and deploy provisioning configuration setup from AD to Azure AD using Cloud Provisioning and manage Azure AD Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless single sign-on (Seamless SSO), and federation settings. Users can also troubleshoot and monitor logs using this role.</p>
Identity Governance Administrator	<p>Users with this role can manage Azure AD identity governance configuration, including access packages, access reviews, catalogs and policies, ensuring access is approved and reviewed and guest users who no longer need access are removed.</p>
Insights Administrator	<p>Users in this role can access the full set of administrative capabilities in the Microsoft Viva Insights app. This role has the ability to read directory information, monitor service health, file support tickets, and access the Insights Administrator settings aspects.</p>
Insights Analyst	<p>Assign the Insights Analyst role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Analyze data in the Microsoft Viva Insights app, but can't manage any configuration settings -Create, manage, and run queries -View basic settings and reports in the Microsoft 365 admin center -Create and manage service requests in the Microsoft 365 admin center
Insights Business Leader	<p>Users in this role can access a set of dashboards and insights via the Microsoft Viva Insights app. This includes full access to all dashboards and presented insights and data exploration functionality. Users in this role don't have access to product configuration settings, which is the responsibility of the Insights Administrator role.</p>
Intune Administrator	<p>Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices to associate policy and create and manage groups. This role can create and manage all security groups. However, Intune Administrator doesn't</p>

Role	Description
	have admin rights over Office groups. That means the admin can't update owners or memberships of all Office groups in the organization. However, you can manage the Office group that's created, which comes as a part of end-user privileges. So, any Office group (not security group) that you create should be counted against your quota of 250.
Kaizala Administrator	Users with this role have global permissions to manage settings within Microsoft Kaizala, when the service is present and the ability to manage support tickets and monitor service health. Additionally, the user can access reports related to adoption and usage of Kaizala by Organization members and business reports generated using the Kaizala actions.
Knowledge Administrator	Users in this role have full access to all knowledge, learning and intelligent features settings in the Microsoft 365 admin center. They have a general understanding of the suite of products, licensing details and have responsibility to control access. Knowledge Administrator can create and manage content, like topics, acronyms and learning resources. Additionally, these users can create content centers, monitor service health, and create service requests.
Knowledge Manager	Users in this role can create and manage content, like topics, acronyms and learning content. These users are primarily responsible for the quality and structure of knowledge. This user has full rights to topic management actions to confirm a topic, approve edits, or delete a topic. This role can also manage taxonomies as part of the term store management tool and create content centers.
License Administrator	Users in this role can add, remove, and update license assignments on users, groups (using group-based licensing), and manage the usage location on users. The role doesn't grant the ability to purchase or manage subscriptions, create or manage groups, or create or manage users beyond the usage location. This role has no access to view, create, or manage support tickets.
Lifecycle Workflows Administrator	Assign the Lifecycle Workflows Administrator role to users who need to do the following tasks: <ul style="list-style-type: none"> -Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Azure AD -Check the execution of scheduled workflows -Launch on-demand workflow runs -Inspect workflow execution logs
Message Center Privacy Reader	Users in this role can monitor all notifications in the Message Center, including data privacy messages. Message Center Privacy Readers get email notifications including those related to data privacy and they can unsubscribe using Message Center Preferences. Only the Global Administrator and the Message Center Privacy Reader can read data privacy messages. Additionally, this role contains the ability to view groups, domains, and subscriptions. This role has no permission to view, create, or manage service requests.
Message Center Reader	Users in this role can monitor notifications and advisory health updates in Message center for their organization on configured services such as Exchange, Intune, and Microsoft Teams. Message Center Readers receive weekly email digests of posts, updates, and can share message center posts in Microsoft 365. In Azure AD, users assigned to this role will only have read-only access on Azure AD services such as users and groups. This role has no access to view, create, or manage support tickets.
Microsoft Hardware Warranty Administrator	Assign the Microsoft Hardware Warranty Administrator role to users who need to do the following tasks: <ul style="list-style-type: none"> -Create new warranty claims for Microsoft manufactured hardware, like Surface and HoloLens -Search and read opened or closed warranty claims -Search and read warranty claims by serial number -Create, read, update, and delete shipping addresses

Role	Description
	<ul style="list-style-type: none"> -Read shipping status for open warranty claims -Create and manage service requests in the Microsoft 365 admin center -Read Message center announcements in the Microsoft 365 admin center
Microsoft Hardware Warranty Specialist	<p>Assign the Microsoft Hardware Warranty Specialist role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Create new warranty claims for Microsoft manufactured hardware, like Surface and HoloLens -Read warranty claims that they created -Read and update existing shipping addresses -Read shipping status for open warranty claims they created -Create and manage service requests in the Microsoft 365 admin center
Modern Commerce User	<p>Don't use. This role is automatically assigned from Commerce, and isn't intended or supported for any other use.</p> <p>The Modern Commerce User role gives certain users permission to access Microsoft 365 admin center and see the left navigation entries for Home, Billing, and Support. The content available in these areas is controlled by commerce-specific roles assigned to users to manage products that they bought for themselves or your organization. This might include tasks like paying bills, or for access to billing accounts and billing profiles. Users with the Modern Commerce User role typically have administrative permissions in other Microsoft purchasing systems, but don't have Global Administrator or Billing Administrator roles used to access the admin center.</p>
Network Administrator	<p>Users in this role can review network perimeter architecture recommendations from Microsoft that are based on network telemetry from their user locations. Network performance for Microsoft 365 relies on careful enterprise customer network perimeter architecture, which is generally user location specific. This role allows for editing of discovered user locations and configuration of network parameters for those locations to facilitate improved telemetry measurements and design recommendations</p>
Office Apps Administrator	<p>Users in this role can manage Microsoft 365 apps' cloud settings. This includes managing cloud policies, self-service download management and the ability to view Office apps related report. This role additionally grants the ability to manage support tickets, and monitor service health within the main admin center. Users assigned to this role can also manage communication of new features in Office apps.</p>
Organizational Messages Writer	<p>Assign the Organizational Messages Writer role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Write, publish, and delete organizational messages using Microsoft 365 admin center or Microsoft Endpoint Manager -Manage organizational message delivery options using Microsoft 365 admin center or Microsoft Endpoint Manager -Read organizational message delivery results using Microsoft 365 admin center or Microsoft Endpoint Manager -View usage reports and most settings in the Microsoft 365 admin center, but can't make changes
Partner Tier1 Support	<p>Don't use. This role has been deprecated and will be removed from Azure AD in the future. This role is intended for use by a few Microsoft resale partners, and isn't intended for general use.</p>
Partner Tier2 Support	<p>Don't use. This role has been deprecated and will be removed from Azure AD in the future. This role is intended for use by a few Microsoft resale partners, and isn't intended for general use.</p>
Password Administrator	<p>Users with this role have limited ability to manage passwords. This role doesn't grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned. Users with this role can't do the following tasks:</p>

