

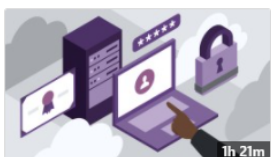
# Microsoft Azure Security Technologies (AZ-500)

## Cert Prep: 1 Manage Identity and Access

Started: 1/20/2022

Updated:

Ended:



COURSE

Microsoft Azure Security Technologies (AZ-500) Cert Prep: 1 Manage Identity and Access

By: Pete Zerger · 2 months ago

1,473 learners

...

### Table of Contents

1. Manage Azure Active Directory (Azure AD) Identities.....	2
1.1 Create and manage a managed identity for Azure resources .....	2
1.2 Manage Azure AD Groups.....	6
1.3 Manage AD Users.....	13
1.4 Manage external identities using Azure AD.....	17
1.5 Manage administrative unit.....	21
1.5 Quiz .....	25
2. Manage Secure Access by Using Azure AD .....	26
2.1 Privileged access for Privileged Identity Management.....	26
2.2 Implement Conditional Access Policies, including MFA .....	34
2.3 Configure Azure AD Privileged Identity Management.....	40
2.4 Configure Azure AD Identity Protection .....	45
3.5 Configure access Reviews .....	48
3.6 Quiz .....	53
References .....	56

## 1. Manage Azure Active Directory (Azure AD) Identities

### 1.1 Create and manage a managed identity for Azure resources

# What Are Managed Identities?

Provide an identity for applications to use when connecting to resources that support Azure AD authentication

## Types of Managed Identities

### System assigned

Is created in Azure AD that is tied to the lifecycle of a **specific service instance**

When the resource is deleted, Azure **automatically deletes the identity** for you

Only that Azure resource can use this identity to request tokens from Azure AD

### User assigned

A managed identity as a **standalone Azure resource**

Can be used by **multiple Azure resources**, determined by you

Has an independent lifecycle, so **must be deprovisioned manually**

**Microsoft recommends using system-assigned managed identities whenever possible.**

# Benefits of Managed Identities

## **You don't need to manage credentials**

Credentials are not even accessible to you.

## **Authenticate to any resource that supports Azure AD**

You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.

## **Improve security, no additional cost**

Freedom from credential management and automated lifecycle management (with system assigned), managed identities benefit security

## Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Configure monitoring and management options for your VM.

### Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

✓ Your subscription is protected by Azure Security Center basic plan.

### Monitoring

Boot diagnostics  ☒ Enable with managed storage account (recommended)  
☐ Enable with custom storage account  
☐ Disable

