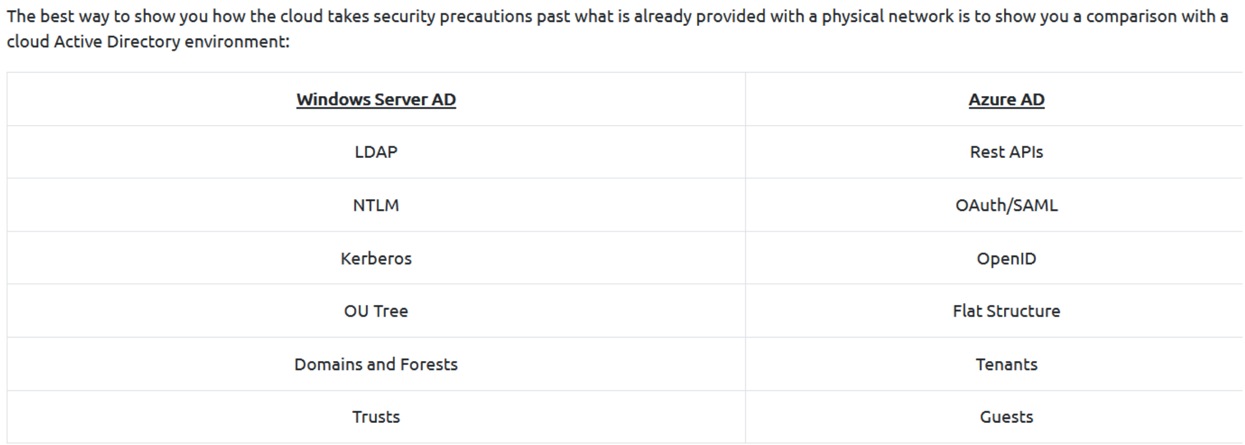
AZ-500 Links

https://aka.ms/ESIStudyGuide_AZ-500

https://www.measureup.com/az-500-microsoft-azure-security-technologies.html

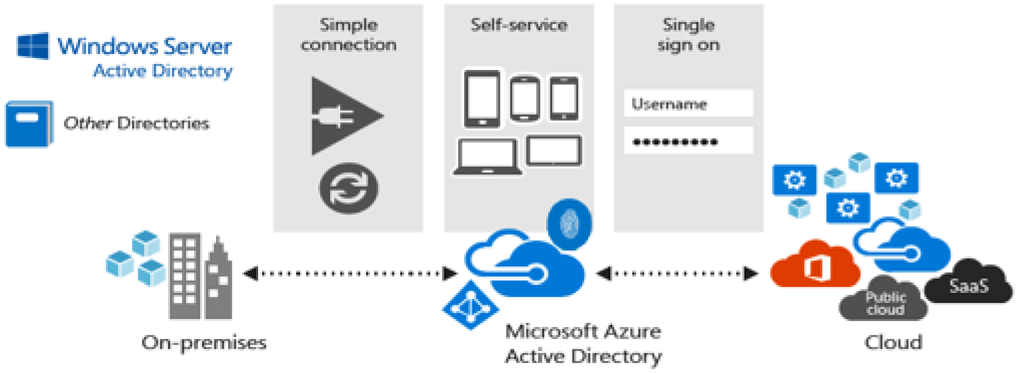
https://docs.microsoft.com/en-us/learn/certifications/exams/az-500

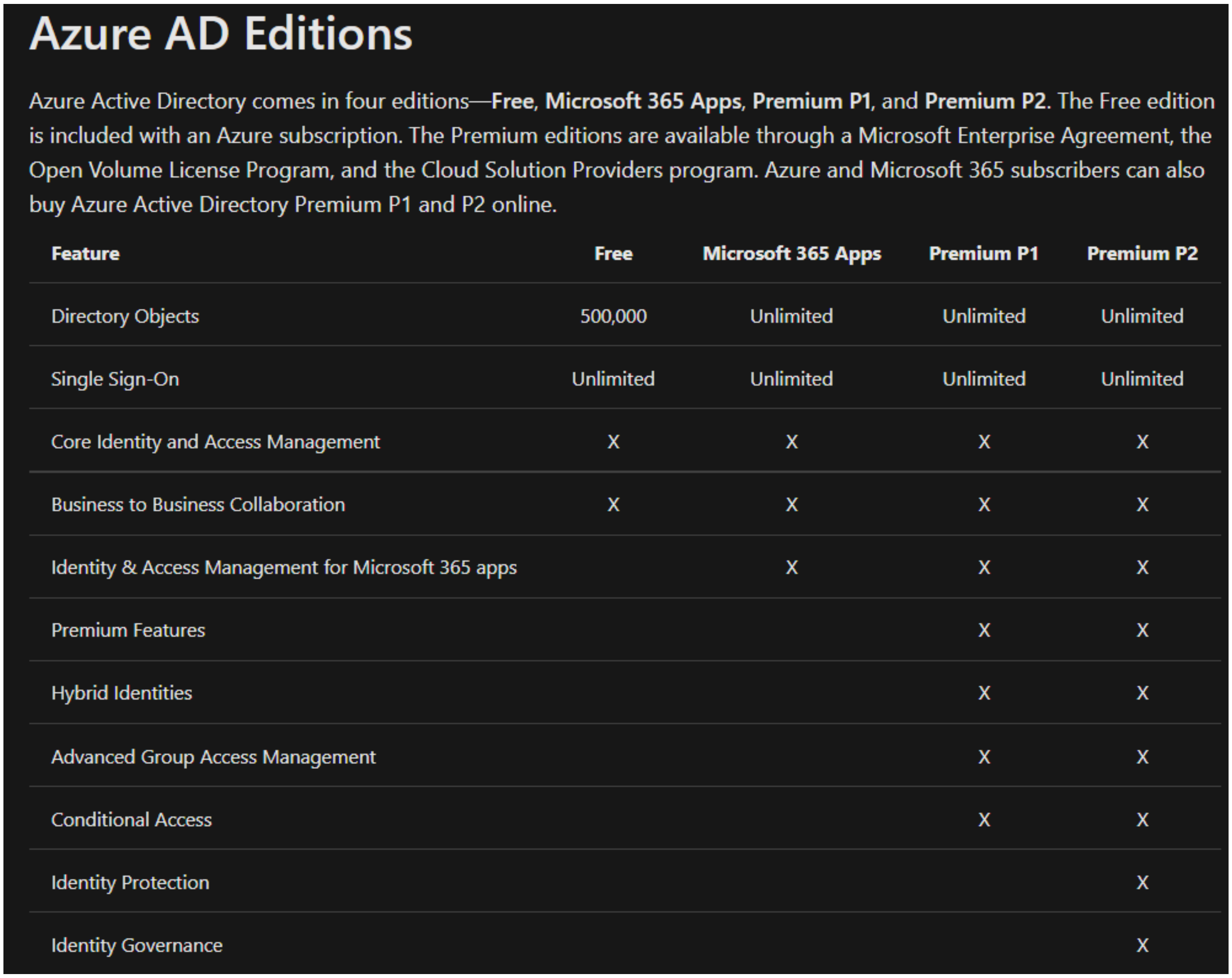


The best way to show you how the cloud takes security precautions past what is already provided with a physical network is to show you a comparison with a cloud Active Directory environment:

Windows Server AD	Azure AD
LDAP	Rest APIs
NTLM	OAuth/SAML
Kerberos	OpenID
OU Tree	Flat Structure
Domains and Forests	Tenants
Trusts	Guests

Azure Directory





Azure AD Editions

Azure Active Directory comes in four editions—**Free**, **Microsoft 365 Apps**, **Premium P1**, and **Premium P2**. The Free edition is included with an Azure subscription. The Premium editions are available through a Microsoft Enterprise Agreement, the Open Volume License Program, and the Cloud Solution Providers program. Azure and Microsoft 365 subscribers can also buy Azure Active Directory Premium P1 and P2 online.

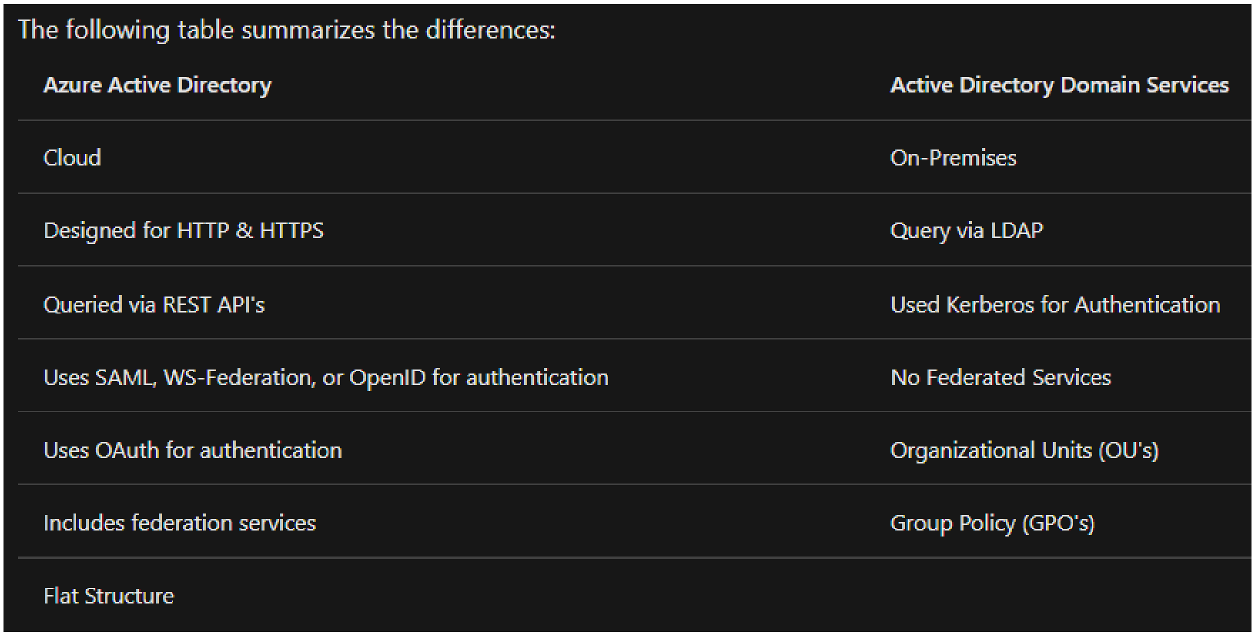
Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-On	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	X	X	X	X
Business to Business Collaboration	X	X	X	X
Identity & Access Management for Microsoft 365 apps		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access Management			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

- **Azure Active Directory Free** – Provides user and group management, on-premises directory synchronization, basic reports, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.

- **Azure Active Directory Microsoft 365 Apps** - This edition is included with O365. In addition to the Free features, this edition provides Identity & Access Management for Microsoft 365 apps including branding, MFA, group access management, and self-service password reset for cloud users.

- **Azure Active Directory Premium P1** - In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

- **Azure Active Directory Premium P2** - In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.



The following table summarizes the differences:

Azure Active Directory	Active Directory Domain Services
Cloud	On-Premises
Designed for HTTP & HTTPS	Query via LDAP
Queried via REST API's	Used Kerberos for Authentication
Uses SAML, WS-Federation, or OpenID for authentication	No Federated Services
Uses OAuth for authentication	Organizational Units (OU's)
Includes federation services	Group Policy (GPO's)
Flat Structure	

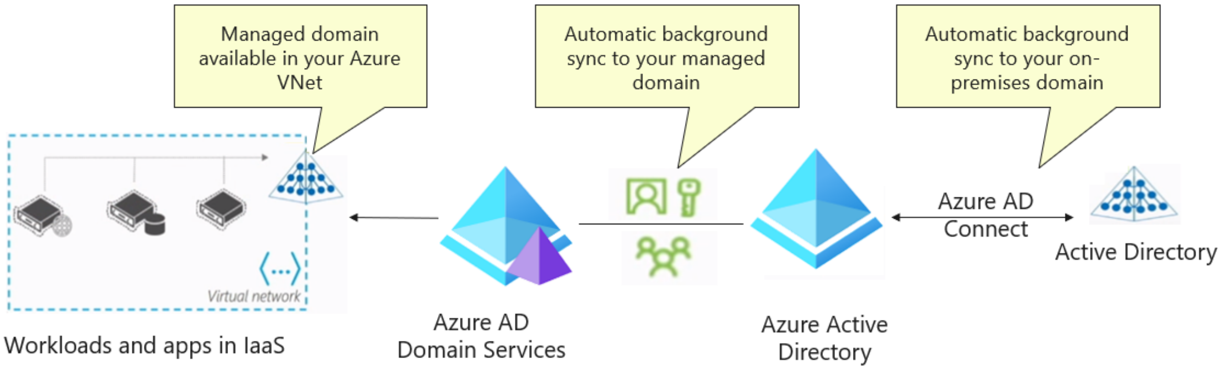
Users who are assigned to the Global administrator role can read and modify every administrative setting in your Azure AD organization. By default, the person who signs up for an Azure subscription is assigned the Global administrator role for the Azure AD organization. Only Global administrators and Privileged Role administrators can delegate administrator roles. To reduce the risk to your business, we recommend that you assign this role to the fewest possible people in your organization.

As a best practice, we recommend that you assign this role to fewer than five people in your organization. If you have more than five admins assigned to the Global Administrator role in your organization, here are some ways to reduce its use.

Available roles

- **Application Administrator** - Users in this role can create and manage all aspects of enterprise applications, application registrations, and application proxy settings.
- **Application Developer** - Users in this role can create application registrations when the "Users can register applications" setting is set to No.
- **Authentication Administrator** - Users with this role can set or reset non-password credentials for some users and can update passwords for all users.
- **Azure DevOps Administrator** - Users with this role can manage the Azure DevOps policy to restrict new Azure DevOps organization creation to a set of configurable users or groups.
- **Azure Information Protection Administrator** - Users with this role have all permissions in the Azure Information Protection service.
- **B2C User Flow Administrator** - Users with this role can create and manage B2C User Flows (also called "built-in" policies) in the Azure portal.

- **B2C User Flow Attribute Administrator** - Users with this role add or delete custom attributes available to all user flows in the tenant.
- **B2C IEF Keyset Administrator** - User can create and manage policy keys and secrets for token encryption, token signatures, and claim encryption/decryption.
- **B2C IEF Policy Administrator** - Users in this role can 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 tenant.
- **Billing Administrator** - Makes purchases, manages subscriptions, manages support tickets, and monitors service health.
- **Cloud Application Administrator** - Users in this role have the same permissions as the Application Administrator role, excluding the ability to manage application proxy.
- **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.
- **Compliance Administrator** - Users with this role have permissions to manage compliance-related features in the Microsoft 365 compliance center, Microsoft 365 admin center, Azure, and Microsoft 365 Security & Compliance Center.
- **Compliance Data Administrator** - Users with this role have permissions to track data in the Microsoft 365 compliance center, Microsoft 365 admin center, and Azure. Users can also track compliance data within the Exchange admin center,
- **Conditional Access Administrator** - Users with this role have the ability to manage Azure Active Directory Conditional Access settings
- **Exchange Administrator** - Users with this role have global permissions within Microsoft Exchange Online, when the service is present.
- **Directory Readers** - Users in this role can read basic directory information.
- **Global Administrator / Company Administrator** - Users with this role have access to all administrative features in Azure Active Directory, as well as services that use Azure Active Directory identities like Microsoft 365 security center, Microsoft 365 compliance center, Exchange Online, SharePoint Online, and Skype for Business Online.
- **Groups Administrator** - Users in this role can create/manage groups and its settings like naming and expiration policies.
- **Security Administrator** - Users with this role have permissions to manage security-related features in the Microsoft 365 security center, Azure Active Directory Identity Protection, Azure Information Protection, and Microsoft 365 Security & Compliance Center.


Managed domain available in your Azure VNet
Automatic background sync to your managed domain
Automatic background sync to your on-premises domain
Virtual network
Workloads and apps in IaaS
Azure AD Domain Services
Azure Active Directory
Azure AD Connect
Active Directory

Azure AD Features

- **Password complexity rules**. This will force users to generate hard(er)-to-guess passwords.
- **Password expiration rules**. You can force users to change their passwords on a periodic basis (and avoid using previous-used passwords).
- **Self-service password reset (SSPR)**. This allows users to self-serve and reset their password if they have forgotten it without involving an IT department.
- **Azure AD Identity Protection**. To help protect your organization's identities, you can configure risk-based policies that automatically respond to risky behaviors. These policies can either automatically block the behaviors or initiate remediation, including requiring password changes.
- **Azure AD password protection**. You can block commonly used and compromised passwords via a globally banned-password list.
- **Azure AD smart lockout**. Smart lockout helps lock out malicious hackers who are trying to guess your users' passwords or use brute-force methods to get in. It recognizes sign-ins coming from valid users and treats them differently than the ones of malicious hackers and other unknown sources.
- **Azure AD Application Proxy**. You can provision security-enhanced remote access to on-premises web applications.
- **Single sign-on (SSO)** access to your applications. This includes thousands of pre-integrated SaaS apps.
- **Azure AD Connect**. Create and manage a single identity for each user across your hybrid enterprise, keeping users, groups, and devices in sync.

How to get Multi-Factor Authentication?

Multi-Factor Authentication comes as part of the following offerings:

- Azure Active Directory Premium or Microsoft 365 Business - Both of these offerings support Azure AD Multi-Factor Authentication using security defaults to require multi-factor authentication.
- Azure AD Free or standalone Microsoft 365 licenses - Use security defaults that require multi-factor authentication for your users and administrators.
- Azure Active Directory Global Administrators - A subset of Azure AD Multi-Factor Authentication capabilities are available as a means to protect global administrator accounts.

Azure AD MFA policies

Azure AD Multi-factor Authentication is enforced with Conditional Access policies. Conditional Access policies are IF-THEN statements. IF a user wants to access a resource, THEN they must complete an action. For example, a payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it. Other common access requests that might require MFA include:

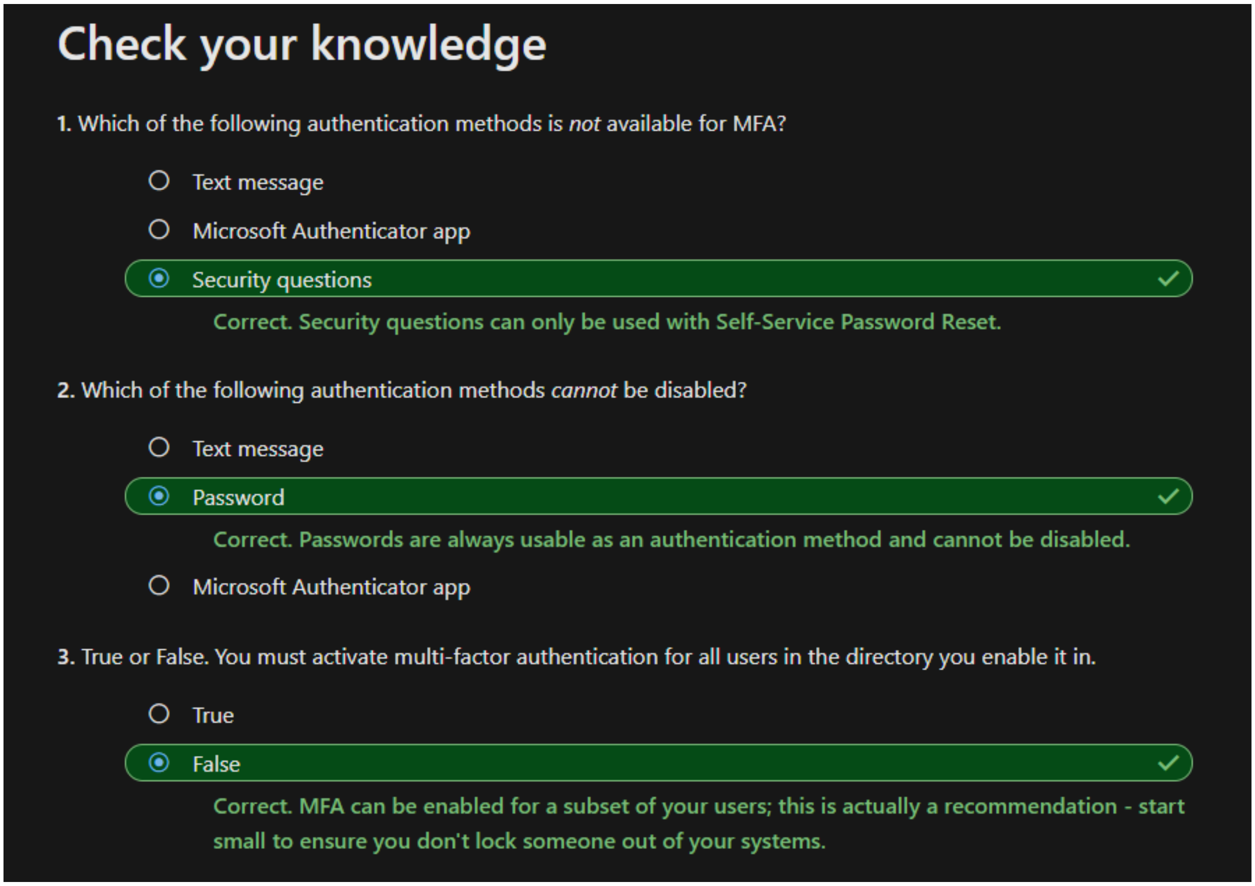
- IF a specific cloud application is accessed
- IF a user is accessing a specific network
- IF a user is accessing a specific client application
- IF a user is registering a new device

DECIDING SUPPORTED AUTHENTICATION METHODS

MethodDescription

- Mobile App Verification code
  - A mobile authentication app such as the Microsoft Authenticator app can be used to retrieve an OATH verification code which is then entered into the sign-in interface. This code is changed every 30 seconds and the app works even if connectivity is limited. Note that this approach doesn't work in China on Android devices.
- Call to a phone
  - Azure can call a supplied phone number. The user then approves the authentication using the keypad. This is a preferred backup method.
- Text message to a phone
  - A text message with a verification code can be sent to a mobile phone. The user then enters the verification code into the sign-in interface to complete the authentication.