Role	Description
	-Can't change the credentials or reset MFA for members and owners of a role-assignable group.
Permissions Management Administrator	<p>Assign the Permissions Management Administrator role to users who need to do the following tasks:</p> <p>-Manage all aspects of Entra Permissions Management, when the service is present</p>
Power Business Intelligence (BI) Administrator	Users with this role have global permissions within Microsoft Power BI, when the service is present and the ability to manage support tickets and monitor service health.
Power Platform Administrator	Users in this role can create and manage all aspects of environments, Power Apps, Flows, Data Loss Prevention policies. Additionally, users with this role have the ability to manage support tickets and monitor service health.
Printer Administrator	Users in this role can register printers and manage all aspects of all printer configurations in the Microsoft Universal Print solution, including the Universal Print Connector settings. They can consent to all delegated print permission requests. Printer Administrators also have access to print reports.
Printer Technician	Users with this role can register printers and manage printer status in the Microsoft Universal Print solution. They can also read all connector information. Key task a Printer Technician can't do is set user permissions on printers and sharing printers.
Privileged Authentication Administrator	<p>Assign the Privileged Authentication Administrator role to users who need to do the following tasks:</p> <p>-Set or reset any authentication method (including passwords) for any user, including Global Administrators.</p> <p>-Delete or restore any users, including Global Administrators. For more information, see Who can perform sensitive actions.</p> <p>-Force users to re-register against existing nonpassword credential (such as MFA or FIDO) and revoke remember MFA on the device, prompting for MFA on the next sign-in of all users.</p> <p>-Update sensitive properties for all users. For more information, see Who can perform sensitive actions.</p> <p>-Create and manage support tickets in Azure and the Microsoft 365 admin center.</p> <p>Users with this role can't do the following tasks:</p> <p>-Can't manage per-user MFA in the legacy MFA management portal. The same functions can be accomplished using the Set-MsolUser commandlet Azure AD PowerShell module.</p>
Privileged Role Administrator	Users with this role can manage role assignments in Azure Active Directory and within Azure AD Privileged Identity Management. They can create and manage groups that can be assigned to Azure AD roles. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Role	Description
Privileged Role Administrator	This role grants the ability to manage assignments for all Azure AD roles including the Global Administrator role. This role doesn't include any other privileged abilities in Azure AD like creating or updating users. However, users assigned to this role can grant themselves or others another privilege by assigning extra roles.
Reports Reader	Users with this role can view usage reporting data and the reports dashboard in Microsoft 365 admin center and the adoption context pack in Power Business Intelligence (Power BI). Additionally, the role provides access to all sign-in logs, audit logs, and activity reports in Azure AD and data returned by the Microsoft Graph reporting API. A user assigned to the Reports Reader role can access only relevant usage and adoption metrics. They don't have any admin permissions to configure settings or access the product-specific admin centers like Exchange. This role has no access to view, create, or manage support tickets.
Search Administrator	Users in this role have full access to all Microsoft Search management features in the Microsoft 365 admin center. Additionally, these users can view the message center, monitor service health, and create service requests.
Search Editor	Users in this role can create, manage, and delete content for Microsoft Search in the Microsoft 365 admin center, including bookmarks, questions and answers, and locations.
Security Administrator	Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Azure Active Directory Identity Protection, Azure Active Directory Authentication, Azure Information Protection, and Office 365 Security and compliance center.
Security Operator	Users with this role can manage alerts and have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management and Office 365 Security & compliance center.
Security Reader	Users with this role have global read-only access on security-related feature, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, and the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security and compliance center.
Service Support Administrator	Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center.
SharePoint Administrator	Users with this role have global permissions within Microsoft SharePoint Online, when the service is present, and the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.
Skype for Business Administrator	Users with this role have global permissions within Microsoft Skype for Business, when the service is present, and manage Skype-specific user attributes in Azure Active Directory. Additionally, this role grants the ability to manage support tickets and monitor service health, and to access the Teams and Skype for Business admin center. The account must also be licensed for Teams or it can't run Teams PowerShell cmdlets.
Teams Administrator	Users in this role can manage all aspects of the Microsoft Teams workload via the Microsoft Teams and Skype for Business admin center and the respective PowerShell modules. This includes, among other areas, all management tools related to telephony, messaging, meetings, and the teams themselves. This role additionally grants the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.
Teams Communications Administrator	Users in this role can manage aspects of the Microsoft Teams workload related to voice and telephony. This includes the management tools for telephone number assignment, voice and meeting policies, and full access to the call analytics toolset.

Role	Description
Teams Communications Support Engineer	Users in this role can troubleshoot communication issues within Microsoft Teams and Skype for Business using the user call troubleshooting tools in the Microsoft Teams and Skype for Business admin center. Users in this role can view full call record information for all participants involved. This role has no access to view, create, or manage support tickets.
Teams Communications Support Specialist	Users in this role can troubleshoot communication issues within Microsoft Teams and Skype for Business using the user call troubleshooting tools in the Microsoft Teams and Skype for Business admin center. Users in this role can only view user details in the call for the specific user they've looked up. This role has no access to view, create, or manage support tickets.
Teams Devices Administrator	Users with this role can manage Teams-certified devices from the Teams admin center. This role allows viewing all devices at single glance, with ability to search and filter devices. The user can check details of each device including logged-in account, make and model of the device. The user can change the settings on the device and update the software versions. This role doesn't grant permissions to check Teams activity and call quality of the device.
Tenant Creator	<p>Assign the Tenant Creator role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Create both Azure Active Directory and Azure Active Directory B2C tenants even if the tenant creation toggle is turned off in the user settings
Usage Summary Reports Reader	Users with this role can access tenant level aggregated data and associated insights in Microsoft 365 admin center for Usage and Productivity Score but can't access any user level details or insights. In Microsoft 365 admin center for the two reports, we differentiate between tenant level aggregated data and user level details. This role gives an extra layer of protection on individual user identifiable data, which was requested by both customers and legal teams.
User Administrator	<p>Assign the User Administrator role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Create users -Update most user properties for all users, including all administrators -Update sensitive properties (including user principal name) for some users -Disable or enable some users -Delete or restore some users -Create and manage user views -Create and manage all groups -Assign licenses for all users, including all administrators -Reset passwords -Invalidate refresh tokens