Enable OS guest diagnostics  ☐

### Identity

System assigned managed identity  ☒ 

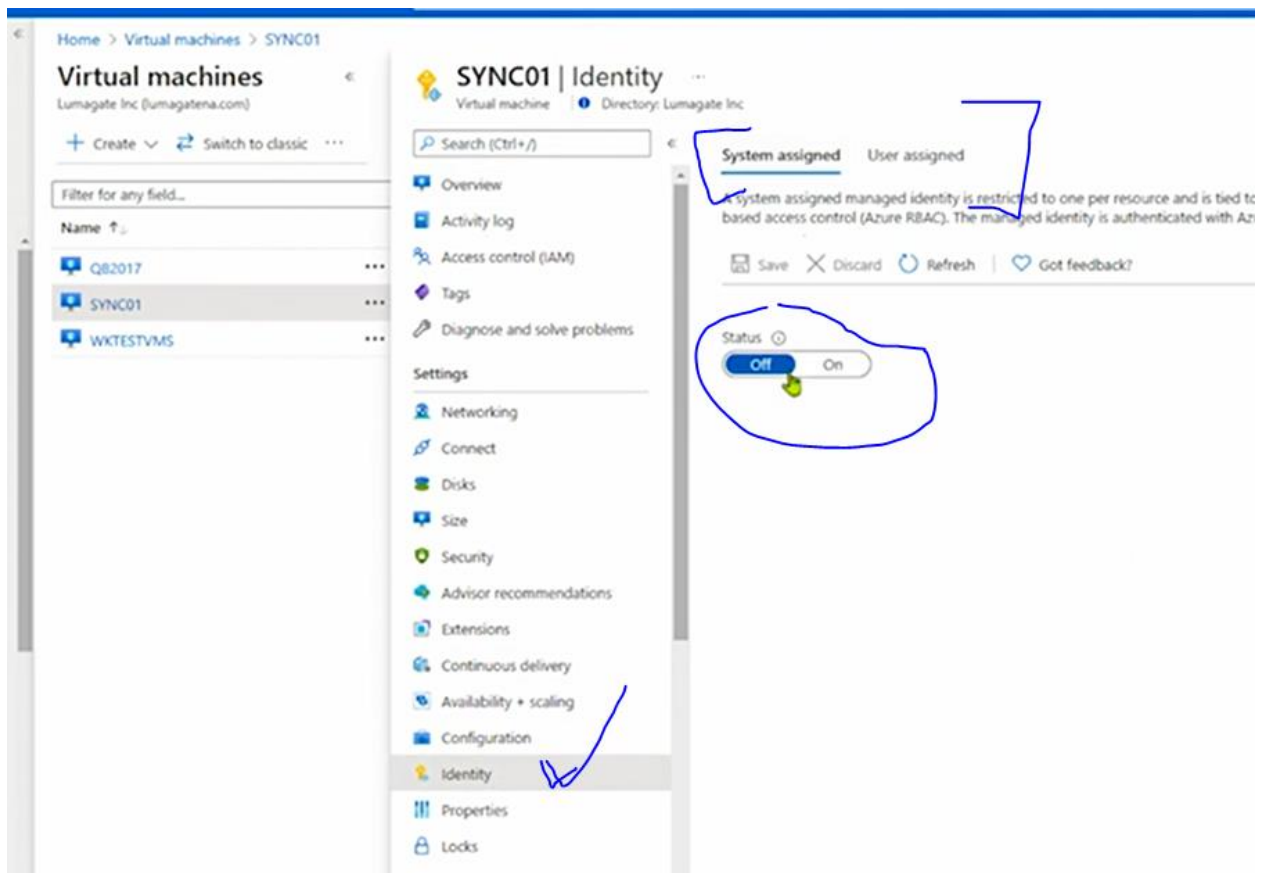
### Azure AD

Login with Azure AD (Preview)  ☐

 RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. [Learn more](#)

# For the Exam

Familiarize yourself with the differences between managed identity types and their implications to security.



# Azure AD Groups Features

- ✓ Dynamic groups
- ✓ Naming policy
- ✓ Access reviews
- ✓ Group licensing
- ✓ Bulk operations
- ✓ Group expiration
- ✓ Office 365 Groups

## Azure AD Group Types

Both store user membership info...

Both help secure files, folders, and apps...