Administrators can enable one or more of the options above and then users can opt-in to each support authentication method they want to use.



Check your knowledge

1. Which of the following authentication methods is *not* available for MFA?

○ Text message

○ Microsoft Authenticator app

● Security questions ✓

Correct. Security questions can only be used with Self-Service Password Reset.

2. Which of the following authentication methods *cannot* be disabled?

○ Text message

● Password ✓

Correct. Passwords are always usable as an authentication method and cannot be disabled.

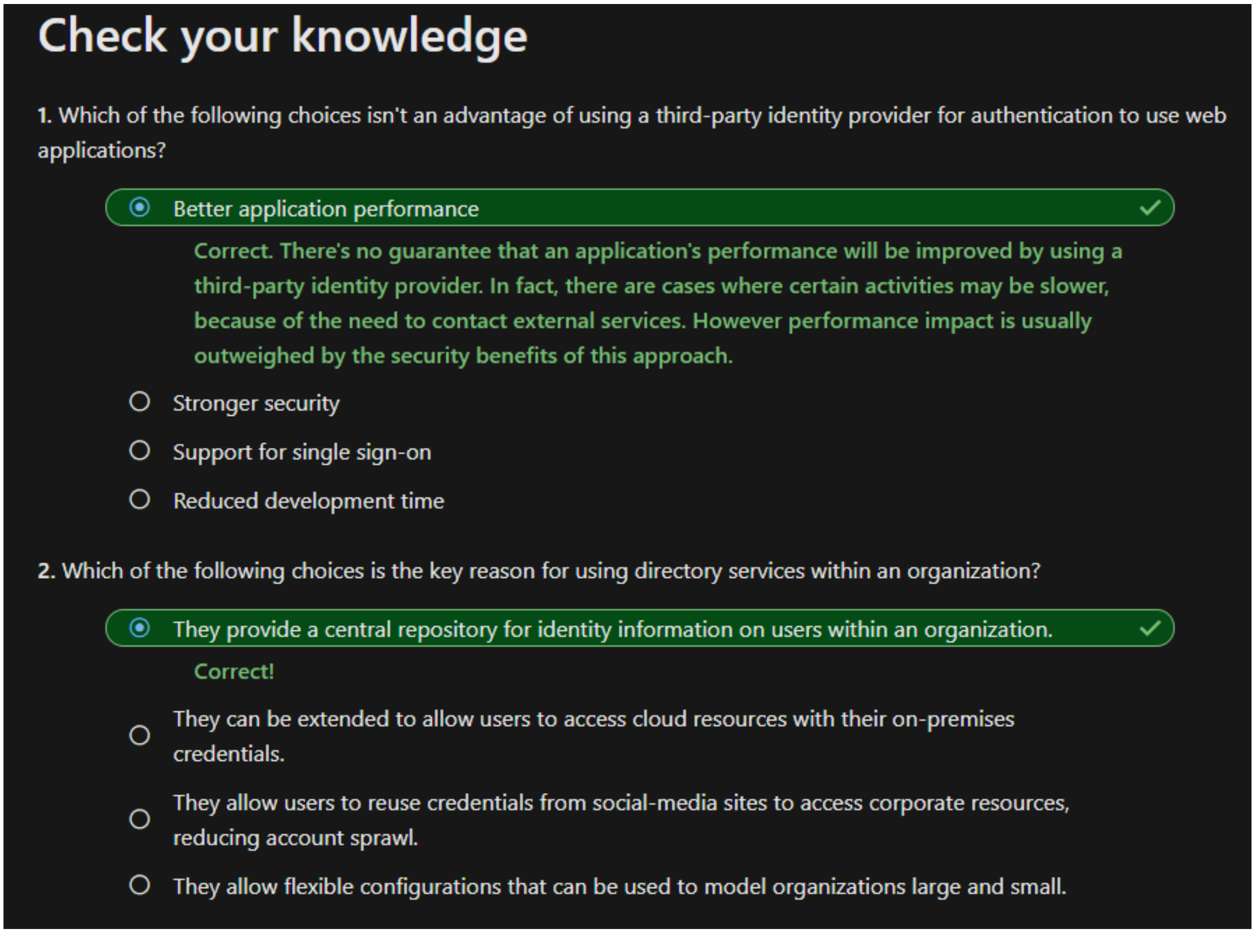
○ Microsoft Authenticator app

3. True or False. You must activate multi-factor authentication for all users in the directory you enable it in.

○ True

● False ✓

Correct. MFA can be enabled for a subset of your users; this is actually a recommendation - start small to ensure you don't lock someone out of your systems.



Check your knowledge

1. Which of the following choices isn't an advantage of using a third-party identity provider for authentication to use web applications?

◉ Better application performance ✓

Correct. There's no guarantee that an application's performance will be improved by using a third-party identity provider. In fact, there are cases where certain activities may be slower, because of the need to contact external services. However performance impact is usually outweighed by the security benefits of this approach.

○ Stronger security

○ Support for single sign-on

○ Reduced development time

2. Which of the following choices is the key reason for using directory services within an organization?

◉ They provide a central repository for identity information on users within an organization. ✓

Correct!

○ They can be extended to allow users to access cloud resources with their on-premises credentials.

○ They allow users to reuse credentials from social-media sites to access corporate resources, reducing account sprawl.

○ They allow flexible configurations that can be used to model organizations large and small.

Federation

Federation predates the cloud. Its purpose is to create a trust relationship between organizations so that Organization A can access Organization B's network resources *without* requiring Organization B to issue credentials to members of Organization A. Federation relies on standards such as WS-Fed, which define protocols used to broker identity information across systems. Federation services such as Microsoft's Active Directory Federation Service (ADFS) implement WS-Fed protocols and bridge identity systems so that Organization A identities can be used as *federated identities* by Organization B. Another way to think about federation is that it allows external users to access internal resources. That is, it extends an organization's identities beyond the organization's boundaries.

Suppose two companies named Contoso and Fabrikam forge a business alliance. Contoso wants Fabrikam employees to have access to certain file shares in Contoso's network and vice versa. The two companies federate their identity systems, allowing Fabrikam employees to access Contoso resources using the same credentials they use to access Fabrikam resources. When IT administrators who work for Contoso add users to the list of users permitted to access the file shares, they see Contoso employees *and* Fabrikam employees -- even though Contoso never created accounts for Fabrikam employees. That's federation in a nutshell.

Federation isn't limited to connecting different organizations' on-premises networks; it can also be used to extend on-premises identities to the cloud. Azure, AWS, and GCP offer identity-management solutions that enable on-premises directory services such as Active Directory to provide identity information to cloud services as well. If a user attempts to access a secured cloud resource, the request is redirected to the on-premises directory solution, which then authenticates the user as if they were accessing an on-premises resource (Figure 3.4). This provides for centralized management of users, credentials, and permissions. It also prevents users from having to use a separate account to access their own organization's cloud resources.

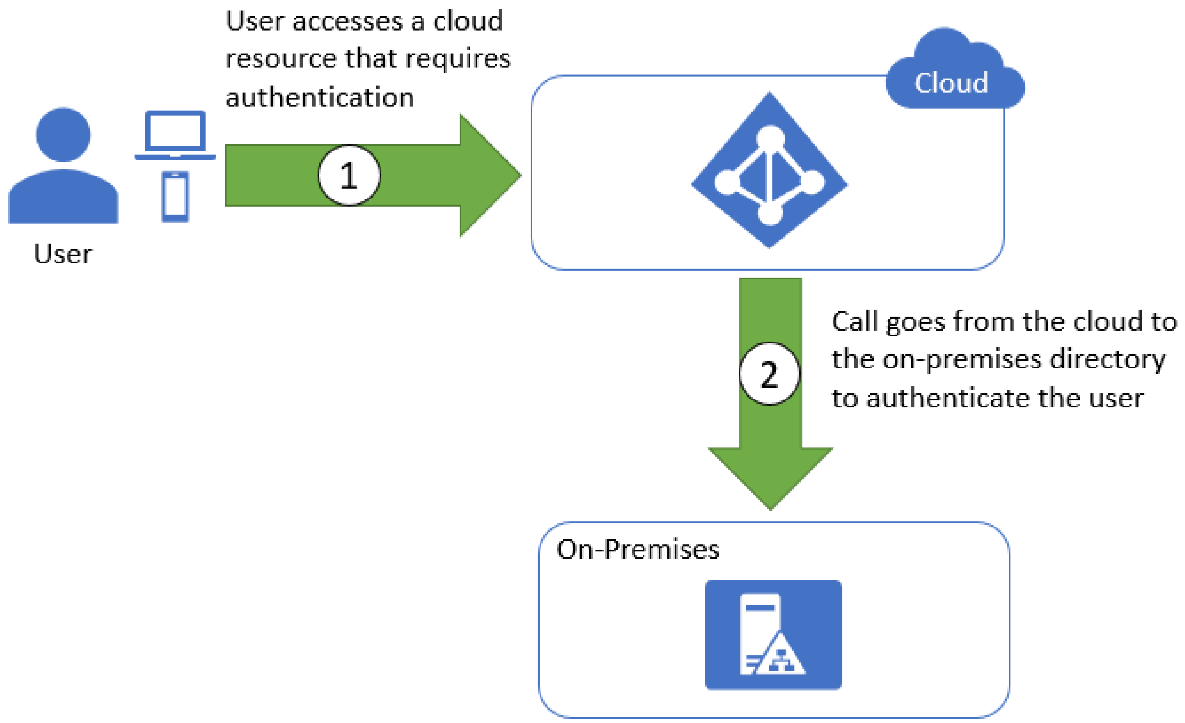

User accesses a cloud resource that requires authentication
1
User
Cloud
2
Call goes from the cloud to the on-premises directory to authenticate the user
On-Premises

Figure 3.4: Federated identity flow.

Federation is widely used by organizations to secure access to cloud resources using the same identity information that secures access to on-premises resources. But it is not perfect. It requires a reliable connection between the on-premises directory service and the cloud so the on-premises directory can be consulted each time a user accesses a cloud resource that requires authentication. One solution to that -- another means for sharing credentials between on-premises directories and the cloud -- is synchronization.

Synchronization

Synchronization is an alternative to federation. With synchronization, on-premises directory information is periodically synchronized with a directory in the cloud. The chief difference between federation and synchronization is that with the former, authentication occurs on-premises, while with synchronization, authentication occurs in the cloud.

Synchronization is implemented by installing a synchronization service within the organization's on-premises systems (Figure 3.5). The service periodically synchronizes the user information between the on-premises directory and the cloud directory. All authentication is then performed against the cloud directory, which contains the same information as the on-premises directory.

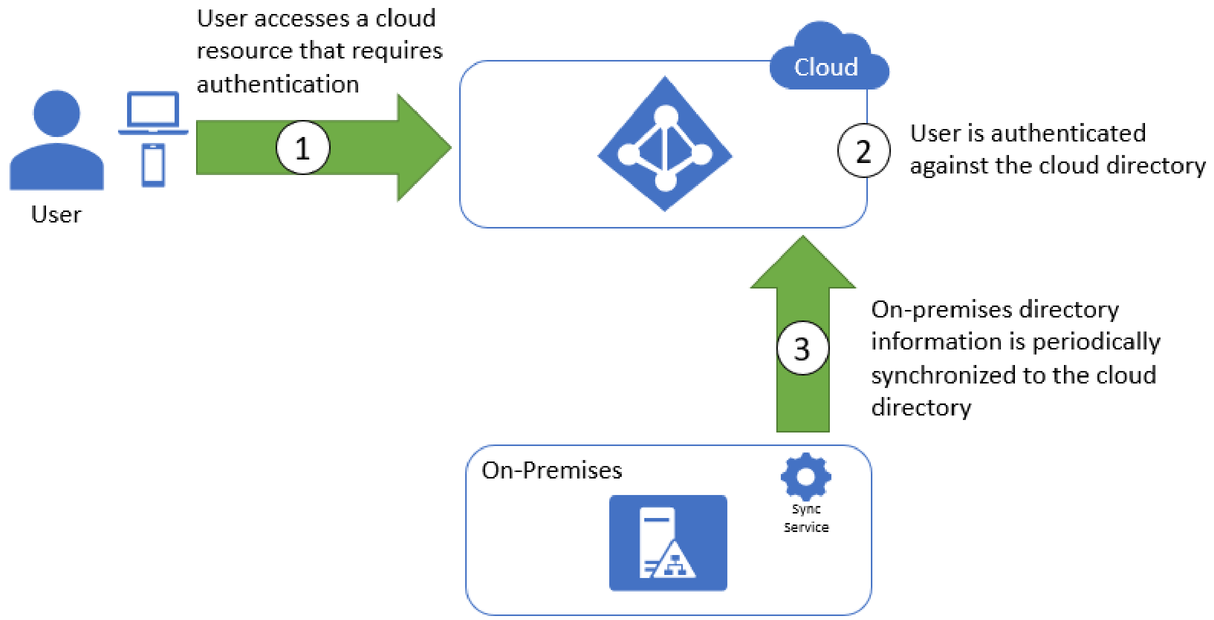

User accesses a cloud resource that requires authentication
Cloud
1
User
2
User is authenticated against the cloud directory
3
On-premises directory information is periodically synchronized to the cloud directory
On-Premises
Sync Service

Figure 3.5: Synchronized identity flow.

A key operational difference between federation and synchronization is that the latter is more resilient to disruptions in connectivity. Synchronization doesn't require access to the on-premises directory every time a user accesses a cloud resource; it only requires access when synchronization occurs. The primary downside to synchronization is that changes made to the on-premises directory take time to propagate to the cloud. If an administrator adds Alice to the on-premises directory but synchronization occurs just once an hour, Alice won't be able to access secured cloud resources for up to one hour after the change is made.

Tools such as Azure Active Directory Connect (AADC) are available for synchronizing directories. AADC synchronizes information stored on-premises in Active Directory with information stored in the cloud in Azure Active Directory. Amazon provides a similar offering in the form of AD Connector, as does Google with Google Cloud Directory Sync (GCDS).

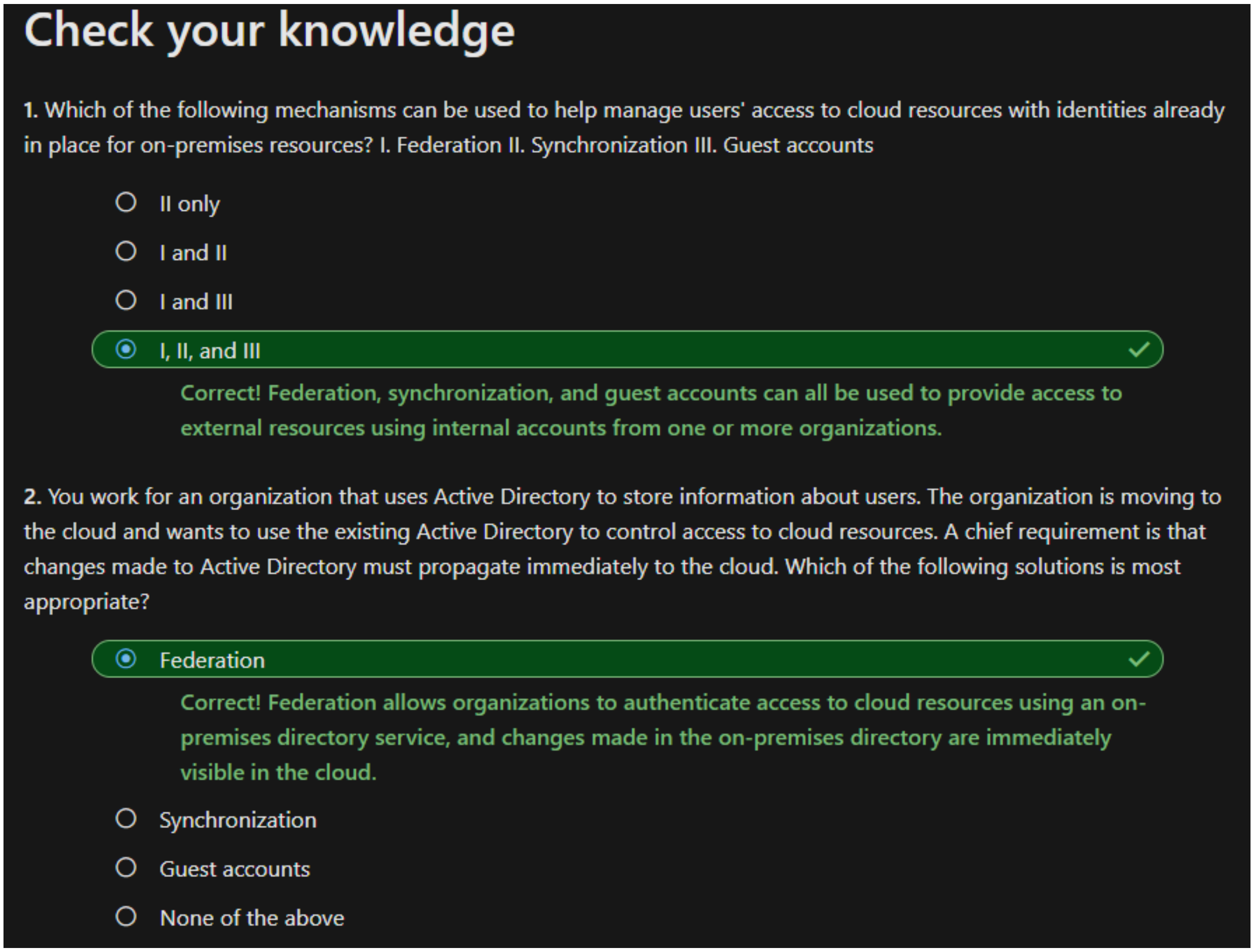
Synchronization solutions are generally preferred to federation-based approaches. They typically incur less management overhead and do not require an always-available connection between directory services. This recommendation is echoed by the UK's National Cyber Security Centre[1].

Guest accounts

Another challenge for IT is how to handle users who are external to the organization. These users often include contractors, consultants, and interns -- users who aren't a formal part of the organization but need access to internal resources as if they were.

One solution is to create internal accounts for external users. Such accounts often use a prefix or suffix in the account names to denote their external nature. At Microsoft, for example, most external accounts have names such as v-jeffpro, where "v" stands for "vendor." This approach, however, is far from perfect. For one, it exacerbates account sprawl. ("Here's another user name to keep track of and another password that has to be changed every 60 days and conform to a policy that's unique to this organization.") It also increases the workload on administrators by increasing the number of accounts for which they are responsible and forcing them to establish a mechanism or process for propagating changes in the status of external users within their own organizations to internal identity-management systems. For example, if a consultant with "extern" credentials retires or takes a job somewhere else, their credentials need to be revoked so they can no longer be used to access your systems.

A better solution is to use *guest accounts*. Guest accounts are a special case of federated accounts. External users are "invited" to join an organization's identity-management system using the credentials from their own organization. A new user record is created, but when the guest user authenticates, they do so against their home organization. This eliminates the need for the user to manage an additional set of credentials. It also eliminates the need for IT to be aware when the user's status changes in their home organization. Once they are removed from the system by their home IT staff, they can no longer authenticate to either system.



Check your knowledge

1. Which of the following mechanisms can be used to help manage users' access to cloud resources with identities already in place for on-premises resources? I. Federation II. Synchronization III. Guest accounts

○ II only

○ I and II

○ I and III

● I, II, and III ✓

Correct! Federation, synchronization, and guest accounts can all be used to provide access to external resources using internal accounts from one or more organizations.

2. You work for an organization that uses Active Directory to store information about users. The organization is moving to the cloud and wants to use the existing Active Directory to control access to cloud resources. A chief requirement is that changes made to Active Directory must propagate immediately to the cloud. Which of the following solutions is most appropriate?