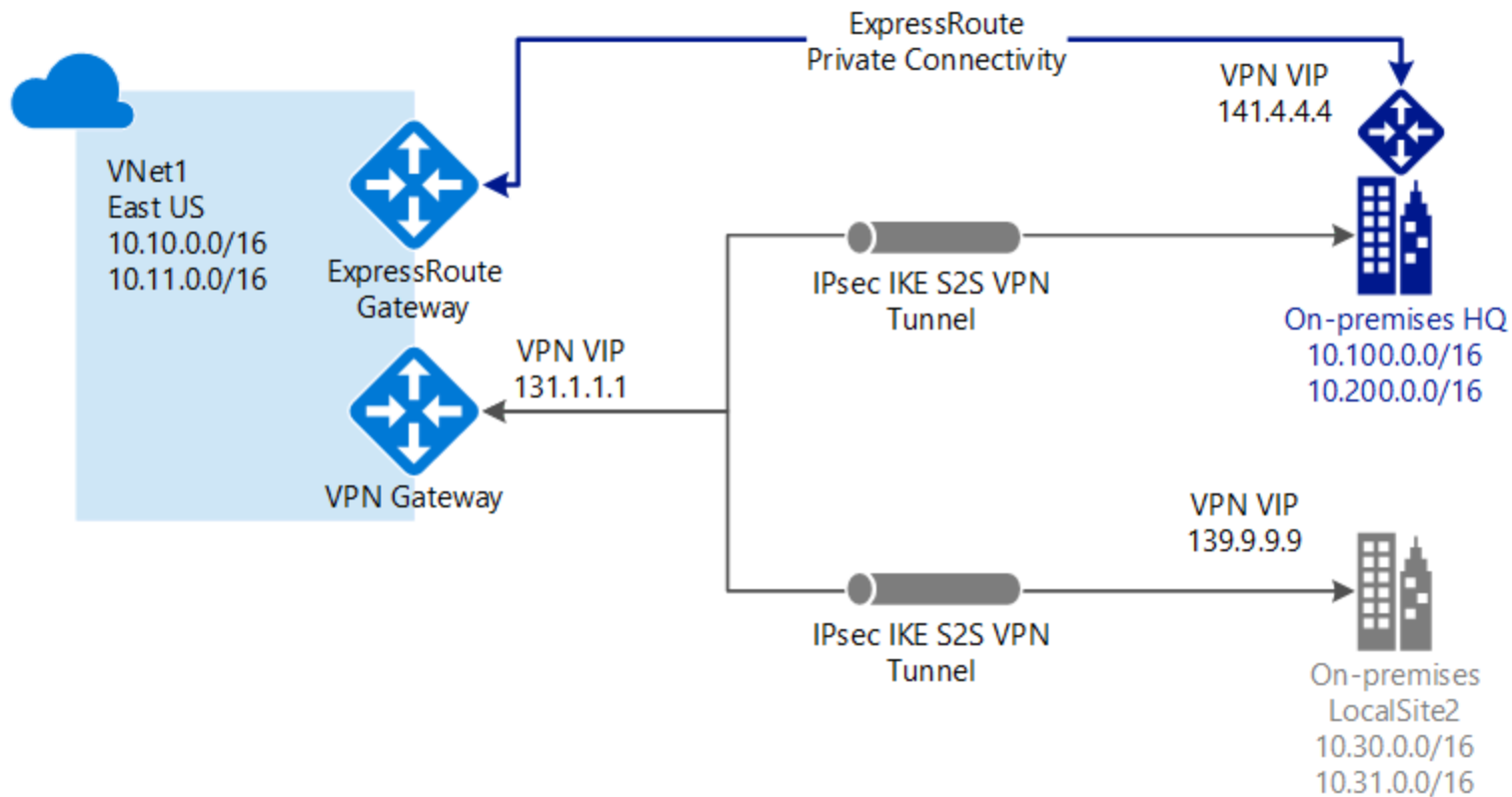
Role	Description
	<ul style="list-style-type: none"> -Update (FIDO) device keys -Update password expiration policies -Create and manage support tickets in Azure and the Microsoft 365 admin center -Monitor service healthUsers with this role can't do the following tasks: -Can't manage MFA. -Can't change the credentials or reset MFA for members and owners of a role-assignable group. -Can't manage shared mailboxes
User Administrator	<p>Users with this role can change passwords for people who may have access to sensitive or private information or critical configuration inside and outside of Azure Active Directory. Changing the password of a user may mean the ability to assume that user's identity and permissions.</p> <p>For example:</p> <ul style="list-style-type: none"> -Application Registration and Enterprise Application owners, who can manage credentials of apps they own. Those apps may have privileged permissions in Azure AD and elsewhere not granted to User Administrators. Through this path, a User Administrator may be able to assume the identity of an application owner and then further assume the identity of a privileged application by updating the credentials for the application. -Azure subscription owners, who may have access to sensitive or private information or critical configuration in Azure. -Security Group and Microsoft 365 group owners, who can manage group membership. Those groups may grant access to sensitive or private information or critical configuration in Azure AD and elsewhere. -Administrators in other services outside of Azure AD like Exchange Online, Office Security and compliance center, and human resources systems. -Nonadministrators like executives, legal counsel, and human resources employees who may have access to sensitive or private information.
Virtual Visits Administrator	<p>Users with this role can do the following tasks:</p> <ul style="list-style-type: none"> -Manage and configure all aspects of Virtual Visits in Bookings in the Microsoft 365 admin center, and in the Teams Electronic Health Record (EHR) connector -View usage reports for Virtual Visits in the Teams admin center, Microsoft 365 admin center, and Power BI -View features and settings in the Microsoft 365 admin center, but can't edit any settings
Windows 365 Administrator	<p>Users with this role have global permissions on Windows 365 resources, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy and create and manage groups.</p>