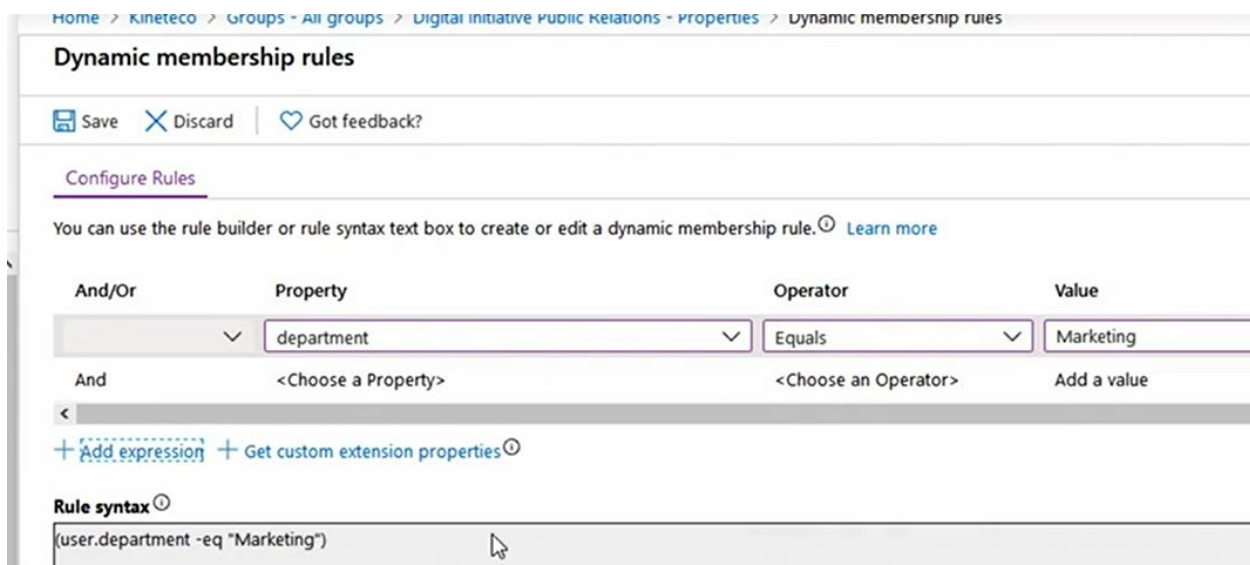
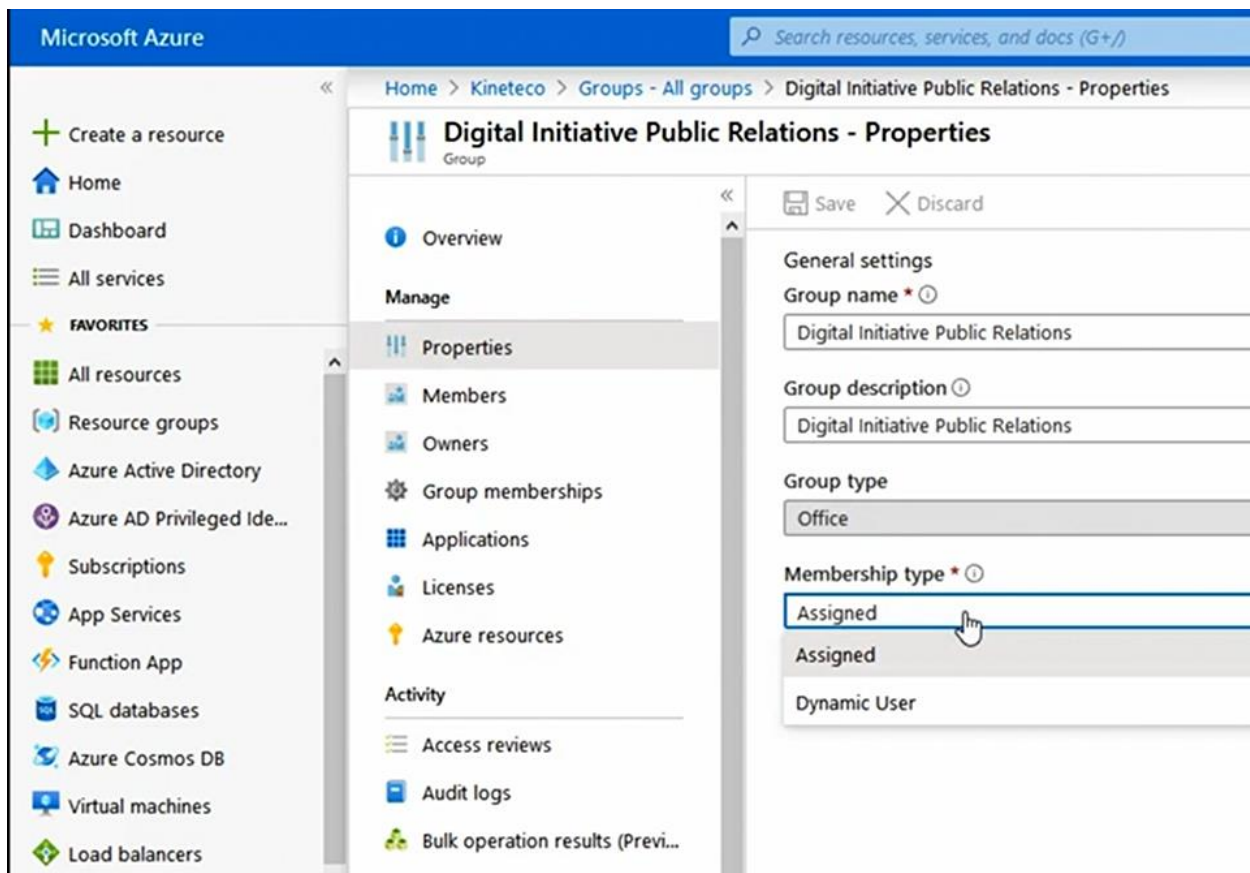