● Federation ✓

Correct! Federation allows organizations to authenticate access to cloud resources using an on-premises directory service, and changes made in the on-premises directory are immediately visible in the cloud.

○ Synchronization

○ Guest accounts

○ None of the above

Role-based access control

A key aspect of administering cloud services for an organization is controlling access to the cloud resources. That means making sure users who require access to a service or one of its components have that access, while others do not. This process is known as *identity and access management (IAM)*. In Azure, AWS, and GCP, IAM is achieved using a technique known as *role-based access control* (RBAC).

With RBAC, users or groups of users are assigned one or more *roles*. Each role has a descriptive name, and uses permissions to define the actions role assignees can perform on the resources involved. For example, a user assigned the "Reader" role, defined for a resource group might be able to view the resources in that resource group, but not modify or delete them.

A user's ability to access resources is controlled by:

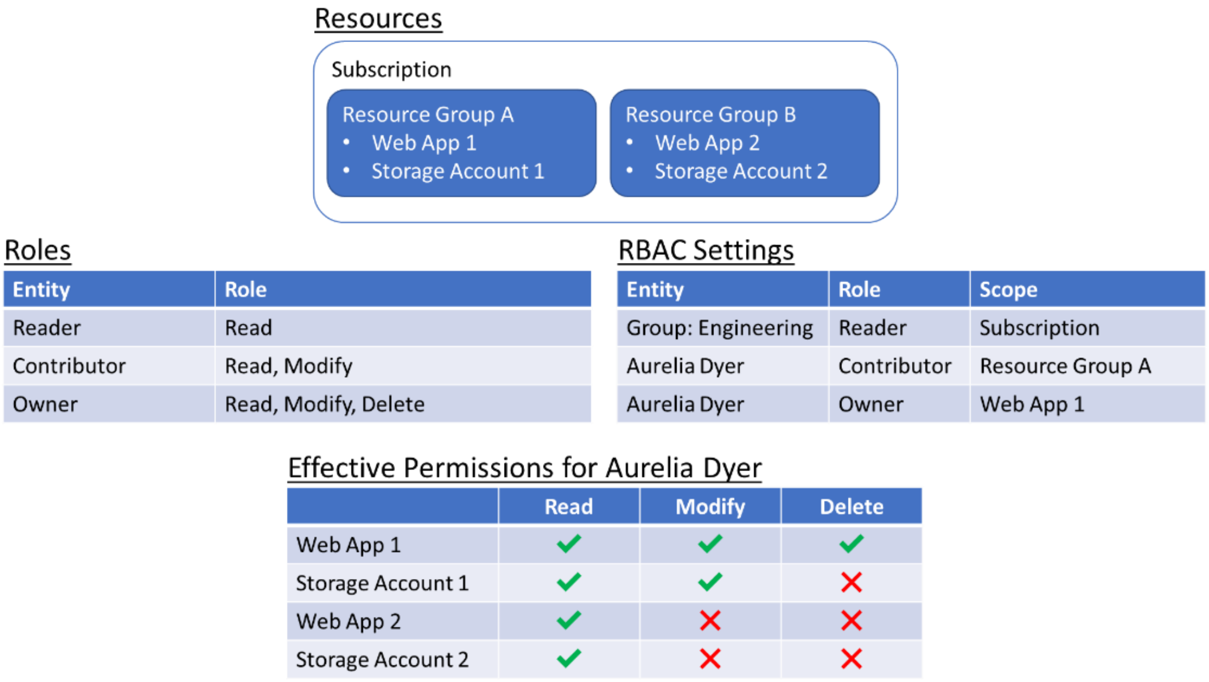
- the roles assigned to them,
- the roles assigned to any groups the user belongs to, and
- the roles' resource scopes.

A *resource scope* is a level in the cloud resource hierarchy. In Azure, for example, roles can apply to individual resources, resource groups, entire subscriptions (in which case the role's permissions apply to all resources created under a given subscription), or groups of subscriptions. By applying different roles to different scopes in the resource hierarchy, you get fine-grained control over who has permissions to do what within an organization.

In the example in Figure 3.6, a set of resources is provisioned within a cloud subscription and organized into two resource groups. A user group named Engineering is assigned a role named "Reader" that permits group members to view all resources created under the subscription. At the same time, a user named Aurelia Dyer is assigned a "Contributor" role that permits her to modify any of the resources in resource group A, and an "Owner" role that lets her delete the Web App resource in the same resource group. Let's assume that Aurelia is a member of the Engineering group. These permissions mean she can:

- View all resources created under the subscription
- Modify the two resources in resource group A -- for example, change configuration settings in Web App 1 or alter the replication settings for Storage Account 1
- Delete the Web App 1 resource in resource group A

While Aurelia can see the resources in resource group B, she can't modify or delete them.



Roles

Entity	Role
Reader	Read
Contributor	Read, Modify
Owner	Read, Modify, Delete

RBAC Settings

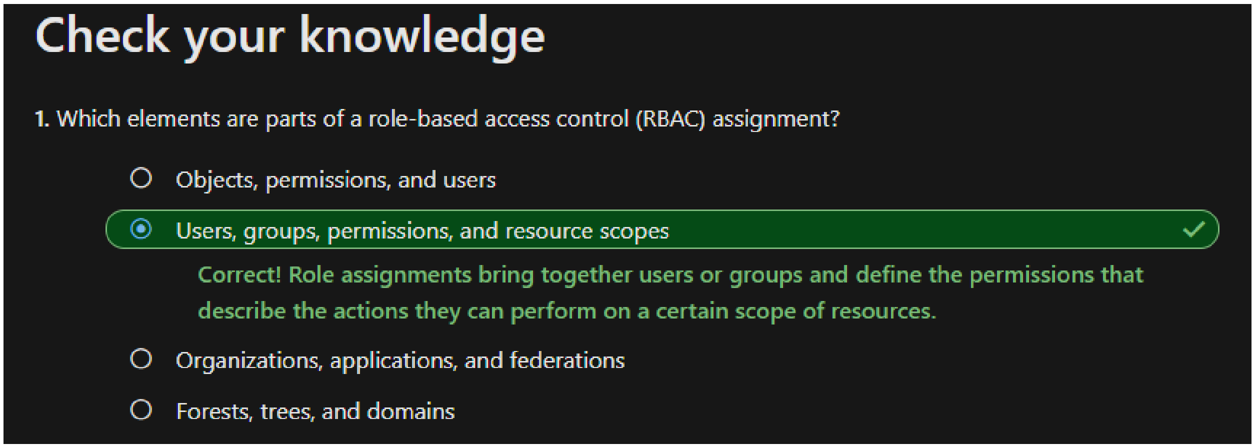
Entity	Role	Scope
Group: Engineering	Reader	Subscription
Aurelia Dyer	Contributor	Resource Group A
Aurelia Dyer	Owner	Web App 1

Effective Permissions for Aurelia Dyer

	Read	Modify	Delete
Web App 1	✓	✓	✓
Storage Account 1	✓	✓	✗
Web App 2	✓	✗	✗
Storage Account 2	✓	✗	✗

Figure 3.6: RBAC and effective permissions.

Given that a user can be assigned multiple roles, there may be some concern about how conflicting permissions are handled. Currently, major cloud service providers support "allow" permissions in their RBAC implementations, but provide little or no support for "deny" permissions. (Only Azure supports "deny" permissions, and only in limited contexts. If a "deny" permission conflicts with an "allow" permission, "deny" takes precedence.) Because "allow" permissions are additive, they can't conflict with each other: a user's permissions are simply the sum of the various "allow" permissions at each applicable scope.



Check your knowledge

1. Which elements are parts of a role-based access control (RBAC) assignment?

○ Objects, permissions, and users

● Users, groups, permissions, and resource scopes ✓

Correct! Role assignments bring together users or groups and define the permissions that describe the actions they can perform on a certain scope of resources.

○ Organizations, applications, and federations

○ Forests, trees, and domains

Summary

Here is a brief summary of the important concepts learned in this module:

- Securing access to resources, whether on-premises or in the cloud, requires us to identify the users accessing those resources.
- For authenticating web-site users, relying on a trusted third-party identity provider offers a number of advantages over implementing authentication yourself. Among those advantages are tighter security, support for single sign-on (SSO), and reduced development time.
- With third-party identity providers, user credentials are stored by the provider and are never seen by the application.
- Cloud service providers offer identity-provider services, as do popular social-media companies such as Facebook and Twitter.
- Identity information regarding users within an organization (for example, a company) are usually stored in directory services such as Active Directory.
- Directory services store identities for users, groups, and applications.
- Federation allows users accessing cloud resources to be authenticated using on-premises directory systems.
- Synchronization allows users accessing cloud resources to be authenticated using cloud-based directory systems whose contents are synced with on-premises directory systems.
- Guest accounts allow users accessing an organization's resources to be authenticated using identities established outside the organization.
- Federation, synchronization, and guest accounts reduce account sprawl and simplify identity management and access control.
- Role-based access control (RBAC) is used to implement identity and access management (IAM) in cloud solutions.
- Roles specify actions that can be performed on resources and are assigned to users and groups.
- Roles can be applied to individual resources, groups of resources, subscriptions, and in some cases, groups of subscriptions. The level at which a role is applied is termed the resource scope.

Azure Active Directory Domain Services (Azure AD DS)

-provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication that is fully compatible with Windows Server Active Directory. You use these domain services without the need to deploy, manage, and patch domain controllers in the cloud. Azure AD DS integrates with your existing Azure AD tenant, which makes it possible for users to sign in using their existing credentials. You can also use existing groups and user accounts to secure access to resources, which provides a smoother lift-and-shift of on-premises resources to Azure.

Azure AD DS replicates identity information from Azure AD, so it works with Azure AD tenants that are cloud-only, or synchronized with an on-premises Active Directory Domain Services (AD DS) environment. The same set of Azure AD DS features exist for both environments.

- If you have an existing on-premises AD DS environment, you can synchronize user account information to provide a consistent identity for users.
- For cloud-only environments, you don't need a traditional on-premises AD DS environment to use the centralized identity services of Azure AD DS.

! Azure AD DS integrates with Azure AD, which itself can synchronize with an on-premises AD DS environment. This ability extends central identity use cases to traditional web applications that run in Azure as part of a lift-and-shift strategy.

- **Cloud identities** - These users exist only in Azure AD. Examples are administrator accounts and users that you manage yourself. Their source is Azure AD.
- **Directory-synchronized identities** - These users exist in on-premises Active Directory. A synchronization activity that occurs via **Azure AD Connect** brings these users in to Azure.
- **Guest users** - These users exist outside Azure. Examples are accounts from other cloud providers and Microsoft accounts.

Azure AD groups

Azure AD allows you to define two different types of groups.

- **Security groups**. These are the most common and are used to manage member and computer access to shared resources for a group of users. For example, you can create a security group for a specific security policy. By doing it this way, you can give a set of permissions to all the members at once, instead of having to add permissions to each member individually. This option requires an Azure AD administrator.
- **Microsoft 365 groups**. These groups provide collaboration opportunities by giving members access to a shared mailbox, calendar, files, SharePoint site, and more. This option also lets you give people outside of your organization access to the group. This option is available to users as well as admins.

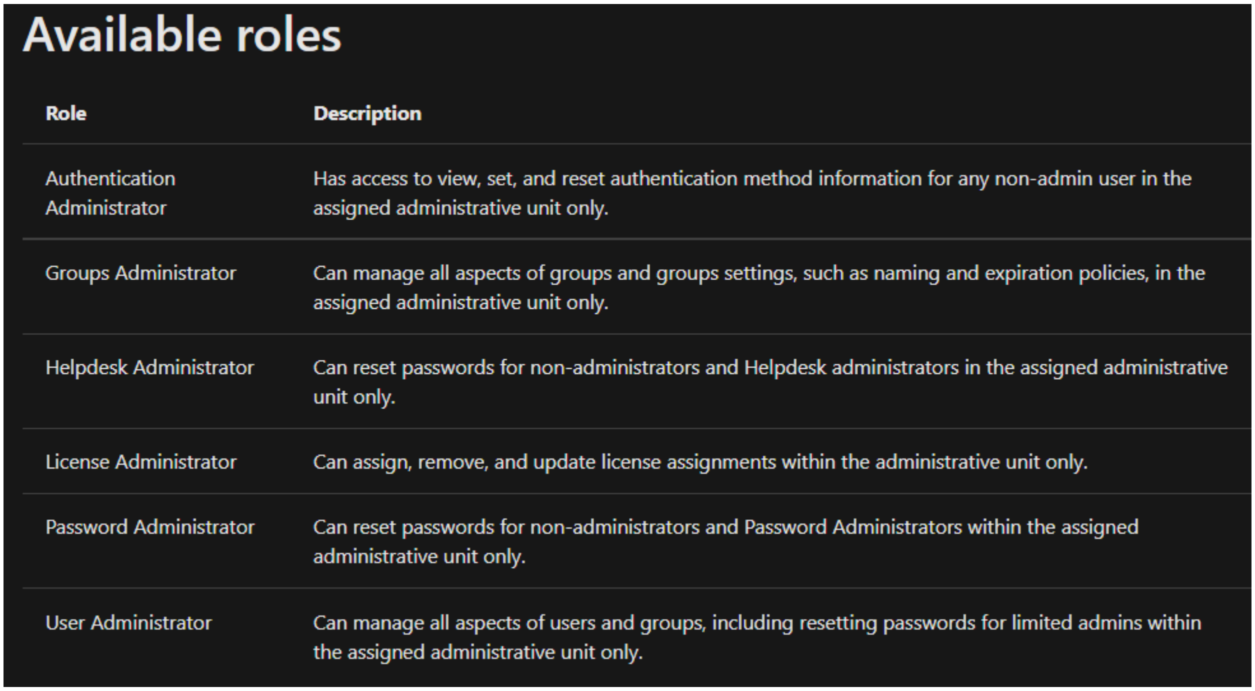
There are different ways you can assign group access rights:

- Assigned. Let’s you add specific users to be members of this group and to have unique permissions.
- Dynamic User. Let’s you use dynamic membership rules to automatically add and remove members. If a member's attributes change, the system reviews your dynamic group rules for the directory to determine if the member meets the rule requirements (is added) or no longer meets the rules requirements (is removed).
- Dynamic Device (Security groups only). Let’s you use dynamic group rules to automatically add and remove devices. If a device's attributes change, the system reviews your dynamic group

rules for the directory to determine if the device meets the rule requirements (is added) or no longer meets the rules requirements (is removed).

Administrative Units

To use administrative units, you need an Azure Active Directory Premium license for each administrative unit admin, and Azure Active Directory Free licenses for administrative unit members.

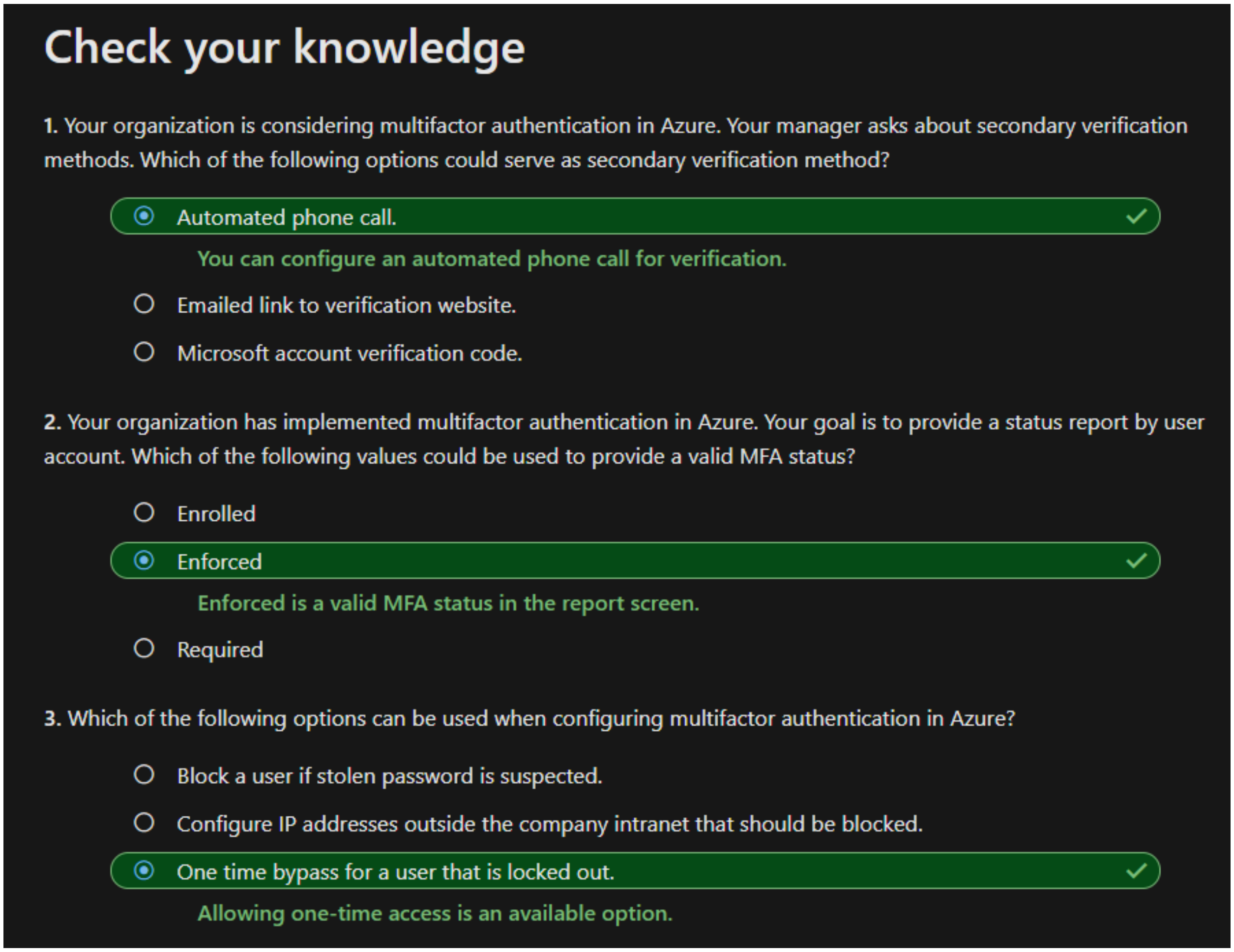


Available roles

Role	Description
Authentication Administrator	Has access to view, set, and reset authentication method information for any non-admin user in the assigned administrative unit only.
Groups Administrator	Can manage all aspects of groups and groups settings, such as naming and expiration policies, in the assigned administrative unit only.
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk administrators in the assigned administrative unit only.
License Administrator	Can assign, remove, and update license assignments within the administrative unit only.
Password Administrator	Can reset passwords for non-administrators and Password Administrators within the assigned administrative unit only.
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins within the assigned administrative unit only.

Passwordless authentication methods

- **Windows Hello for Business** - biometric and PIN credentials are directly tied to the user's PC, which prevents access from anyone other than the owner.
- **FIDO2 Security Keys** - generally stored on a USB stick, FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor.
- **Microsoft Authenticator App** - Authenticator App turns any iOS or Android phone into a strong, passwordless credential. Users can sign in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.
- **FIDO2 Smartcards (preview)** - new method to use FIDO2 keys for passwordless login via a smartcard.
- **Temporary Access Pass (preview)** - time-limited passcode allows you to set up security keys and the Microsoft Authenticator without ever needing to use, much less know, your password!



Check your knowledge

1. Your organization is considering multifactor authentication in Azure. Your manager asks about secondary verification methods. Which of the following options could serve as secondary verification method?

- ● Automated phone call. ✓

  You can configure an automated phone call for verification.
- ○ Emailed link to verification website.
- ○ Microsoft account verification code.

2. Your organization has implemented multifactor authentication in Azure. Your goal is to provide a status report by user account. Which of the following values could be used to provide a valid MFA status?