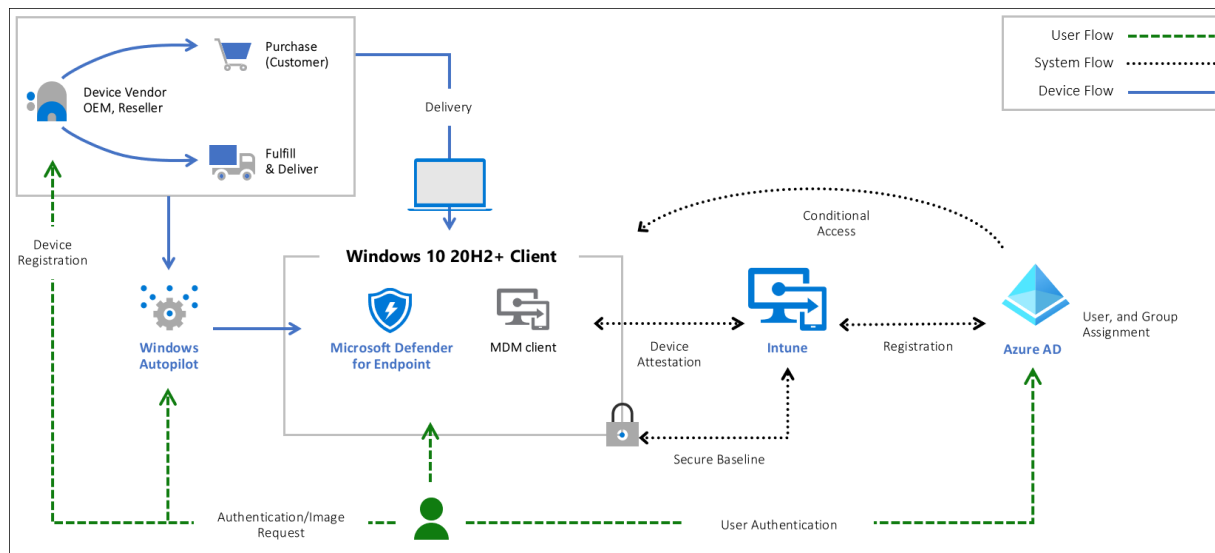
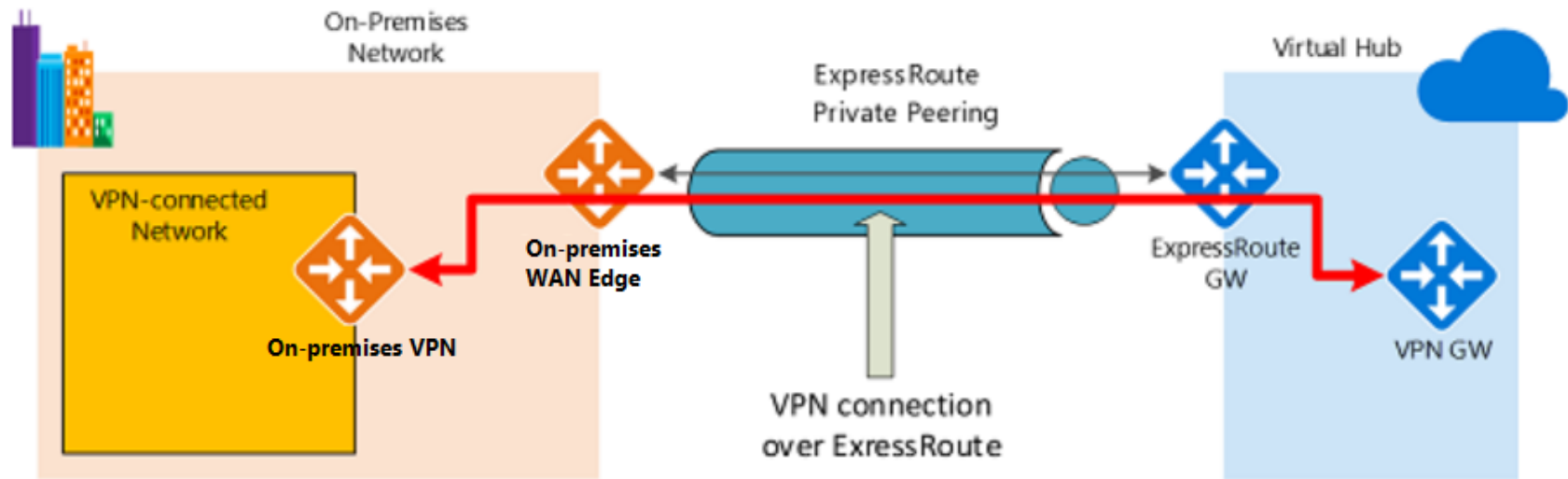
Role	Description
	<p>This role can create and manage security groups, but doesn't have administrator rights over Microsoft 365 groups. That means administrators can't update owners or memberships of Microsoft 365 groups in the organization. However, they can manage the Microsoft 365 group they create, which is a part of their end-user privileges. So, any Microsoft 365 group (not security group) they create is counted against their quota of 250.</p> <p>Assign the Windows 365 Administrator role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Manage Windows 365 Cloud PCs in Microsoft Endpoint Manager -Enroll and manage devices in Azure AD, including assigning users and policies -Create and manage security groups, but not role-assignable groups -View basic properties in the Microsoft 365 admin center -Read usage reports in the Microsoft 365 admin center -Create and manage support tickets in Azure and the Microsoft 365 admin center
Windows Update Deployment Administrator	<p>Users in this role can create and manage all aspects of Windows Update deployments through the Windows Update for Business deployment service. The deployment service enables users to define settings for when and how updates are deployed, and specify which updates are offered to groups of devices in their tenant. It also allows users to monitor the update progress.</p>
Yammer Administrator	<p>Assign the Yammer Administrator role to users who need to do the following tasks:</p> <ul style="list-style-type: none"> -Manage all aspects of Yammer -Create, manage, and restore Microsoft 365 Groups, but not role-assignable groups -View the hidden members of Security groups and Microsoft 365 groups, including role assignable groups -Read usage reports in the Microsoft 365 admin center -Create and manage service requests in the Microsoft 365 admin center -View announcements in the Message center, but not security announcements -View service health

Features included with Front Door:

- **Accelerate application performance** - Using split TCP-based anycast protocol, Front Door ensures that your end users promptly connect to the nearest Front Door POP (Point of Presence).
- **Increase application availability with smart health probes** - Front Door delivers high availability for your critical applications using its smart health probes, monitoring your backends for both latency and availability and providing instant automatic failover when a backend goes down.
- **URL-based routing** - URL Path Based Routing allows you to route traffic to backend pools based on URL paths of the request. One of the scenarios is to route requests for different content types to different backend pools.
- **Multiple-site hosting** - Multiple-site hosting enables you to configure more than one web site on the same Front Door configuration.
- **Session affinity** - The cookie-based session affinity feature is useful when you want to keep a user session on the same application backend.
- **TLS termination** - Front Door supports TLS termination at the edge that is, individual users can set up a TLS connection with Front Door environments instead of establishing it over long haul connections with the application backend.

- **Custom domains and certificate management** - When you use Front Door to deliver content, a custom domain is necessary if you would like your own domain name to be visible in your Front Door URL.
- **Application layer security** - Azure Front Door allows you to author custom Web Application Firewall (WAF) rules for access control to protect your HTTP/HTTPS workload from exploitation based on client IP addresses, country code, and http parameters.
- **URL redirection** - With the strong industry push on supporting only secure communication, web applications are expected to automatically redirect any HTTP traffic to HTTPS.
- **URL rewrite** - Front Door supports URL rewrite by allowing you to configure an optional Custom Forwarding Path to use when constructing the request to forward to the backend.
- **Protocol support - IPv6 and HTTP/2 traffic** - Azure Front Door natively supports end-to-end IPv6 connectivity and HTTP/2 protocol.

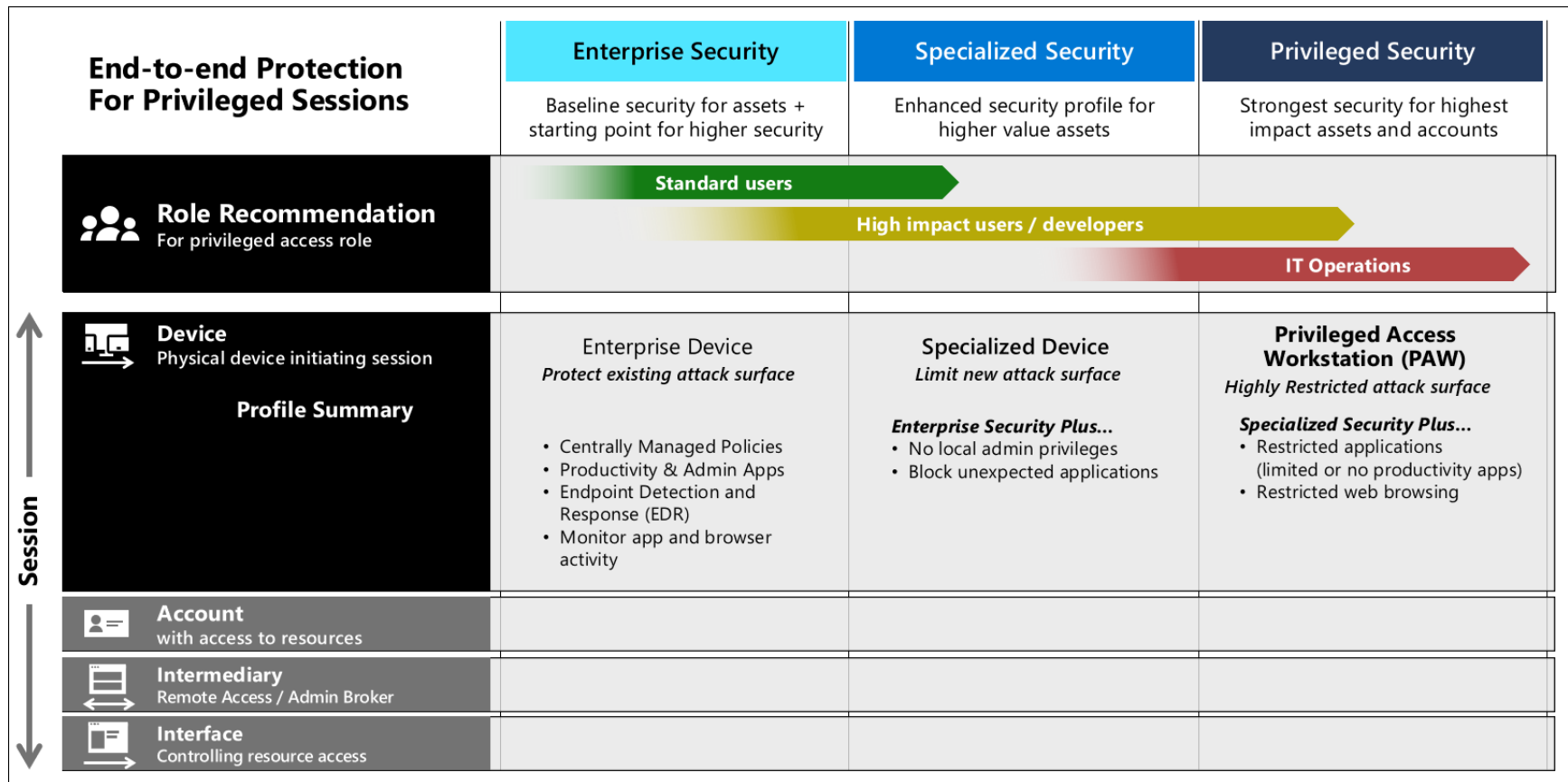




Hardware root-of-trust

To have a secured workstation you need to make sure the following security technologies are included on the device:

- Trusted Platform Module (TPM) 2.0
- BitLocker Drive Encryption
- UEFI Secure Boot
- Drivers and Firmware Distributed through Windows Update
- Virtualization and HVCI Enabled
- Drivers and Apps HVCI-Ready
- Windows Hello
- DMA I/O Protection
- System Guard
- Modern Standby



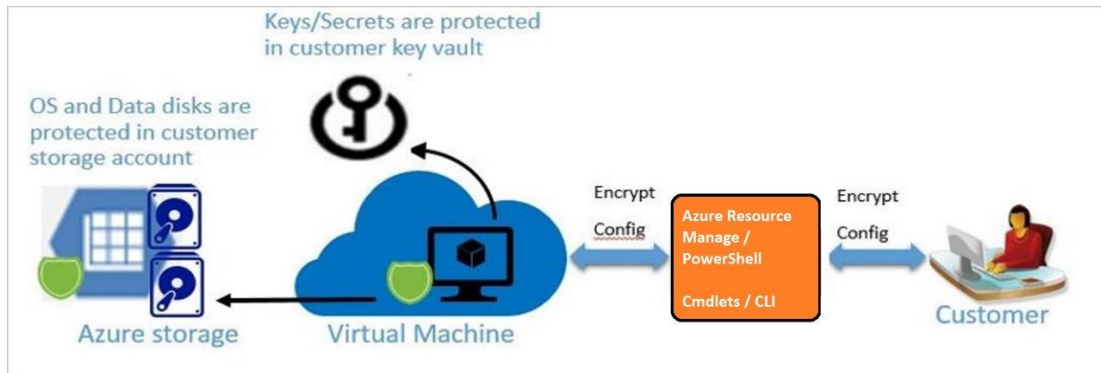
Levels of device security

Device Type	Common usage scenario	Permitted activities	Security guidance
Enterprise Device	Home users, small business users, general purpose developers, and enterprise	Run any application, browse any website	Anti-malware and virus protection and policy based security posture for the enterprise.
Specialized Device	Specialized or secure enterprise users	Run approved applications, but cannot install apps. Email and web browsing allowed. No admin controls	No self administration of device, no application installation, policy based security, and endpoint management
Privileged Device	Extremely sensitive roles	IT Operations	No local admins, no productivity tools, locked down browsing. PAW device

Device security controls

A secure workstation requires it be part of an end-to-end approach including device security, account security, and security policies applied to the device at all times. Here are some common security measures you should consider implementing based on the users needs. Using a device with security measures directly aligned to the security needs of it users is the more secure solution.