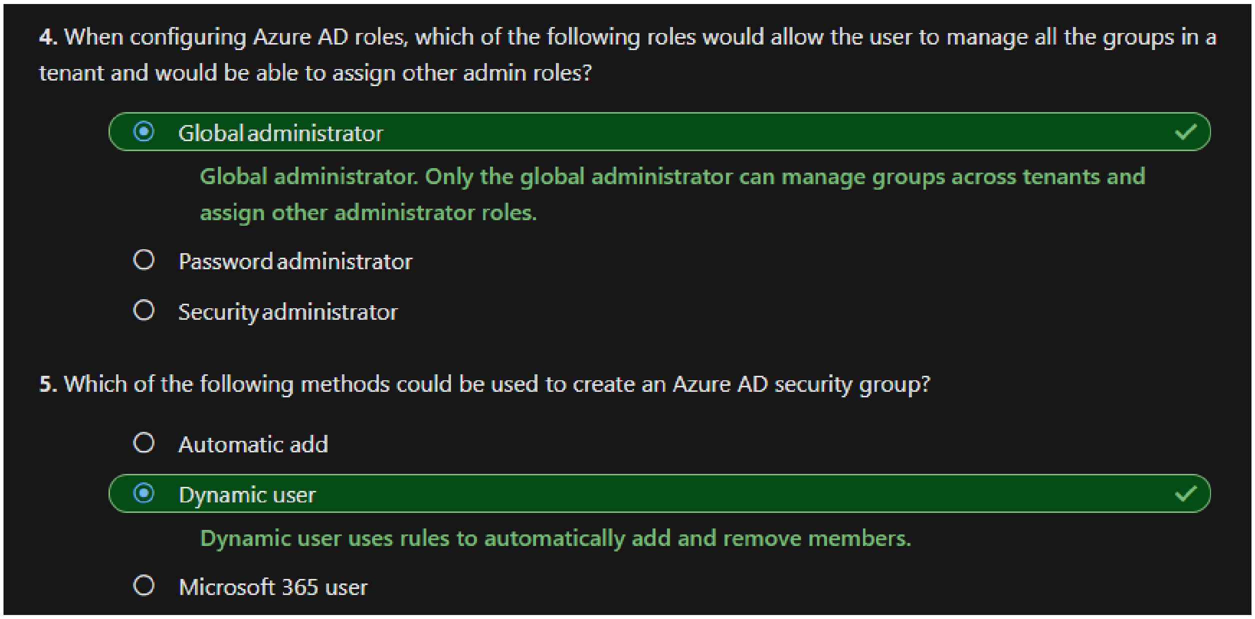
- ○ Enrolled
- ● Enforced ✓

  Enforced is a valid MFA status in the report screen.
- ○ Required

3. Which of the following options can be used when configuring multifactor authentication in Azure?

- ○ Block a user if stolen password is suspected.
- ○ Configure IP addresses outside the company intranet that should be blocked.
- ● One time bypass for a user that is locked out. ✓

  Allowing one-time access is an available option.



4. When configuring Azure AD roles, which of the following roles would allow the user to manage all the groups in a tenant and would be able to assign other admin roles?

- ● Global administrator ✓

  Global administrator. Only the global administrator can manage groups across tenants and assign other administrator roles.
- ○ Password administrator
- ○ Security administrator

5. Which of the following methods could be used to create an Azure AD security group?

- ○ Automatic add
- ● Dynamic user ✓

  Dynamic user uses rules to automatically add and remove members.
- ○ Microsoft 365 user

Azure AD Connect

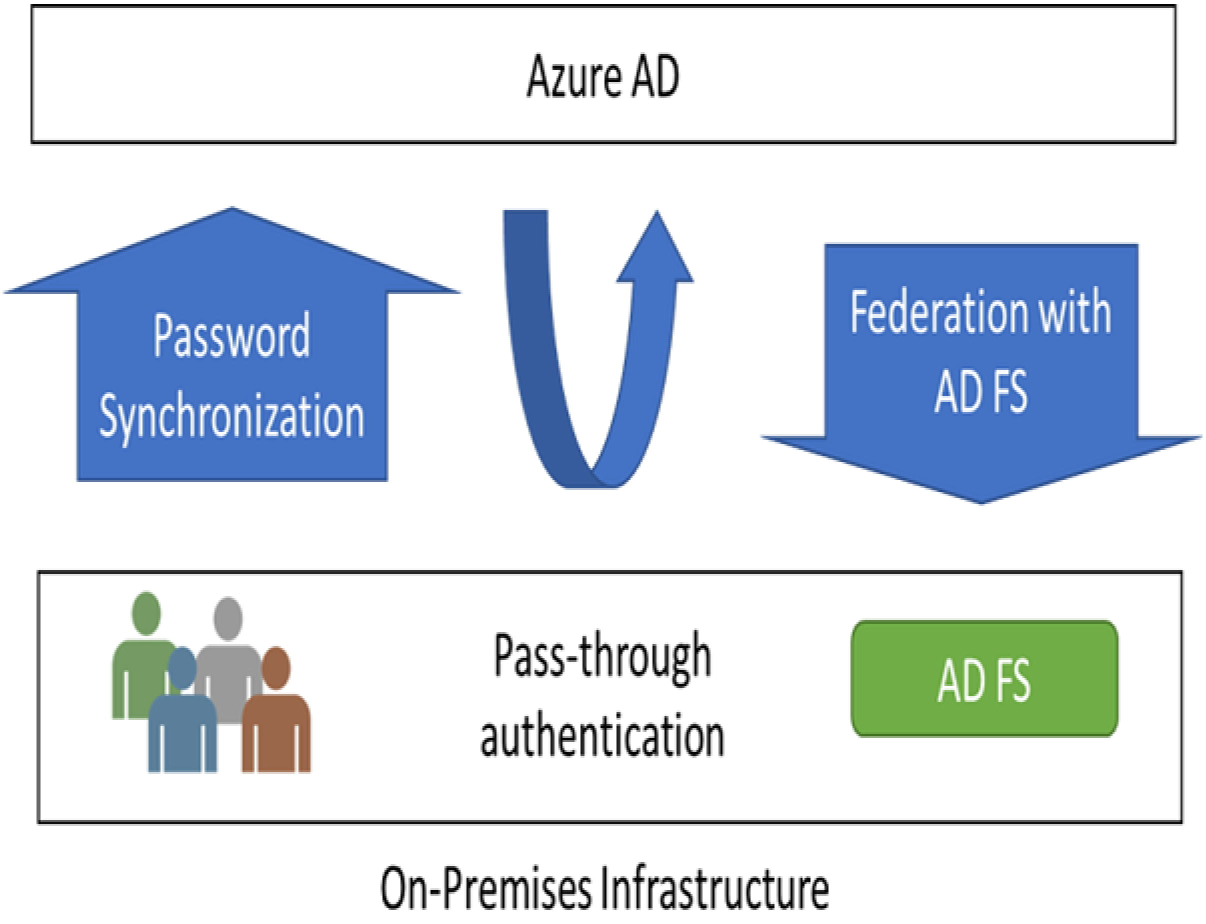
Azure AD Connect provides the following features:

- **Password hash synchronization**. A sign-in method that synchronizes a hash of users on-premises AD password with Azure AD.
- **Pass-through authentication**. A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.
- **Federation integration**. Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- **Synchronization**. Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
- **Health Monitoring**. Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Explore authentication options

Choosing an Azure AD Authentication method is important as it is one of the first important decisions when moving to the cloud as it will be the foundation of your cloud environment and is difficult to change at a later date.

You can choose **cloud authentication** which includes: Azure AD password hash synchronization and Azure AD Pass-through Authentication. You can also choose **federated authentication** where Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user’s password.



Summary

- Do you need on-premises Active Directory integration? If the answer is No, then you would use Cloud-Only authentication.
- If you do need on-premises Active Directory integration, then do you need to use cloud authentication, password protection, and your authentication requirements are natively supported by Azure AD? If the answer is Yes, Then you would use **Password Hash Sync + Seamless SSO**.
- If you do need on-premises Active Directory integration, but you do not need to use cloud authentication, password protection, and your authentication requirements are natively supported by Azure AD, then you would use **Pass-through Authentication Seamless SSO**.
- If you need on-premises Active Directory integration, have an existing federation provider and your authentication requirements are NOT natively supported by Azure AD, then you would use **Federation** authentication.

Password Hash Synchronization (PHS)

How does this work?

In the background, the password synchronization component takes the user's password hash from on-premises Active Directory, encrypts it, and passes it as a string to Azure. Azure decrypts the encrypted hash and stores the password hash as a user attribute in Azure AD.

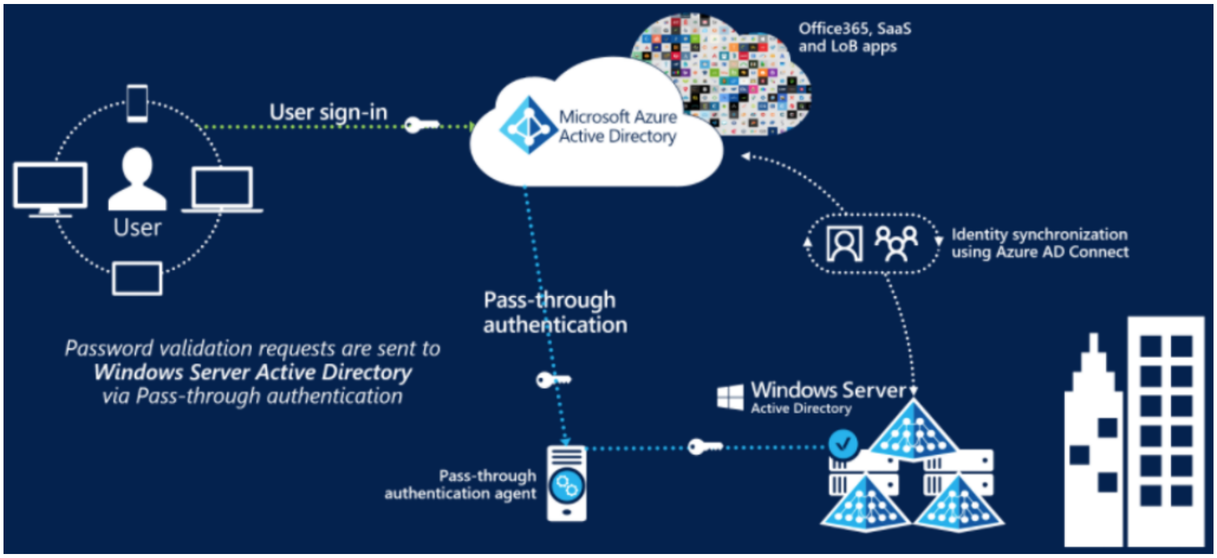
When the user signs in to an Azure service, the sign-in challenge dialog box generates a hash of the user's password and passes that hash back to Azure. Azure then compares the hash with the one in that user's account. If the two hashes match, then the two passwords must also match and the user receives access to the resource. The dialog box provides the facility to save the credentials so that the next time the user accesses the Azure resource, the user will not be prompted.

Important

It is important to understand that this is **same sign-in**, not single sign-on. The user still authenticates against two separate directory services, albeit with the same user name and password. This solution provides a simple alternative to an AD FS implementation.

Pass-through Authentication (PTA)

Azure AD Pass-through Authentication (PTA) is an alternative to Azure AD Password Hash Synchronization, and provides the same benefit of cloud authentication to organizations. PTA allows users to sign in to both on-premises and cloud-based applications using the same user account and passwords. When users sign-in using Azure AD, Pass-through authentication validates the users' passwords directly against an organizations on-premise Active Directory.


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

Feature benefits

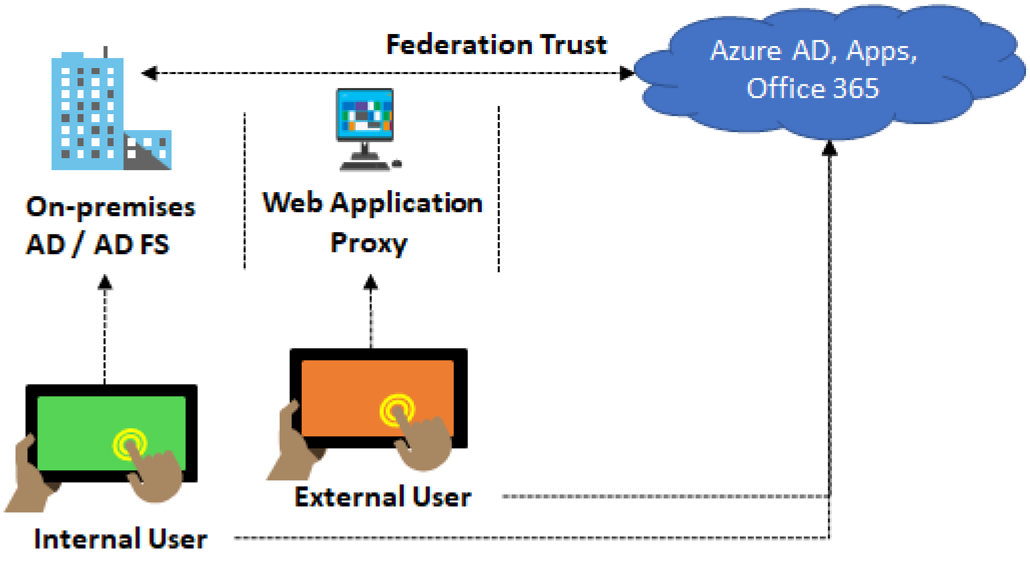
- Supports user sign-in into all web browser-based applications and into Microsoft Office client applications that use modern authentication.

- Sign-in usernames can be either the on-premises default username (userPrincipalName) or another attribute configured in Azure AD Connect (known as Alternate ID).
- Works seamlessly with conditional access features such as Azure Active Directory Multi-Factor Authentication to help secure your users.
- Integrated with cloud-based self-service password management, including password writeback 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.
- PTA is a free feature, and you don't need any paid editions of Azure AD to use it.
- PTA can be enabled via Azure AD Connect.
- PTA 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.
- PTA protects your on-premises accounts against brute force password attacks in the cloud.

Important

This feature can be configured without using a federation service so that any organization, regardless of size, can implement a hybrid identity solution. Pass-through authentication is not only for user sign-in but allows an organization to use other Azure AD features, such as password management, role-based access control, published applications, and conditional access policies.

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.

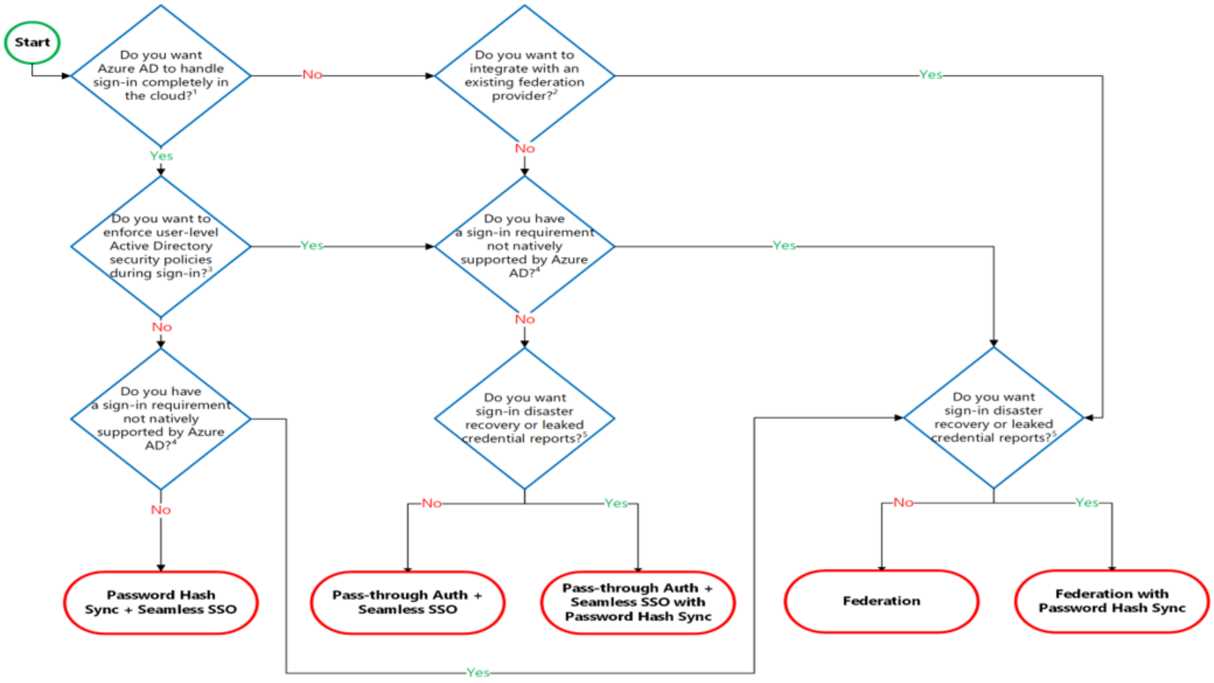


You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control.

Important

If you decide to use Federation with Active Directory Federation Services (AD FS), you can optionally set up password hash synchronization as a backup in case your AD FS infrastructure fails.

Decision tree


Start
Do you want Azure AD to handle sign-in completely in the cloud?1
No
Do you want to integrate with an existing federation provider?2
Yes
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?3
Yes
Do you have a sign-in requirement not natively supported by Azure AD?4
Yes
No
No
Do you have a sign-in requirement not natively supported by Azure AD?4
Do you want sign-in disaster recovery or leaked credential reports?5
Do you want sign-in disaster recovery or leaked credential reports?5
No
No
Yes
No
Yes
Password Hash Sync + Seamless SSO
Pass-through Auth + Seamless SSO
Pass-through Auth + Seamless SSO with Password Hash Sync
Federation
Federation with Password Hash Sync
Yes

Details on decision questions:

- Azure AD can handle sign-in for users without relying on on-premises components to verify passwords.
- Azure AD can hand off user sign-in to a trusted authentication provider such as Microsoft's AD FS.
- If you need to apply, user-level Active Directory security policies such as account expired, disabled account, password expired, account locked out, and sign-in hours on each user sign-in, Azure AD requires some on-premises components.
- Sign-in features not natively supported by Azure AD:
  - Sign-in using smartcards or certificates.
  - Sign-in using on-premises MFA Server.
  - Sign-in using third-party authentication solution.
  - Multi-site on-premises authentication solution.
- Azure AD Identity Protection requires Password Hash Sync regardless of which sign-in method you choose, to provide the Users with leaked credentials report. Organizations can fail over to Password Hash Sync if their primary sign-in method fails and it was configured before the failure event.

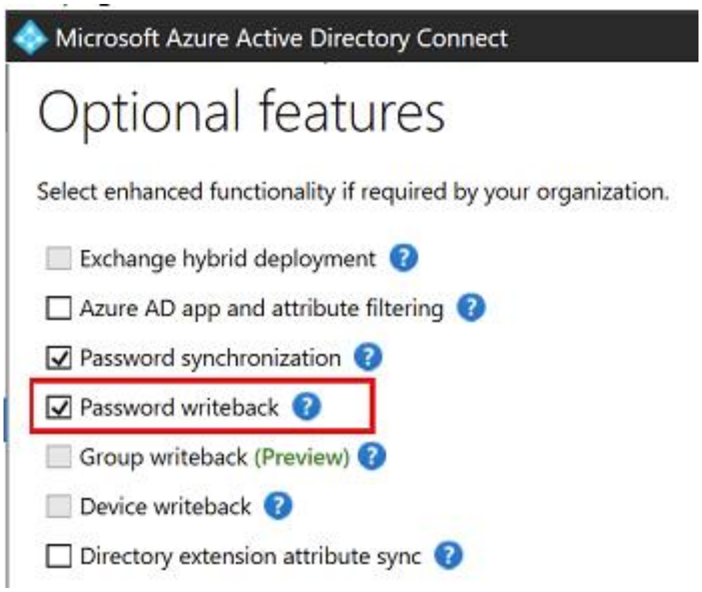
Important

This decision tree is intended as a starting point to understand your options, but there can be others or even combinations of different options. For example, you can use Azure AD B2C and configure it to allow user sign-in for multi-tenant Azure AD tenants - with or without the traditional support for self-service sign up and social identity providers.

Configure password writeback

Having a cloud-based password reset utility is great but most companies still have an on-premises directory where their users exist. How does Microsoft support keeping traditional on-premises Active Directory Domain Services (AD DS) in sync with password changes in the cloud?

Password writeback is a feature enabled with Azure AD Connect that allows password changes in the cloud to be written back to an existing on-premises directory in real time.



Microsoft Azure Active Directory Connect

Optional features

Select enhanced functionality if required by your organization.