Security Control	Enterprise Device	Specialized Device	Privileged Device
Microsoft Endpoint Manager (MEM) managed	Yes	Yes	Yes
Deny BYOD Device enrollment	No	Yes	Yes
MEM security baseline applied	Yes	Yes	Yes
Microsoft Defender for Endpoint	Yes	Yes	Yes
Join personal device via Autopilot	Yes	Yes	No
URLs restricted to approved list	Allow Most	Allow Most	Deny Default
Removal of admin rights		Yes	Yes
Application execution control (AppLocker)		Audit -> Enforced	Yes
Applications installed only by MEM		Yes	Yes



Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security posture

Showing subscription 'MCAPS-Hybrid-REQ-48118-2022-serlingdavis'

Search

Secure score over time Governance report Guides & Feedback

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture**
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

Azure environment

1 Secure score

60% SECURE SCORE

Environment

- 3 Management groups
- 1 Subscriptions
- 2/5 Unhealthy resources
- 25 Recommendations

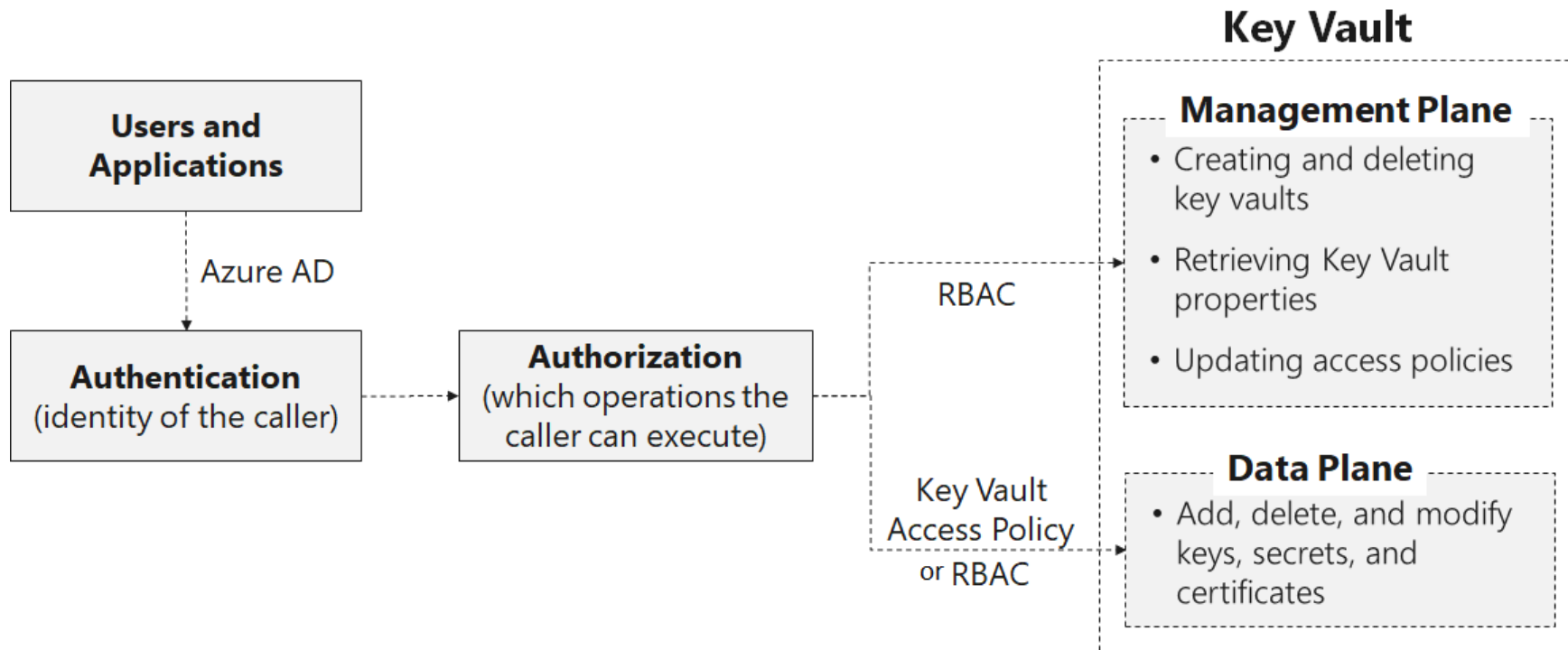
Environment Owner

Search by name Environment == All

Name ↑↓	Secure score ↑↓	Unhealthy resources ↑↓
Tenant Root Group Azure management group	60%	2 of 5
MCAPS-Root Azure management group	60%	2 of 5

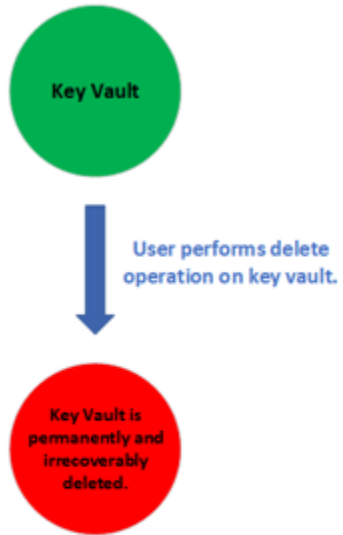
The following table lists security best practices for using Key Vault.

Best practice	Solution
Grant access to users, groups, and applications at a specific scope.	Use RBAC's predefined roles. For example, to grant access to a user to manage key vaults, you would assign the predefined role Key Vault Contributor to this user at a specific scope. The scope in this case would be a subscription, a resource group, or just a specific key vault. If the predefined roles don't fit your needs, you can define your own roles.
Control what users have access to.	Access to a key vault is controlled through two separate interfaces: management plane, and data plane. The management plane and data plane access controls work independently. Use RBAC to control what users have access to. For example, if you want to grant an application access to use keys in a key vault, you only need to grant data plane access permissions by using key vault access policies, and no management plane access is needed for this application. Conversely, if you want a user to be able to read vault properties and tags but not have any access to keys, secrets, or certificates, you can grant this user read access by using RBAC, and no access to the data plane is required.
Store certificates in your key vault.	Azure Resource Manager can securely deploy certificates stored in Azure Key Vault to Azure VMs when the VMs are deployed. By setting appropriate access policies for the key vault, you also control who gets access to your certificate. Another benefit is that you manage all your certificates in one place in Azure Key Vault.
Ensure that you can recover a deletion of key vaults or key vault objects.	Deletion of key vaults or key vault objects can be either inadvertent or malicious. Enable the soft delete and purge protection features of Key Vault, particularly for keys that are used to encrypt data at rest. Deletion of these keys is equivalent to data loss, so you can recover deleted vaults and vault objects if needed. Practice Key Vault recovery operations on a regular basis.

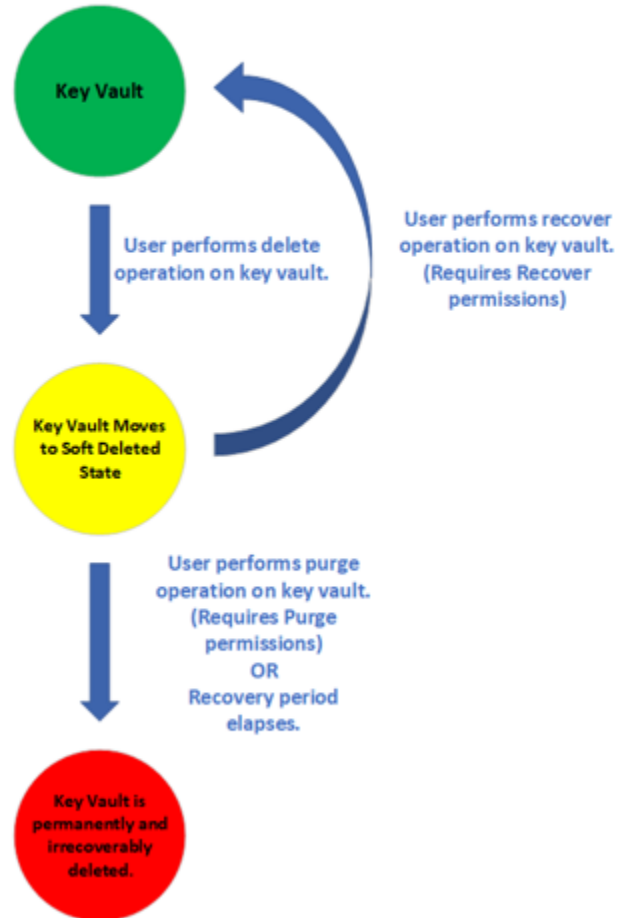


Role	Management plane permissions	Data plane permissions
Security team	Key Vault Contributor	Keys: backup, create, delete, get, import, list, restore. Secrets: all operations
Developers and operators	Key Vault deploy permission Note: This permission allows deployed VMs to fetch secrets from a key vault.	None
Auditors	None	Keys: list Secrets: list. Note: This permission enables auditors to inspect attributes (tags, activation dates, expiration dates) for keys and secrets not emitted in the logs.
Application	None	Keys: sign Secrets: get

Without Soft Delete Protection

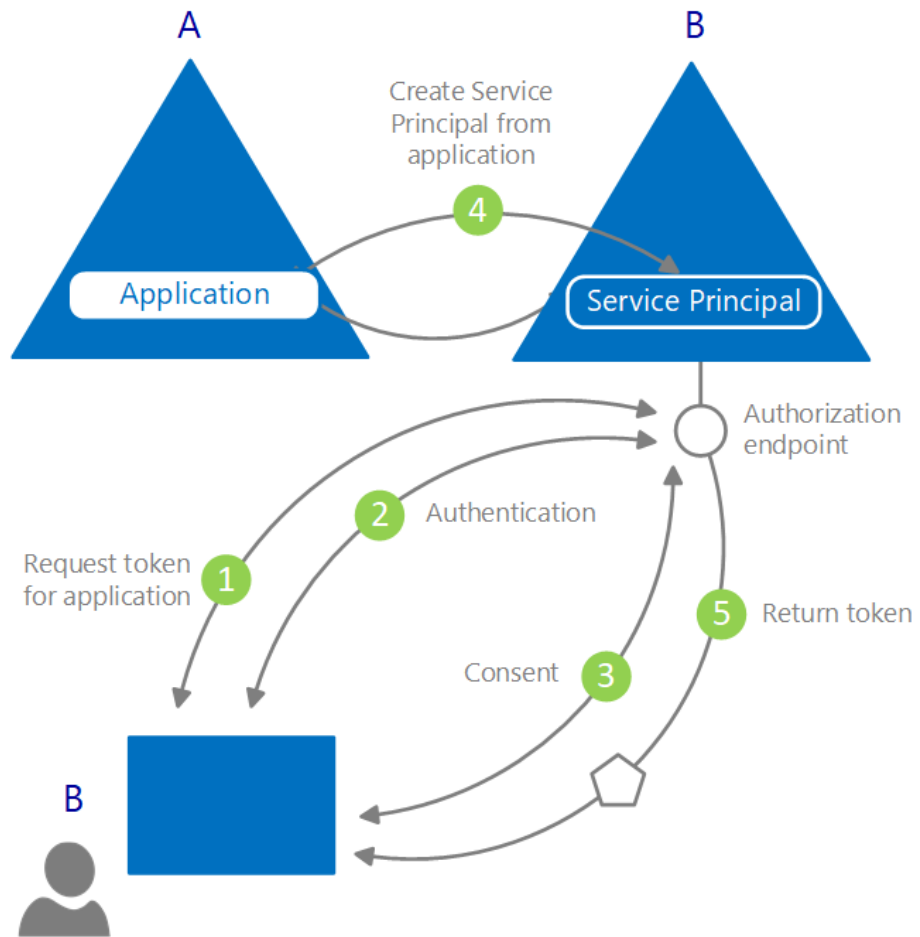


With Soft Delete Protection





Azure AD application scenarios

Frontend	Authentication	Backend
Single page application are frontends that run in a browser	Azure AD Authorization Endpoint	Web API
Web apps are applications that authenticate a user in a web browser to a web application	Azure AD WS-Federation or SAML Endpoint	Web application
Native apps are applications that call a web API on behalf of a user	Azure AD Authorization Endpoint and Azure AD Token Endpoint	Web API
Web API apps are web applications that need to get resources from a web API	Azure AD Authorization Endpoint and Azure AD Token Endpoint	Web application and Web API
Service-to-service applications are daemon or server application that needs to get resources from a web API	Azure AD Authorization Endpoint and Azure AD Token Endpoint	Web API



[Home](#) > [App registrations](#) >

Register an application ...