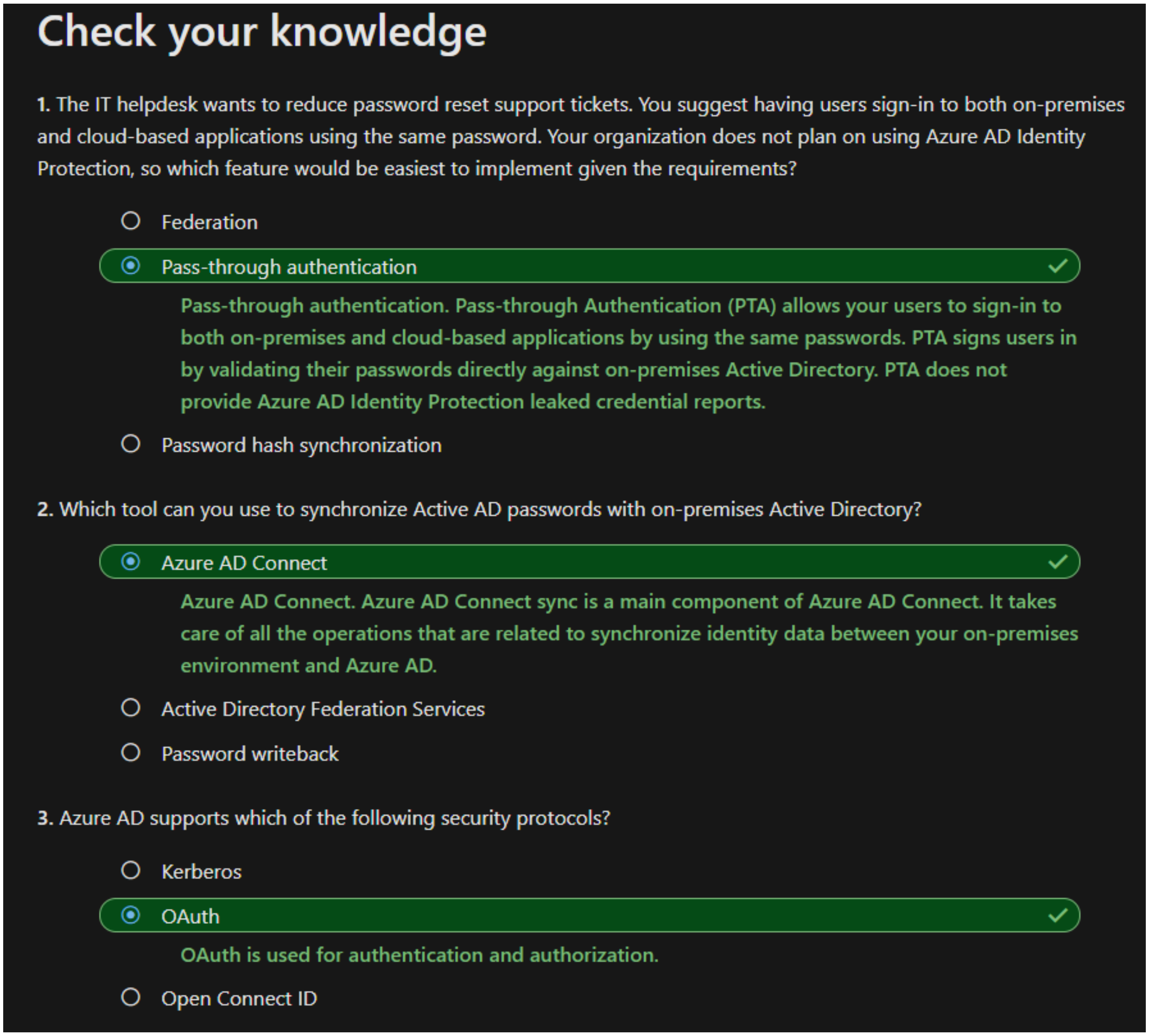
- ☐ Exchange hybrid deployment
- ☐ Azure AD app and attribute filtering
- ☑ Password synchronization
- ☑ Password writeback
- ☐ Group writeback (Preview)
- ☐ Device writeback
- ☐ Directory extension attribute sync

Password writeback provides:

- **Enforcement of on-premises Active Directory Domain Services password policies**. When a user resets their password, it is checked to ensure it meets your on-premises Active Directory Domain Services policy before committing it to that directory. This review includes checking the history, complexity, age, password filters, and any other password restrictions that you have defined in local Active Directory Domain Services.
- **Zero-delay feedback**. Password writeback is a synchronous operation. Your users are notified immediately if their password did not meet the policy or could not be reset or changed for any reason.
- **Supports password changes from the access panel and Microsoft 365**. When federated or password hash synchronized users come to change their expired or non-expired passwords, those passwords are written back to your local Active Directory Domain Services environment.
- **Supports password writeback when an admin resets them from the Azure portal**. Whenever an admin resets a user’s password in the Azure portal, if that user is federated or password hash synchronized, the password is written back to on-premises. This functionality is currently not supported in the Microsoft admin portal.
- **Doesn’t require any inbound firewall rules**. Password writeback uses an Azure Service Bus relay as an underlying communication channel. All communication is outbound over port 443.

Important

To use SSPR you must have already configured Azure AD Connect in your environment.



Check your knowledge

1. The IT helpdesk wants to reduce password reset support tickets. You suggest having users sign-in to both on-premises and cloud-based applications using the same password. Your organization does not plan on using Azure AD Identity Protection, so which feature would be easiest to implement given the requirements?

○ Federation

● Pass-through authentication ✓

Pass-through authentication. Pass-through Authentication (PTA) allows your users to sign-in to both on-premises and cloud-based applications by using the same passwords. PTA signs users in by validating their passwords directly against on-premises Active Directory. PTA does not provide Azure AD Identity Protection leaked credential reports.

○ Password hash synchronization

2. Which tool can you use to synchronize Active AD passwords with on-premises Active Directory?

● Azure AD Connect ✓

Azure AD Connect. Azure AD Connect sync is a main component of Azure AD Connect. It takes care of all the operations that are related to synchronize identity data between your on-premises environment and Azure AD.

○ Active Directory Federation Services

○ Password writeback

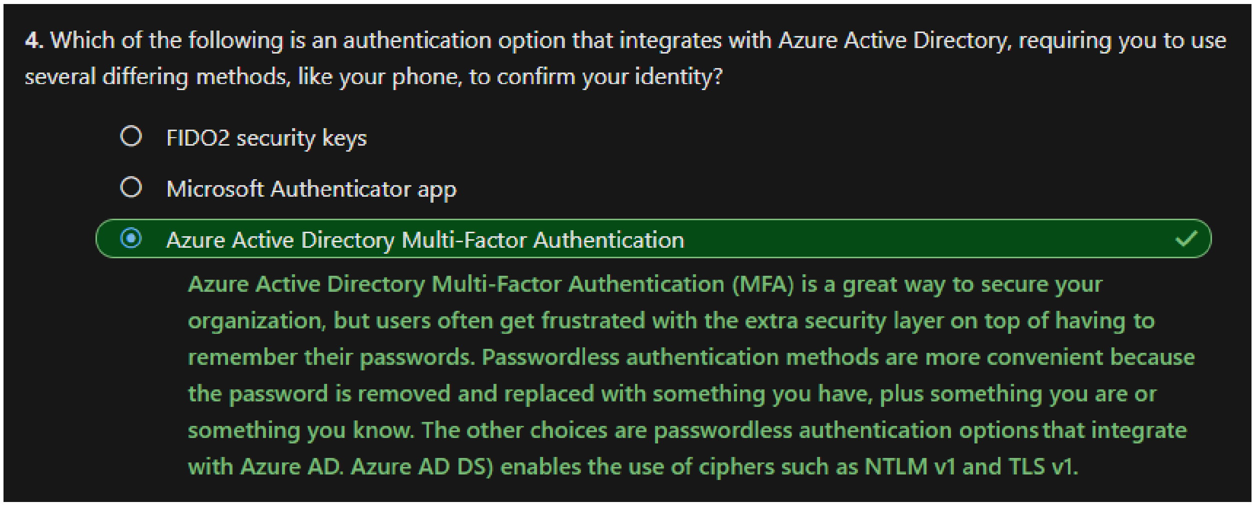
3. Azure AD supports which of the following security protocols?

○ Kerberos

● OAuth ✓

OAuth is used for authentication and authorization.

○ Open Connect ID



4. Which of the following is an authentication option that integrates with Azure Active Directory, requiring you to use several differing methods, like your phone, to confirm your identity?

○ FIDO2 security keys

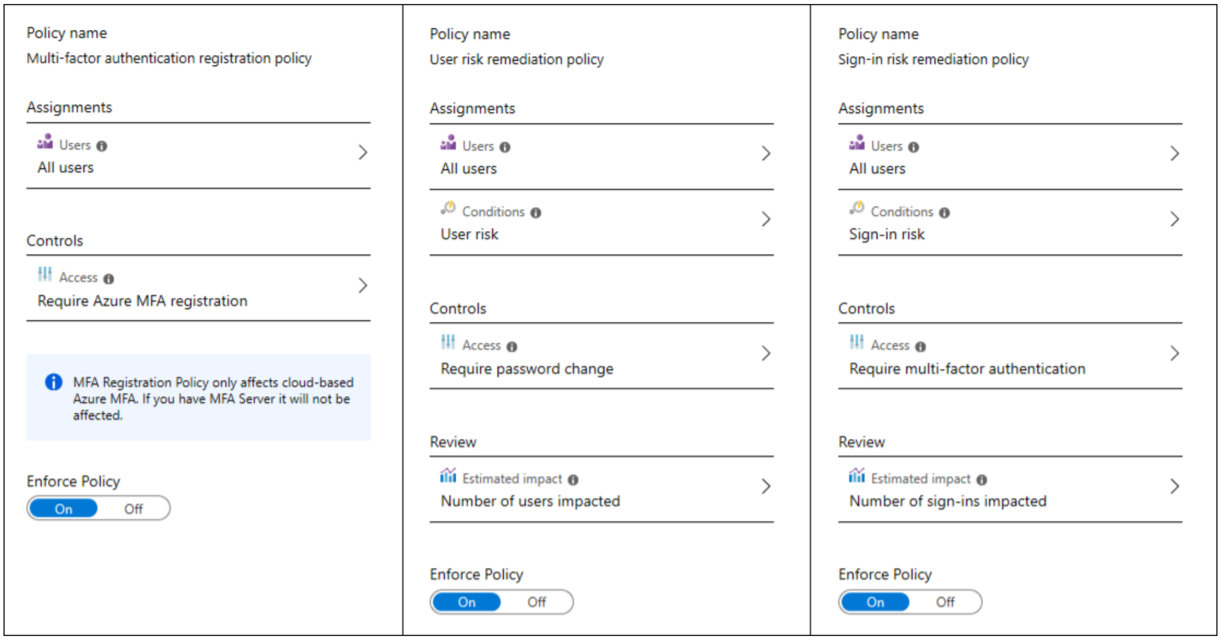
○ Microsoft Authenticator app

● Azure Active Directory Multi-Factor Authentication ✓

Azure Active Directory Multi-Factor Authentication (MFA) is a great way to secure your organization, but users often get frustrated with the extra security layer on top of having to remember their passwords. Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus something you are or something you know. The other choices are passwordless authentication options that integrate with Azure AD. Azure AD DS) enables the use of ciphers such as NTLM v1 and TLS v1.

Identity Protection policies

Azure Active Directory Identity Protection includes three default policies that administrators can choose to enable. These policies include limited customization but are applicable to most organizations. All the policies allow for excluding users such as your emergency access or break-glass administrator accounts.



Policy name
Multi-factor authentication registration policy

Assignments

Users
All users

Controls

Access
Require Azure MFA registration

MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected.

Enforce Policy
On Off

Policy name
User risk remediation policy

Assignments

Users
All users

Conditions
User risk

Controls

Access
Require password change

Review

Estimated impact
Number of users impacted

Enforce Policy
On Off

Policy name
Sign-in risk remediation policy

Assignments

Users
All users

Conditions
Sign-in risk

Controls

Access
Require multi-factor authentication

Review

Estimated impact
Number of sign-ins impacted

Enforce Policy
On Off

Risk Detections

There are two places where you review reported risk detections:

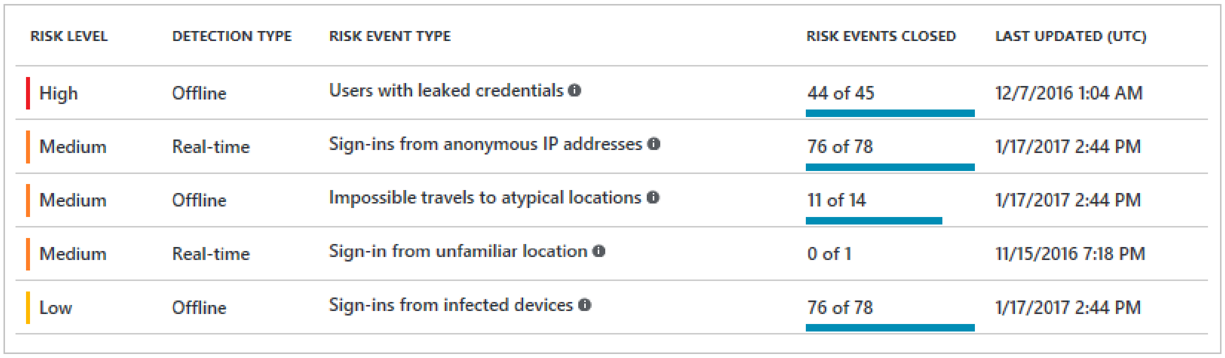
- **Azure AD reporting** - Risk detections are part of Azure AD's security reports.
- **Azure AD Identity Protection** - Risk detections are also part of the reporting capabilities of Azure Active Directory Identity Protection.

In addition, you can use the Identity Protection risk detections API to gain programmatic access to security detections using Microsoft Graph.

Currently, Azure Active Directory detects six types of risk detections:

- **Users with leaked credentials** - When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.
- **Sign-ins from anonymous IP addresses** - This risk detection type identifies users who have successfully signed in from an IP address that has been identified as an anonymous proxy IP address.

- **Impossible travel to atypical locations** - This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior.
- **Sign-ins from infected devices** - This risk detection type identifies sign-ins from devices infected with malware, that are known to actively communicate with a bot server.
- **Sign-in from unfamiliar locations** - This risk detection type considers past sign-in locations (IP, Latitude / Longitude and ASN) to determine new / unfamiliar locations.
- **Sign-ins from IP addresses with suspicious activity** - This risk detection type identifies IP addresses from which a high number of failed sign-in attempts were seen, across multiple user accounts, over a short period of time.



RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices	76 of 78	1/17/2017 2:44 PM

The insight you get for a detected risk detection is tied to your Azure AD subscription.

- With the **Azure AD Premium P2 edition**, you get the most detailed information about all underlying detections.
- With the **Azure AD Premium P1 edition**, advanced detections (such as unfamiliar sign-in properties) are not covered by your license, and will appear under the name Sign-in with additional risk detected. Additionally, the risk level and risk detail fields are hidden.

Important

While the detection of risk detections already represents an important aspect of protecting your identities, you also have the option to either manually address them or implement automated responses by configuring Conditional Access policies.

MFA

Method	Description
Call to phone	Places an automated voice call. The user answers the call and presses # in the phone keypad to authenticate. The phone number is not synchronized to on-premises Active Directory. A voice call to phone is important because it persists through a phone handset upgrade, allowing the user to register the mobile app on the new device.

Method	Description
Text message to phone	Sends a text message that contains a verification code. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS. Two-way SMS means that the user must text back a particular code. Two-way SMS is deprecated and not supported after November 14, 2018. Users who are configured for two-way SMS are automatically switched to call to phone verification at that time.
Notification through mobile app	Sends a push notification to your phone or registered device. The user views the notification and selects Approve to complete verification. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS. Push notifications through the mobile app provide the best user experience.
Verification code from mobile app	The Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS. Verification code from mobile app can be used when the phone has no data connection or cellular signal.

Important

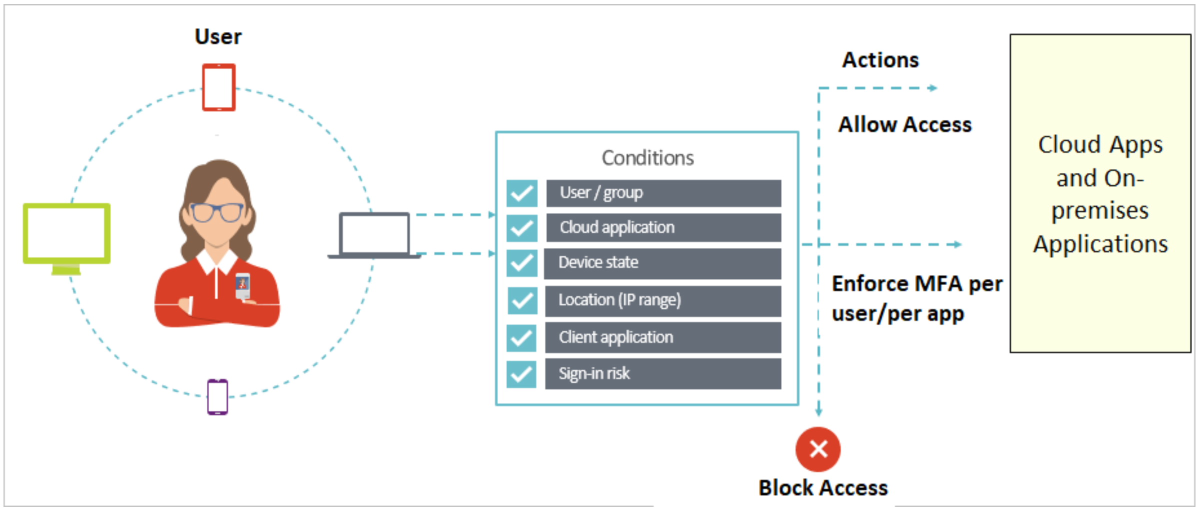
There is also a selection to cache passwords so that users do not have to authenticate on trusted devices. The number of days before a user must re-authenticate on trusted devices can also be configured with the value from 1 to 60 days. The default is 14 days.

Conditional Access

Conditional access comes with six conditions:

1. user/group,
2. cloud application,
3. device state,
4. location (IP range),
5. client application,
6. and sign-in risk.

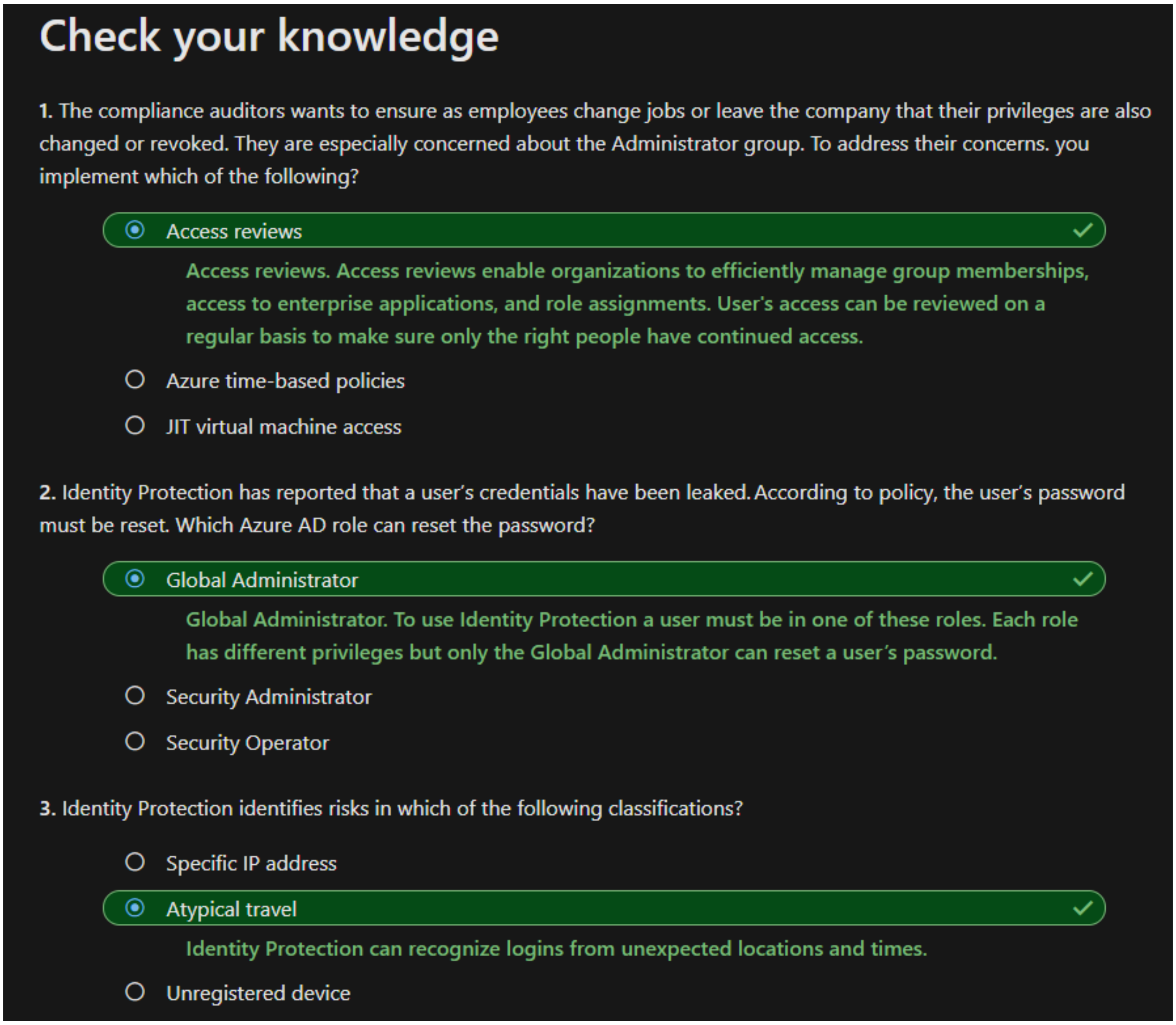
You can use combinations of these conditions to get the exact conditional access policy you need. Notice on this image the conditions determine the access control from the previous topic.



With access controls, you can either Block Access altogether or Grant Access with additional requirements by selecting the desired controls. You can have several options:

- Require MFA from Azure AD or an on-premises MFA (combined with AD FS).
- Grant access to only trusted devices.
- Require a domain-joined device.
- Require mobile devices to use Intune app protection policies.

Requiring additional account verification through MFA is a common conditional access scenario. While users may be able to sign-in to most of your organization's cloud apps, you may want that additional verification for things like your email system, or apps that contain personnel records or sensitive information. In Azure AD, you can accomplish this with a conditional access policy.



Check your knowledge

1. The compliance auditors wants to ensure as employees change jobs or leave the company that their privileges are also changed or revoked. They are especially concerned about the Administrator group. To address their concerns. you implement which of the following?

- ◉ Access reviews ✓

  Access reviews. Access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.
- ○ Azure time-based policies
- ○ JIT virtual machine access

2. Identity Protection has reported that a user’s credentials have been leaked. According to policy, the user’s password must be reset. Which Azure AD role can reset the password?

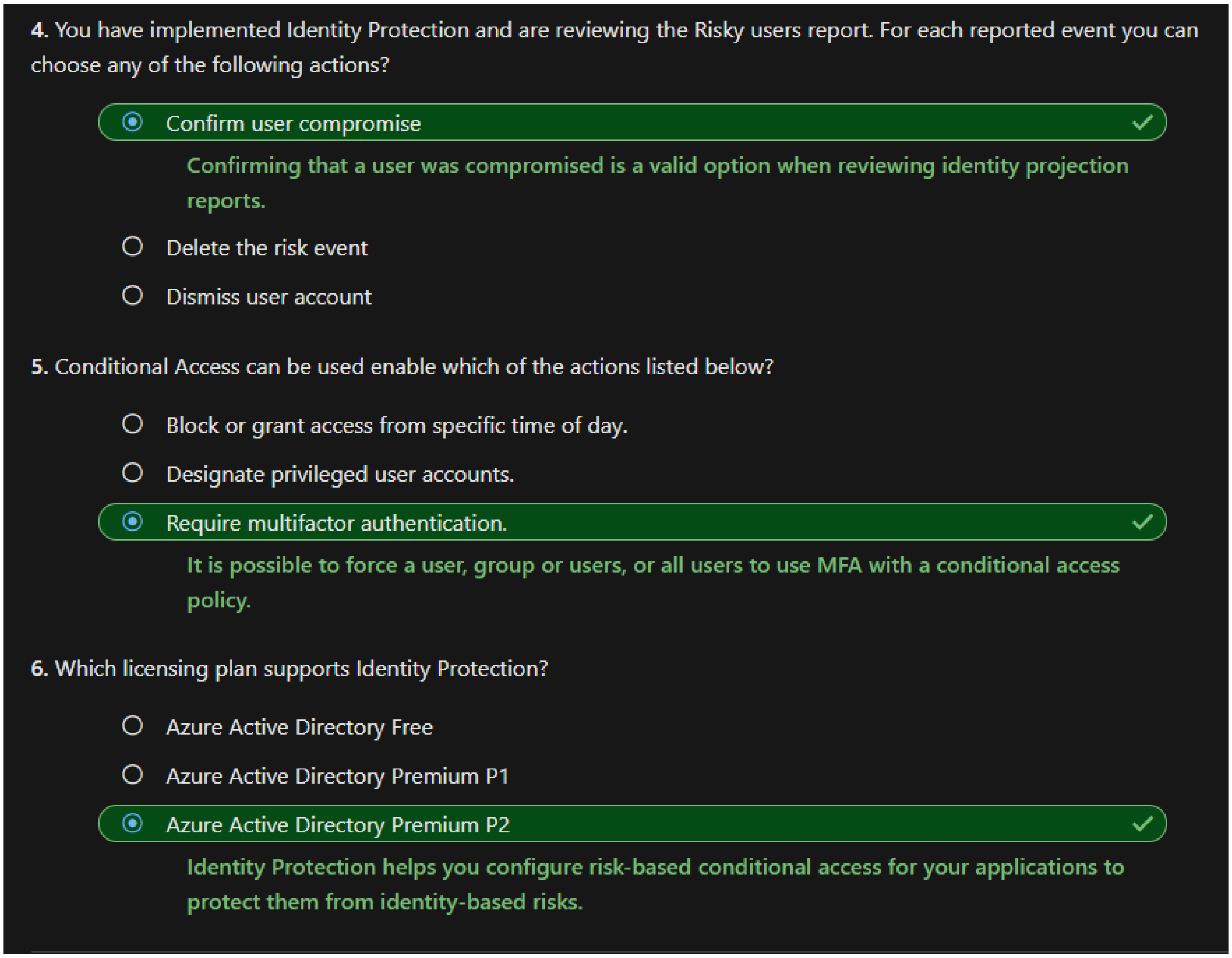
- ◉ Global Administrator ✓

  Global Administrator. To use Identity Protection a user must be in one of these roles. Each role has different privileges but only the Global Administrator can reset a user’s password.
- ○ Security Administrator
- ○ Security Operator

3. Identity Protection identifies risks in which of the following classifications?

- ○ Specific IP address
- ◉ Atypical travel ✓

  Identity Protection can recognize logins from unexpected locations and times.
- ○ Unregistered device



4. You have implemented Identity Protection and are reviewing the Risky users report. For each reported event you can choose any of the following actions?

◉ Confirm user compromise ✓

Confirming that a user was compromised is a valid option when reviewing identity projection reports.

○ Delete the risk event

○ Dismiss user account

5. Conditional Access can be used enable which of the actions listed below?

○ Block or grant access from specific time of day.

○ Designate privileged user accounts.

◉ Require multifactor authentication. ✓

It is possible to force a user, group or users, or all users to use MFA with a conditional access policy.

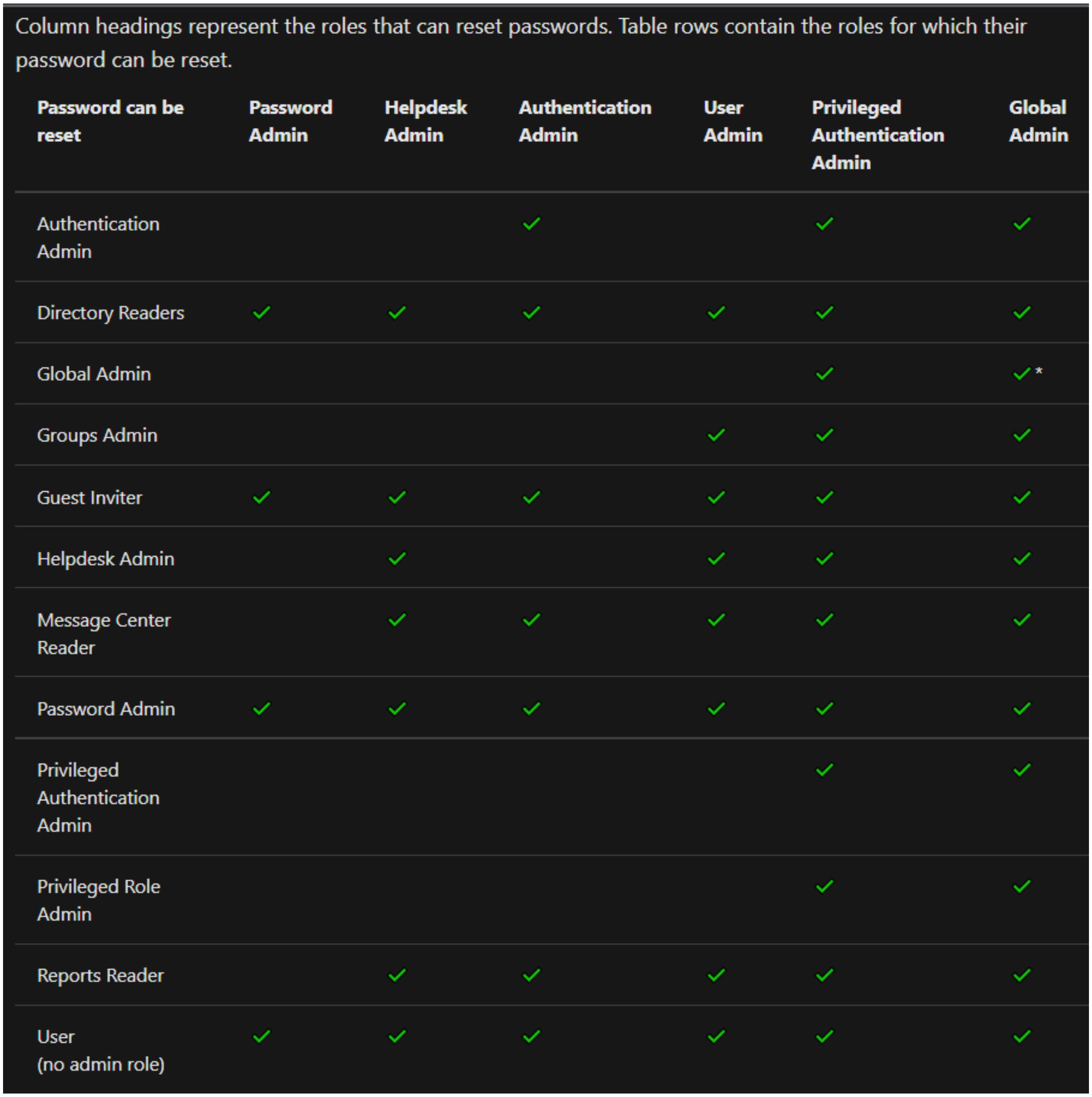
6. Which licensing plan supports Identity Protection?

○ Azure Active Directory Free

○ Azure Active Directory Premium P1

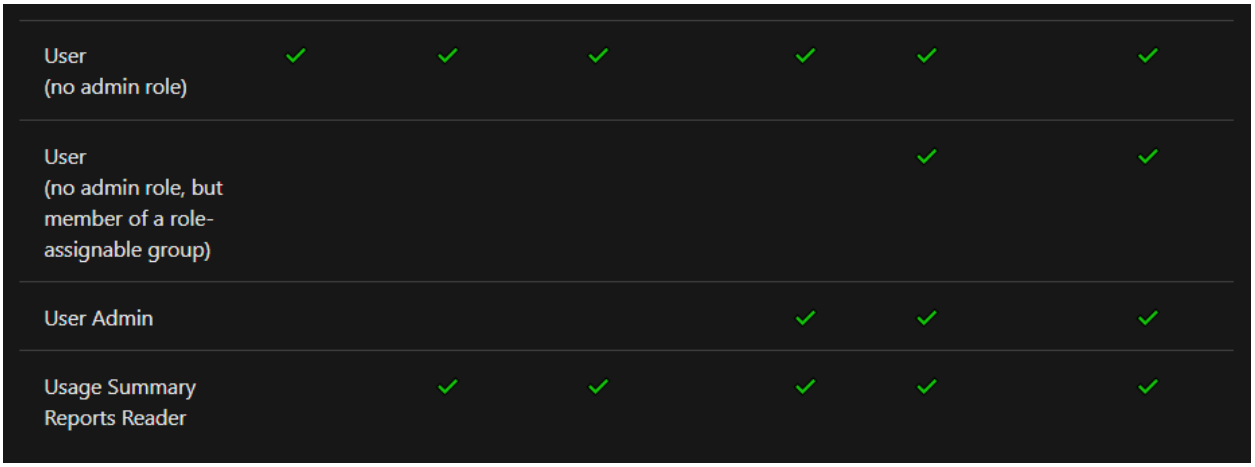
◉ Azure Active Directory Premium P2 ✓

Identity Protection helps you configure risk-based conditional access for your applications to protect them from identity-based risks.



Column headings represent the roles that can reset passwords. Table rows contain the roles for which their password can be reset.

Password can be reset	Password Admin	Helpdesk Admin	Authentication Admin	User Admin	Privileged Authentication Admin	Global Admin
Authentication Admin			✓		✓	✓
Directory Readers	✓	✓	✓	✓	✓	✓
Global Admin					✓	✓*
Groups Admin				✓	✓	✓
Guest Inviter	✓	✓	✓	✓	✓	✓
Helpdesk Admin		✓		✓	✓	✓
Message Center Reader		✓	✓	✓	✓	✓
Password Admin	✓	✓	✓	✓	✓	✓
Privileged Authentication Admin					✓	✓
Privileged Role Admin					✓	✓
Reports Reader		✓	✓	✓	✓	✓
User (no admin role)	✓	✓	✓	✓	✓	✓

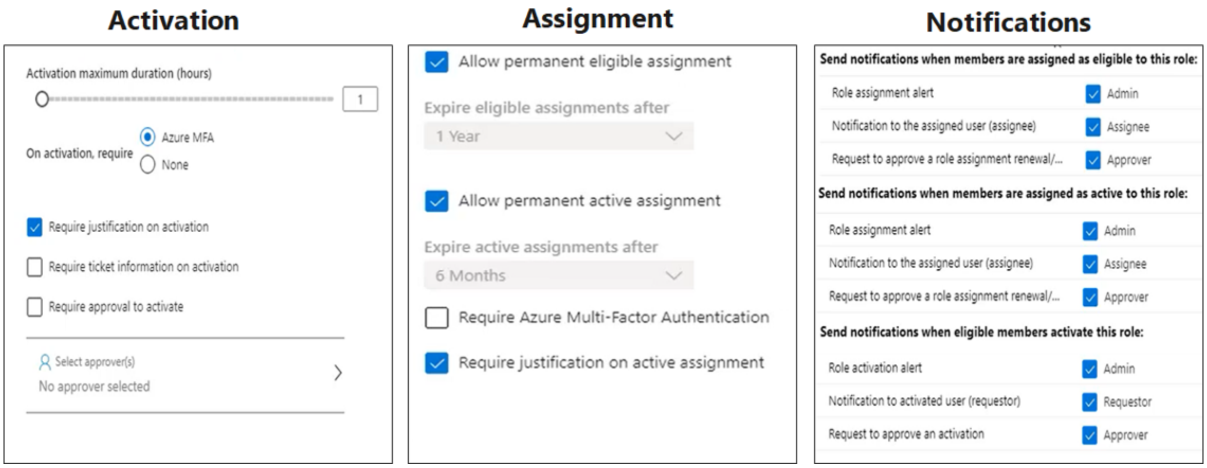


User (no admin role)	✓	✓	✓	✓	✓	✓
User (no admin role, but member of a role-assignable group)					✓	✓
User Admin				✓	✓	✓
Usage Summary Reports Reader		✓	✓	✓	✓	✓

Explore privileged identity management configuration settings

Completed100 XP

- 3 minutes



Activation

Activation maximum duration (hours) 1

On activation, require ● Azure MFA ○ None

☑ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

Select approver(s)
No approver selected

Assignment

☑ Allow permanent eligible assignment

Expire eligible assignments after: 1 Year

☑ Allow permanent active assignment

Expire active assignments after: 6 Months

□ Require Azure Multi-Factor Authentication

☑ Require justification on active assignment

Notifications

Send notifications when members are assigned as eligible to this role:

Role assignment alert	☑ Admin
Notification to the assigned user (assignee)	☑ Assignee
Request to approve a role assignment renewal/...	☑ Approver

Send notifications when members are assigned as active to this role:

Role assignment alert	☑ Admin
Notification to the assigned user (assignee)	☑ Assignee
Request to approve a role assignment renewal/...	☑ Approver

Send notifications when eligible members activate this role:

Role activation alert	☑ Admin
Notification to activated user (requestor)	☑ Requestor
Request to approve an activation	☑ Approver

Activation settings

- **Activation duration**. Set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.
- **Require multifactor authentication on activation**. You can require users who are eligible for a role to prove who they are using Azure Active Directory Multi-Factor Authentication (MFA) before they can activate. Multifactor authentication ensures that the user is who they say they are with reasonable certainty. Enforcing this option protects critical resources in situations when the user account might have been compromised.
- **Require justification**. You can require that users enter a business justification when they activate.
- **Require approval to activate**. If setting multiple approvers, approval completes as soon as one of them approves or denies. You can't require approval from at least two users.

Assignment settings

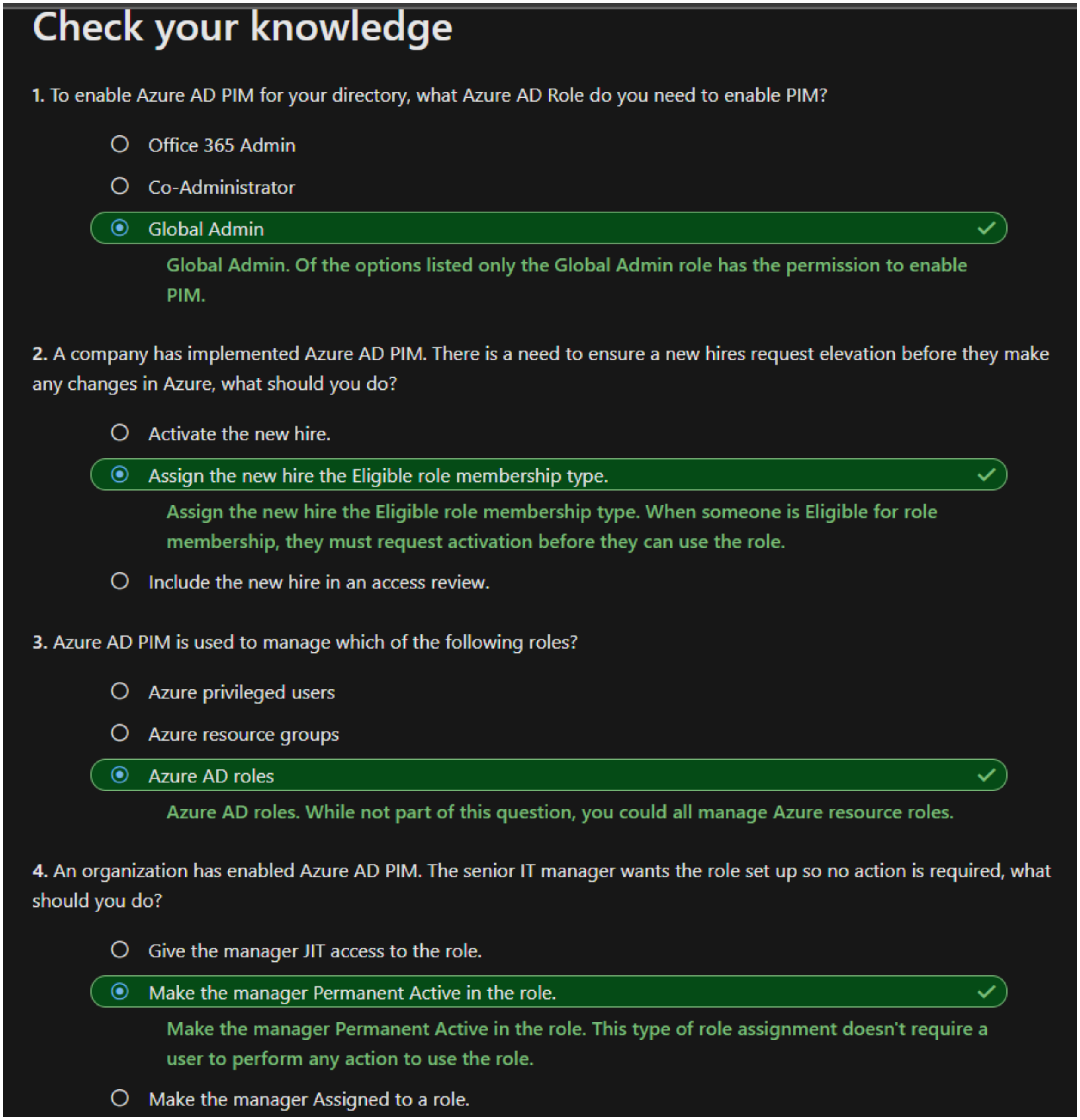
- **Allow permanent eligible assignment**. Global admins and Privileged role admins can assign permanent eligible assignment. They can also require that all eligible assignments have a specified start and end date.
- **Allow permanent active assignment**. Global admins and Privileged role admins can assign active eligible assignment. They can also require that all active assignments have a specified start and end date.

Note

In some cases, you might want to assign a user to a role for a short duration (one day, for example). In this case, the assigned users don't need to request activation. In this scenario, Privileged Identity Management can't enforce multifactor authentication when the user uses their role assignment because they are already active in the role from the time that it is assigned.

Notification settings

- Notifications can be sent when members are assigned as eligible in a role, assigned as active in a role, and when the role is activated.
- Notifications can be sent to Admins, Requestors, and Approvers.



Check your knowledge

1. To enable Azure AD PIM for your directory, what Azure AD Role do you need to enable PIM?

○ Office 365 Admin

○ Co-Administrator

● Global Admin ✓

Global Admin. Of the options listed only the Global Admin role has the permission to enable PIM.