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#) 

* Name

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

Supported account types


Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Microsoft only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only


[Help me choose...](#)

Redirect URI (optional)

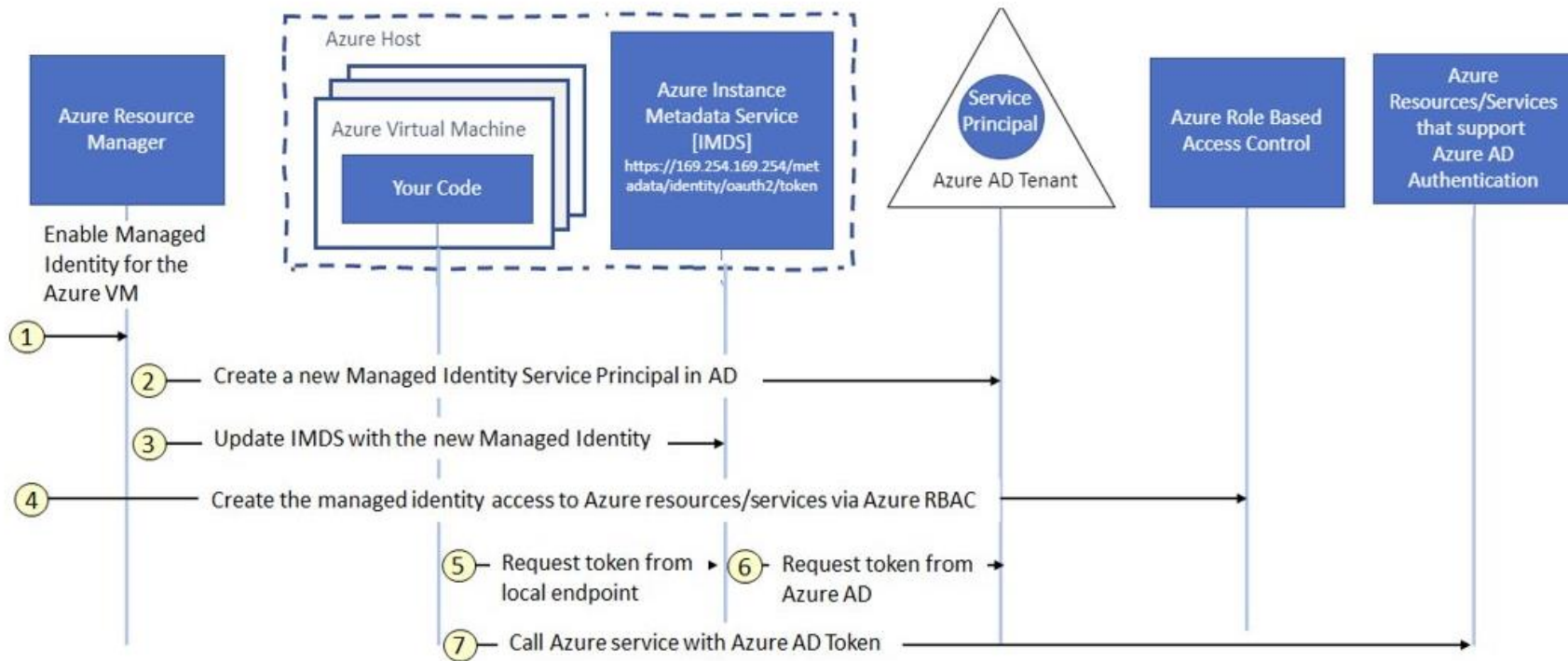
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web 	e.g. https://example.com/auth
---	--

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

By proceeding, you agree to the [Microsoft Platform Policies](#) 

Register



Azure App Service is a fully managed platform as a service (PaaS) offering for developers that allows you to host web applications, REST APIs, and mobile backends. With App Service, you can use your favorite language or framework, such as .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python, and run your apps on Windows or Linux-based environments.

Some key features of App Service include:

- Multiple languages and frameworks
- Managed production environment
- Containerization and Docker
- DevOps optimization
- Global scale with high availability
- Connections to SaaS platforms and on-premises data

- Security and compliance
- Application templates
- Visual Studio and Visual Studio Code integration
- API and mobile features
- Serverless code

App Service is a pay-as-you-go service, where you pay for the compute resources you use. The service offers features such as security, load balancing, autoscaling, and automated management, as well as DevOps capabilities like continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and TLS/SSL certificates.

While Azure offers other services that can be used for hosting websites and web applications, App Service is the best choice for most scenarios.

Azure App Service is a fully managed PaaS offering for hosting web apps, REST APIs, and mobile backends. It supports multiple languages and frameworks, containerization, DevOps optimization, global scale, connections to SaaS platforms and on-premises data, security, compliance, and more.

App Service is a pay-as-you-go service that provides features like security, load balancing, autoscaling, automated management, and DevOps capabilities. It is the best choice for most scenarios.

An app service runs in an App Service plan that defines a set of compute resources for a web app to run. The plan determines the operating system, region, number, and size of VM instances, and pricing tier. There are shared compute, dedicated compute, and isolated pricing tiers available.

Visual Summary:

Azure App Service:

- Fully managed PaaS offering for web apps, REST APIs, and mobile backends
- Supports multiple languages and frameworks
- Containerization, DevOps optimization, global scale, connections to SaaS platforms and on-premises data, security, compliance, and more
- Pay-as-you-go service with security, load balancing, autoscaling, automated management, and DevOps capabilities
- Best choice for most scenarios

App Service Plan:

- Defines a set of compute resources for a web app to run
- Determines the operating system, region, number, and size of VM instances, and pricing tier
- Shared compute, dedicated compute, and isolated pricing tiers available

	Microsoft-managed keys	Customer-managed keys	Customer-provided keys
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob storage, Azure Files	Blob storage
Key storage	Microsoft key store	Azure Key Vault	Azure Key Vault or any other key store
Key rotation responsibility	Microsoft	Customer	Customer
Key usage	Microsoft	Azure portal, Storage Resource Provider REST API, Azure Storage management libraries, PowerShell, CLI	Azure Storage REST API (Blob storage), Azure Storage client libraries
Key access	Microsoft only	Microsoft, Customer	Customer only