2. A company has implemented Azure AD PIM. There is a need to ensure a new hires request elevation before they make any changes in Azure, what should you do?

○ Activate the new hire.

● Assign the new hire the Eligible role membership type. ✓

Assign the new hire the Eligible role membership type. When someone is Eligible for role membership, they must request activation before they can use the role.

○ Include the new hire in an access review.

3. Azure AD PIM is used to manage which of the following roles?

○ Azure privileged users

○ Azure resource groups

● Azure AD roles ✓

Azure AD roles. While not part of this question, you could all manage Azure resource roles.

4. An organization has enabled Azure AD PIM. The senior IT manager wants the role set up so no action is required, what should you do?

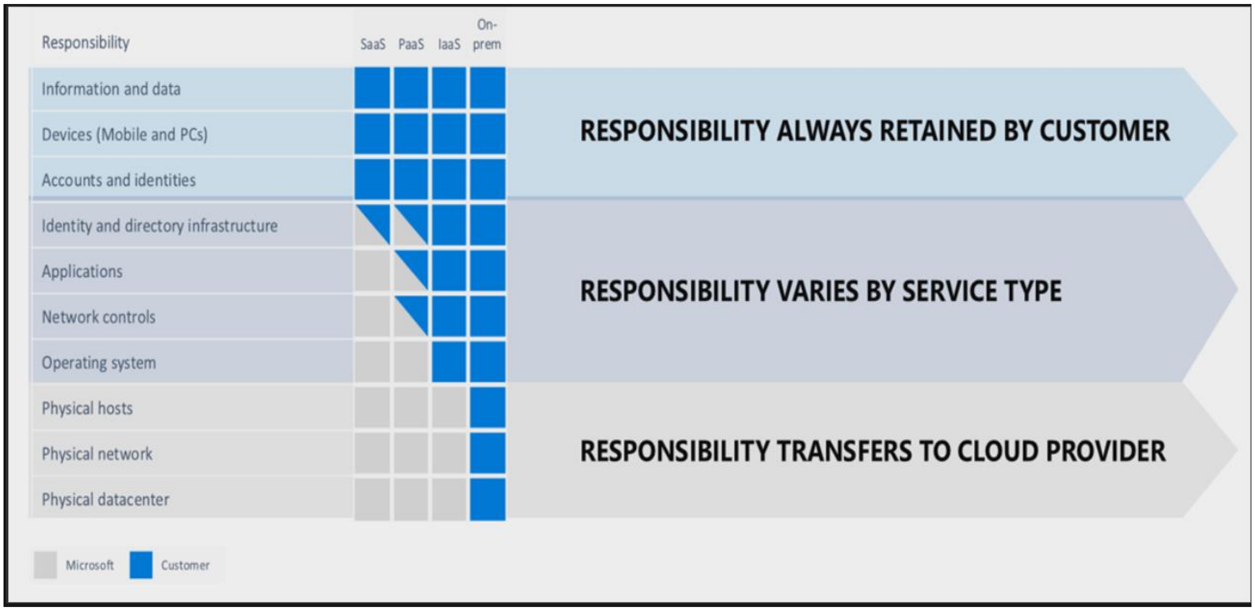
○ Give the manager JIT access to the role.

● Make the manager Permanent Active in the role. ✓

Make the manager Permanent Active in the role. This type of role assignment doesn't require a user to perform any action to use the role.

○ Make the manager Assigned to a role.

The following figure depicts the various responsibility zones.



Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◩	◩	🟦	🟦
Applications	⬜	◩	🟦	🟦
Network controls	⬜	◩	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

⬜ Microsoft 🟦 Customer

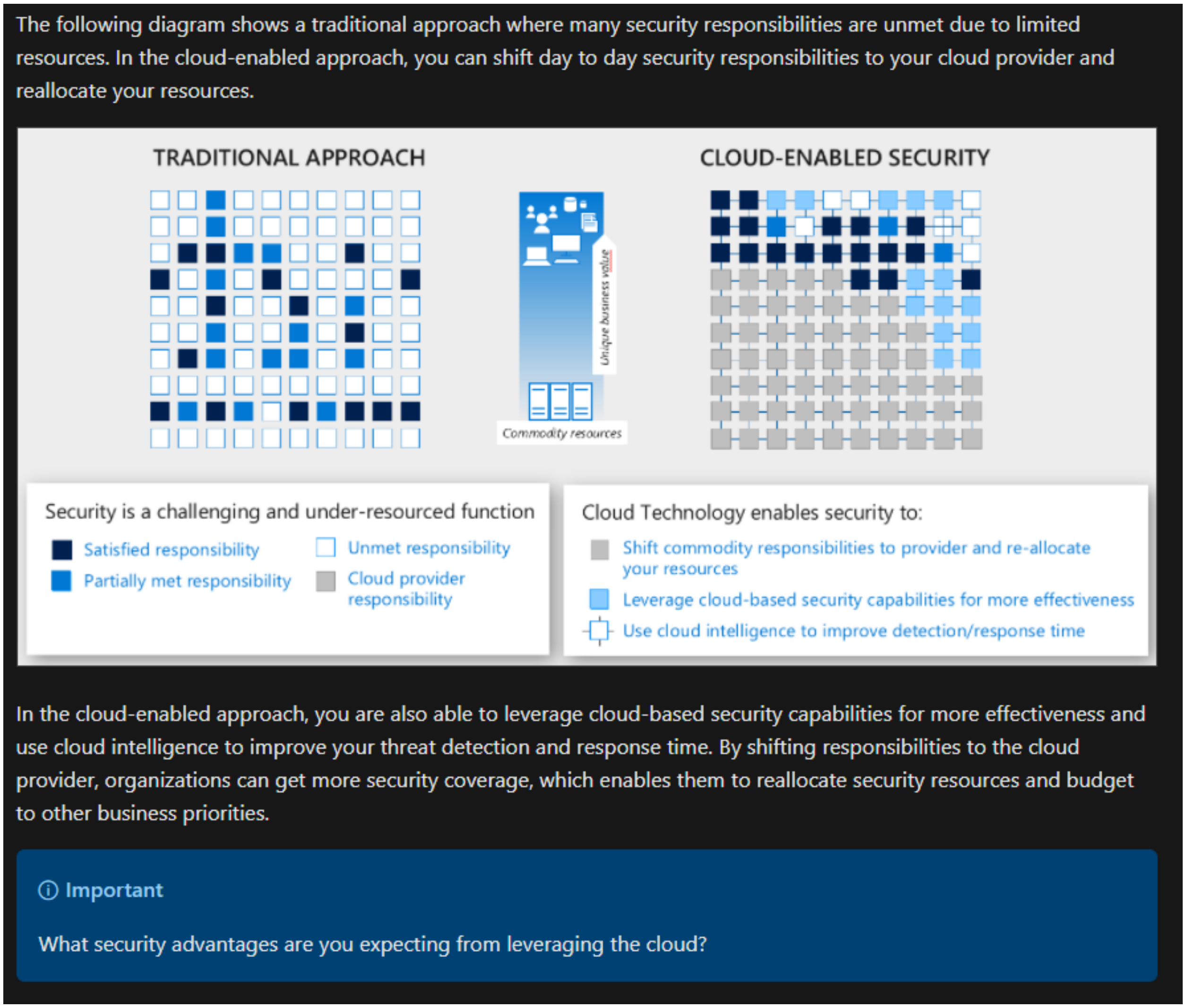
For all cloud deployment types, you own your data and identities. You are responsible for helping secure your data and identities, your on-premises resources, and the cloud components you control (which vary by service type).

Regardless of the deployment type, **you always retain responsibility for the following:**

- Data
- Endpoints
- Accounts
- Access management

Important

It’s important to understand the division of responsibility between you and Microsoft in a Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) deployment.



The following diagram shows a traditional approach where many security responsibilities are unmet due to limited resources. In the cloud-enabled approach, you can shift day to day security responsibilities to your cloud provider and reallocate your resources.

TRADITIONAL APPROACH
CLOUD-ENABLED SECURITY
Unique business value
Commodity resources
Security is a challenging and under-resourced function
Satisfied responsibility
Unmet responsibility
Partially met responsibility
Cloud provider responsibility
Cloud Technology enables security to:
Shift commodity responsibilities to provider and re-allocate your resources
Leverage cloud-based security capabilities for more effectiveness
Use cloud intelligence to improve detection/response time

In the cloud-enabled approach, you are also able to leverage cloud-based security capabilities for more effectiveness and use cloud intelligence to improve your threat detection and response time. By shifting responsibilities to the cloud provider, organizations can get more security coverage, which enables them to reallocate security resources and budget to other business priorities.

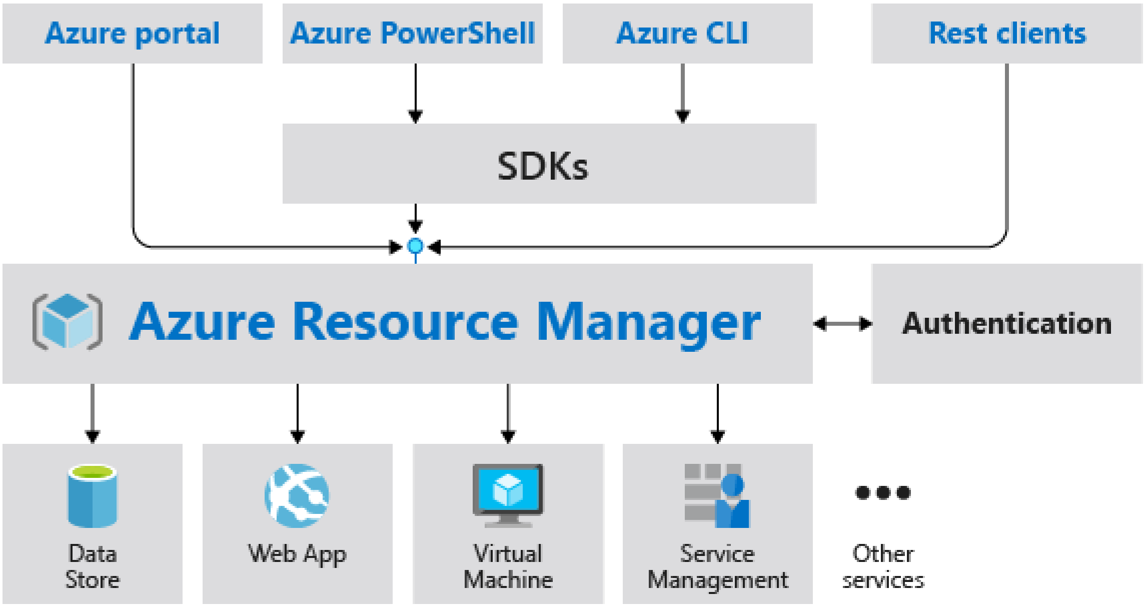
ⓘ Important

What security advantages are you expecting from leveraging the cloud?

Review Azure hierarchy of systems

Azure Resource Manager is the deployment and management service for Azure. It provides a consistent management layer that allows you to create, update, and delete resources in your Azure subscription. You can use its access control, auditing, and tagging features to help secure and organize your resources after deployment.

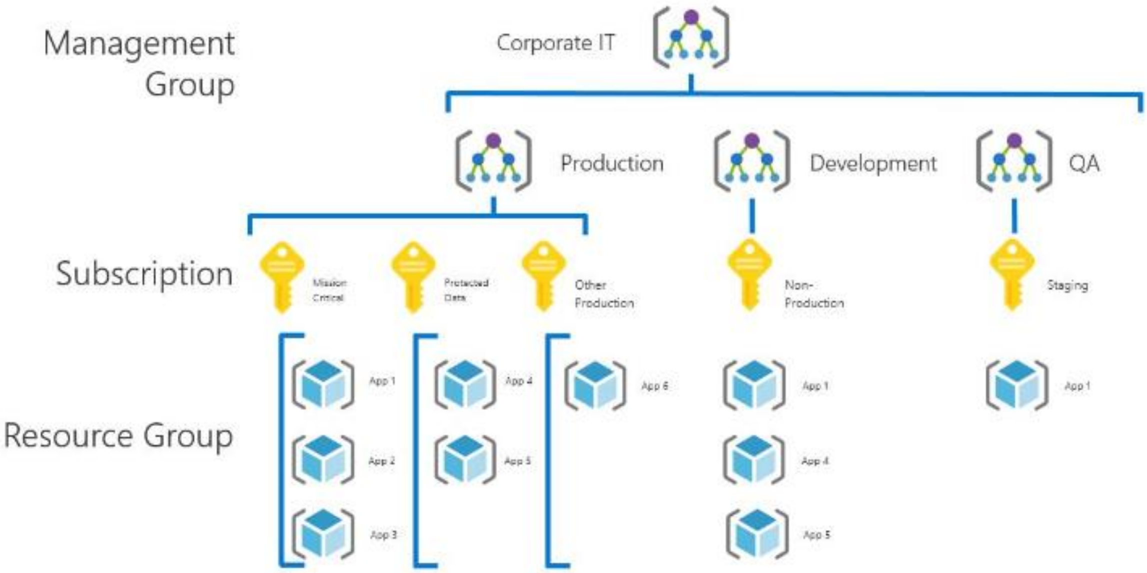
When you take actions through the portal, Azure PowerShell, the Azure CLI, REST APIs, or client software development kits (SDKs), the Resource Manager API handles your request. Because the same API handles all requests, you get consistent results and capabilities from all the different tools. Functionality initially released through APIs should be represented in the portal within 180 days of the initial release.



The Azure Resource Manager uses APIs and authentication to allow access to resources.

Understand Scope

Azure provides four levels of scope: management groups, subscriptions, resource groups, and resources. The following image shows an example of these layers. Though not labeled as such, the blue cubes are resources.



You apply management settings at any of these levels of scope. The level you select determines how widely the setting is applied. Lower levels inherit settings from higher levels. For example, when you apply a policy to the subscription, the policy is applied to all resource groups and resources in your subscription. When you apply a policy on the resource group, that policy is applied to the resource group and all its resources. However, another resource group doesn't have that policy assignment.

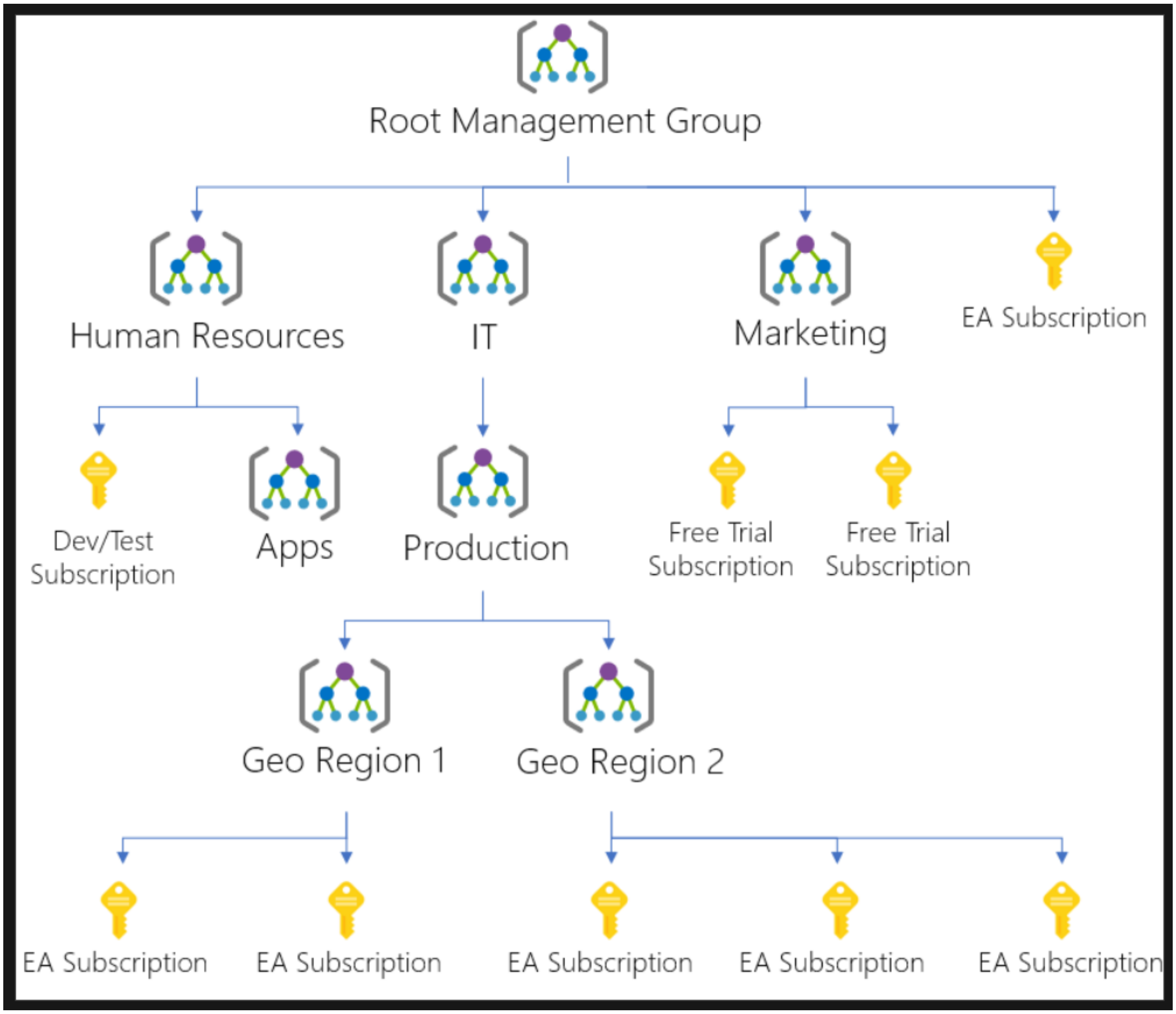
You can deploy templates to management groups, subscriptions, or resource groups.

There are some **important factors to consider** when defining your resource group:

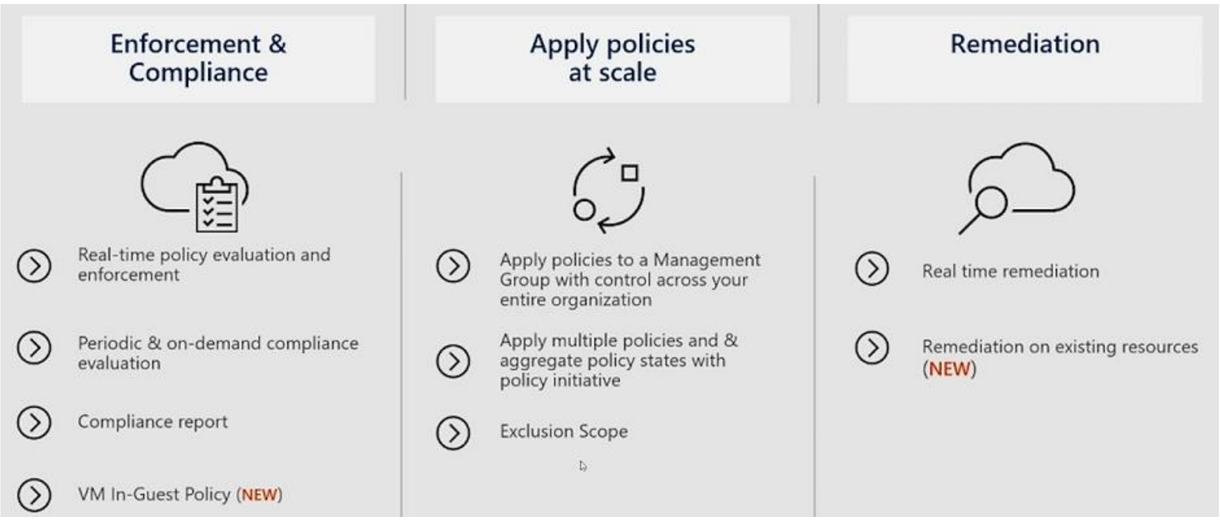
- All the resources in your group **should share the same lifecycle**. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can only exist in **one resource group**.
- You can **add or remove a resource** to a resource group **at any time**.
- You can **move a resource from one resource group to another group**.
- A **resource group** can **contain resources that are located in different regions**.
- A **resource group** can be used to **scope access control for administrative actions**.
- A **resource** can **interact with resources in other resource groups**. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

When creating a resource group, you need to provide a location for that resource group. You may be wondering, **"Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?"** The **resource group stores metadata about the resources**. Therefore, when you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

If the resource group's region is temporarily unavailable, you can't update resources in the resource group because the metadata is unavailable. The resources in other regions will still function as expected, but you can't update them.



There are three main pillars in the functionalities of Azure policy.



Enforcement & Compliance

- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- Compliance report
- VM In-Guest Policy (NEW)

Apply policies at scale

- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Remediation

- Real time remediation
- Remediation on existing resources (NEW)

Policy permissions and custom policies

Azure Policy has several permissions, known as operations, in two resource providers:

- **Microsoft.Authorization**
- **Microsoft.PolicyInsights**

Many built-in roles grant permissions to Azure Policy resources. The **Resource Policy Contributor** role includes most Azure Policy operations. The **Owner** role has full rights. Both **Contributor** and **Reader** can use all Azure Policy read operations, but Contributor can also trigger remediation.

If none of the built-in roles have the required permissions, create a custom role. Azure has by default, security policies that work across subscriptions or on management groups. If these policies need to be augmented with your own organizational policies, new policies can be created.

Whatever the business driver for creating a custom policy, the steps are the same for defining the new custom policy. Before creating a custom policy, check the policy samples to determine if a policy that matches your needs already exists.

The approach to creating a custom policy follows these steps:

- Identify your business requirements
- Map each requirement to an Azure resource property
- Map the property to an alias
- Determine which effect to use
- Compose the policy definition

Composing an Azure Policy

The steps for composing and implementing a policy in Azure Policy begins with creating:

- **Policy definition** - Every policy definition has conditions under which it's enforced. And, it has a defined effect that takes place if the conditions are met.
- **Policy assignment** - A policy definition that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the policy definition is assigned to.
- **Policy parameters** - They help simplify your policy management by reducing the number of policy definitions you must create. You can define parameters when creating a policy definition to make it more generic.

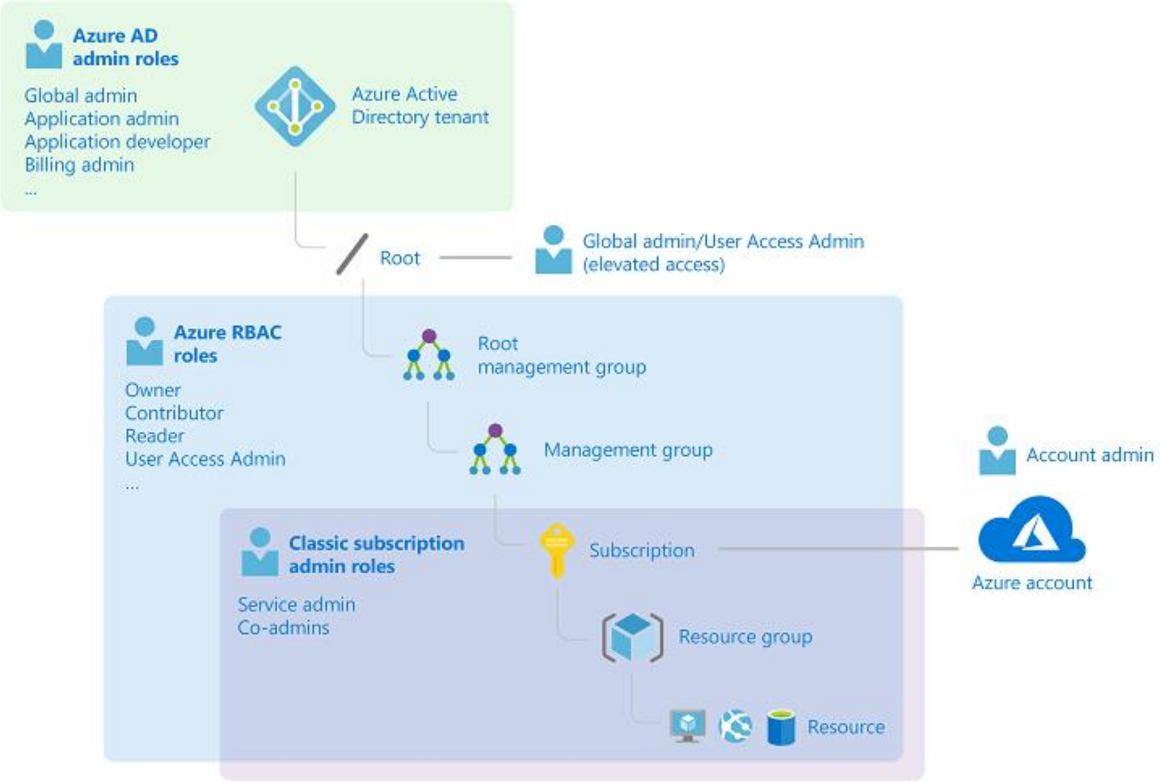
Create and assign an Initiative definition

In order to easily track compliance for multiple resources, create and assign an **Initiative definition**. With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.

To implement these policy definitions (both built-in and custom definitions), you'll need to assign them. You can assign any of these policies through the Azure portal, PowerShell, or Azure CLI.

Azure role-based access control

The following diagram depicts how the classic subscription administrator roles, RBAC roles, and Azure AD administrator roles are related at a high level. Roles assigned at a higher scope, like a subscription, are inherited by child scopes, like service instances.



Important

Note that a subscription is associated with only one Azure AD tenant. Also note that a resource group can have multiple resources but is associated with only one subscription. Lastly, a resource can be bound to only one resource group.

Compare and contrast Azure RBAC vs Azure policies

A few key differences between Azure Policy and RBAC exist. RBAC focuses on user actions at different scopes. You might be added to the contributor role for a resource group, allowing you to make changes to that resource group. Azure Policy focuses on resource properties during deployment and for already-existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, **Azure Policy is a default-allow-and-explicit-deny system**.

RBAC

Azure Role Based Access Control and Azure Policies play an important role in governance to ensure everyone and every resource stays within the required boundaries. They are controls put in place to meet an organizations standards for resource utilization and creation.

RBAC manages who has access to Azure resources, what areas they have access to and what they can do with those resources. RBAC can be used to assign duties within a team and grant only the amount of access needed to allow the assigned user the ability to perform their job instead of giving everybody unrestricted permissions in an Azure subscription or resource.

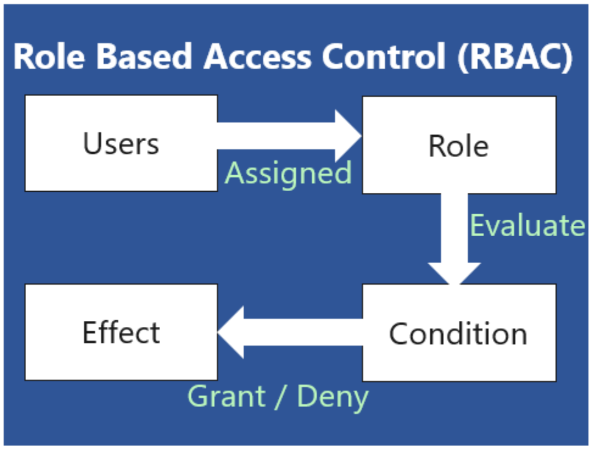
Examples of Role Based Access Control (RBAC) include:

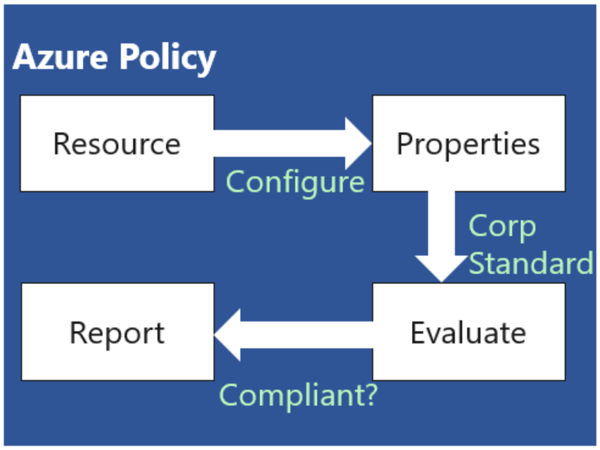
- Allowing a user, the ability to only manage virtual machines in a subscription and not the ability to manage virtual networks
- Allowing a user, the ability to manage all resources, such as virtual machines, websites, and subnets, within a specified resource group
- Allowing an app, to access all resources in a resource group
- Allowing a DBA group, to manage SQL databases in a subscription

RBAC achieves the ability to grant users the least amount privilege to get their work done without affecting other aspects of an instance or subscription as set by the governance plan

Policies

Policies on the other hand play a slightly different role in governance. Azure Policies focus on resource properties during deployment and for already existing resources. As an example, a policy can be issued to ensure users can only deploy DS series VMs within a specified resource should the user have the permission to deploy the VMs. In an existing resource, a policy could be implemented to add or append tags to resources that do not currently have tags to make reporting on costs easier and provide a better way to assign resources to business cost centers.





Important

RBAC and Polices in Azure play a vital role in a governance strategy. While different, they both work together to ensure organizational business rules are followed be ensuring proper access and resource creation guidelines are met.

Built-in roles (RBAC)

Azure role-based access control (RBAC) has several Azure built-in roles that you can assign to users, groups, service principals, and managed identities. Role assignments are the way you control access to Azure resources. If the built-in roles don't meet the specific needs of your organization, you can create your own Azure custom roles.

The four general built-in roles are:

CONFIGURE BUILT-IN ROLES

Built-in Role	Description
Contributor	Lets you manage everything except granting access to resources.
Owner	Lets you manage everything, including access to resources.
Reader	Lets you view everything, but not make any changes.
User Access Administrator	Lets you manage user access to Azure resources.

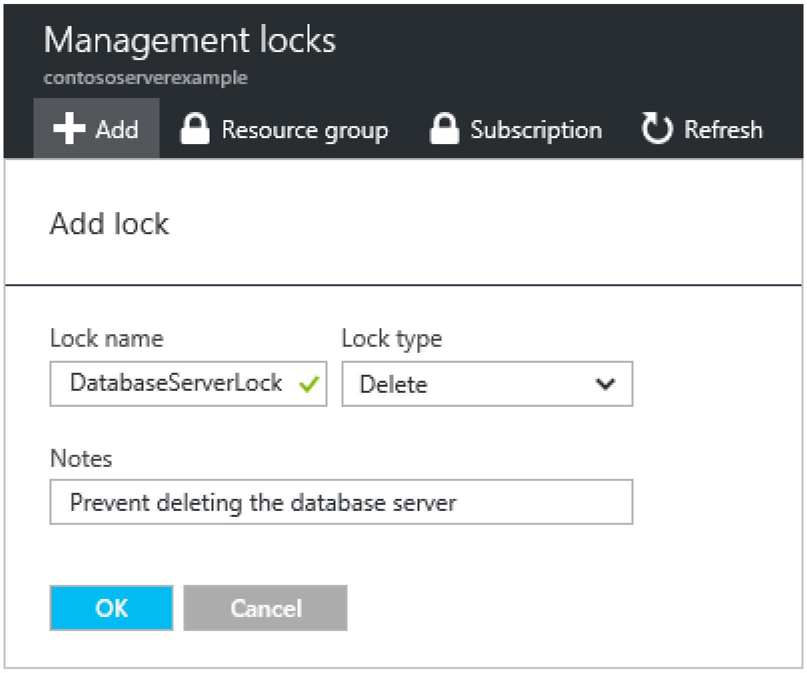
Custom role limits

The following list describes the limits for custom roles.

- Each directory can have up to **5000** custom roles.
- Azure Germany and Azure China 21Vianet can have up to 2000 custom roles for each directory.
- You cannot set AssignableScopes to the root scope ("/").
- You can only define one management group in AssignableScopes of a custom role. Adding a management group to AssignableScopes is currently in preview.
- Custom roles with DataActions cannot be assigned at the management group scope.
- Azure Resource Manager doesn't validate the management group's existence in the role definition's assignable scope.

Enable resource locks

As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to **CanNotDelete or ReadOnly**. In the portal, the locks are called **Delete and Read-only** respectively.



Management locks
contososerverexample

Add lock

Lock name: DatabaseServerLock ✓

Lock type: Delete

Notes: Prevent deleting the database server

- **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Once a resource has been locked, the resource lock must first be removed before the resource can be modified or deleted.

Important

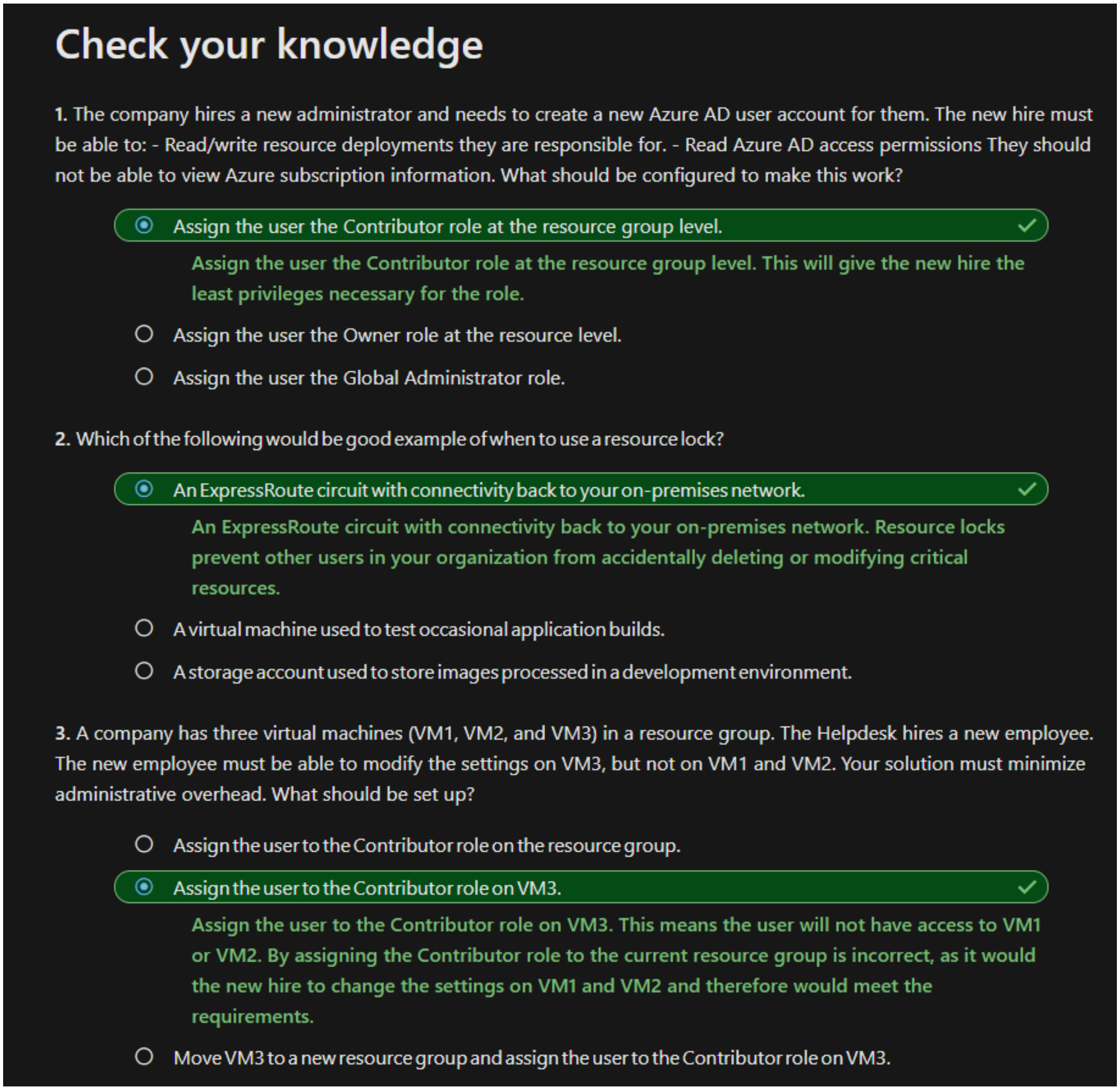
Not every Azure user should have permission to create or remove locks. The role a user is a member of should have permission to set and remove locks. This requires access to one of the following RBAC permissions: **Microsoft.Authorization/**, ***Microsoft.Authorization/locks/*** action. The Owner and User Access Administrator roles have access to those actions. However, these actions can be added to custom roles as required.

Who can transfer a subscription?

A billing administrator or the account administrator is a person who has permission to manage billing for an account. They're authorized to access billing on the Azure portal and do various billing tasks like create subscriptions, view and pay invoices, or update payment methods. If you're an Enterprise Agreement (EA) customer, your enterprise administrators can transfer billing ownership of your subscriptions between accounts.

To identify accounts for which you're a billing administrator, use the following steps:

- Visit the Cost Management + Billing page in Azure portal.
- Select All billing scopes from the left-hand pane.
- The subscriptions page lists all subscriptions where you're a billing administrator.



Check your knowledge

1. The company hires a new administrator and needs to create a new Azure AD user account for them. The new hire must be able to: - Read/write resource deployments they are responsible for. - Read Azure AD access permissions They should not be able to view Azure subscription information. What should be configured to make this work?

◉ Assign the user the Contributor role at the resource group level. ✓

Assign the user the Contributor role at the resource group level. This will give the new hire the least privileges necessary for the role.

○ Assign the user the Owner role at the resource level.

○ Assign the user the Global Administrator role.

2. Which of the following would be good example of when to use a resource lock?

◉ An ExpressRoute circuit with connectivity back to your on-premises network. ✓

An ExpressRoute circuit with connectivity back to your on-premises network. Resource locks prevent other users in your organization from accidentally deleting or modifying critical resources.

○ A virtual machine used to test occasional application builds.

○ A storage account used to store images processed in a development environment.

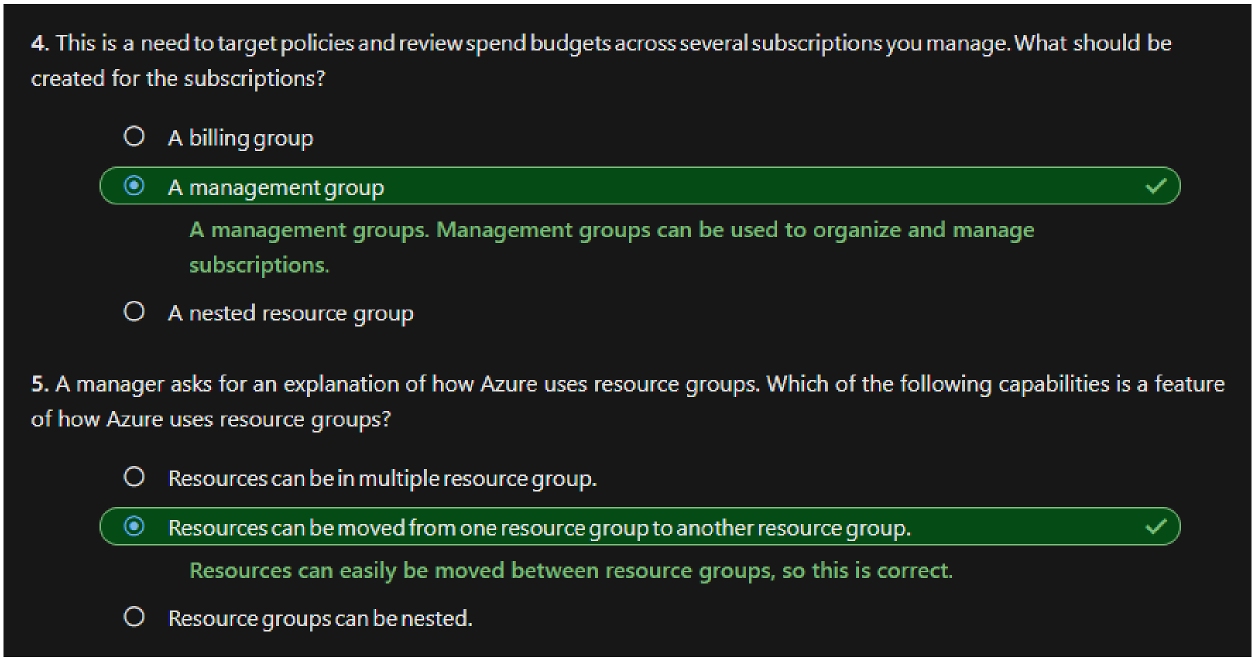
3. A company has three virtual machines (VM1, VM2, and VM3) in a resource group. The Helpdesk hires a new employee. The new employee must be able to modify the settings on VM3, but not on VM1 and VM2. Your solution must minimize administrative overhead. What should be set up?

○ Assign the user to the Contributor role on the resource group.

◉ Assign the user to the Contributor role on VM3. ✓

Assign the user to the Contributor role on VM3. This means the user will not have access to VM1 or VM2. By assigning the Contributor role to the current resource group is incorrect, as it would the new hire to change the settings on VM1 and VM2 and therefore would meet the requirements.

○ Move VM3 to a new resource group and assign the user to the Contributor role on VM3.



4. This is a need to target policies and review spend budgets across several subscriptions you manage. What should be created for the subscriptions?

○ A billing group

● A management group ✓

A management groups. Management groups can be used to organize and manage subscriptions.

○ A nested resource group

5. A manager asks for an explanation of how Azure uses resource groups. Which of the following capabilities is a feature of how Azure uses resource groups?

○ Resources can be in multiple resource group.

● Resources can be moved from one resource group to another resource group. ✓

Resources can easily be moved between resource groups, so this is correct.

○ Resource groups can be nested.