# Office 365 Groups

Automate creation of multiple resources, centralize membership in one place, and allow admins to apply policies at the group level

## Resources with Office 365 Groups

- A shared Outlook inbox
- A shared calendar
- A SharePoint doc library
- A Planner
- Power BI
- Yammer
- A Team
- Roadmap





## Update license assignments

### Select licenses

- ☐ Enterprise Mobility + Security, E5
- ☐ Office 365 E3
- ☐ Office 365 E5
- ☐ Windows 10 Enterprise E3

### Review license options

Select

## Digital Initiative Public Relations - Access reviews

Group

### Overview

#### Manage

#### Properties

#### Members

#### Owners

#### Group memberships

#### Applications

#### Licenses

#### Azure resources

#### Activity

#### Access reviews

#### Audit logs

#### Bulk operation results (Previ...

#### Troubleshooting + Support

#### Troubleshoot

#### New support request

### Active Directory (Azure AD) Access Reviews.

[Learn more about Azure AD Access Reviews](#)

Getting started is fast and easy. You can start your access review within minutes.

1. Onboard with one-click
2. Create your first access review

Use Azure AD Access Reviews to:

- ✓ Recertify employee and guest's group memberships, access to applications, and role assignments on a recurring basis
- ✓ Automate access removal with custom settings
- ✓ Make informed decisions with the help of smart recommendations
- ✓ Organize and track reviews for compliance and risk management initiatives

[Onboard now](#)

Home > Kineteco > Groups - All groups > Digital Initiative Public Relations - Bulk operation results (Preview)

### Digital Initiative Public Relations - Bulk operation results (Preview)

Group

Refresh Help Columns

Got a second? We would love your feedback on Bulk operations →

File name Type

File name All

File name Upload time

No data

# S... # F... Total r... Admin uploa

Download group members

Import group members

Remove group members

Overview

Manage

Properties

Members

Owners

Group memberships

Applications

Licenses

Azure resources

Activity

Access reviews

Audit logs

Bulk operation results (Previ...

Home > Kineteco > Groups - Naming policy

## Groups - Naming policy

Kineteco - Azure Active Directory

Save Discard Delete policy Got feedback?

[Learn more](#) about group naming policies.

**Blocked words** [Group naming policy](#)

### Enable custom blocked words list

You can upload a list of words you wish to block to prevent Office 365 groups being given profane or reserved names and aliases. You may download the .csv file to view and/or edit the existing list of blocked words.

To view and/or edit blocked words list:

1. Download .csv file of blocked words

[Download](#)

2. Add or remove terms (5,000 word maximum)
3. Upload your .csv file

Select a file

**Left Navigation:**

- All groups
- Deleted groups
- Settings
  - General
  - Expiration
  - Naming policy**
- Activity
  - Access reviews
  - Audit logs
  - Bulk operation results (Preview)
- Troubleshooting + Support
  - Troubleshoot
  - New support request

Home > Kineteco > Groups - Naming policy

## Groups - Naming policy

Kineteco - Azure Active Directory

Save Discard Delete policy Got feedback?

[Learn more about group naming policies.](#)

[Blocked words](#) **Group naming policy**

### Group naming policy

The Office 365 groups naming policy allows you to add a specific prefix and/or suffix to the group name and alias of any Office 365 group created by users. For example: <Finance> <group> <Seattle>

#### Current policy

**<Group name>**

Delete

☒ **Add prefix**

Select the type of prefix

Delete

☒ **Add suffix**

Select the type of suffix

Home > Kineteco > Groups - Expiration

## Groups - Expiration

Kineteco - Azure Active Directory

Save Discard

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

Group lifetime (in days) \*

Email contact for groups with \*

Enable expiration for these groups

180

365

Custom

resses separated by a semicolon ;

st not be empty.

ted None

# Exam Tip

Focus on the advanced, security-related features of groups in Azure AD

## 1.3 Manage AD Users

# Managing Azure AD Users

- ✓ Provisioning options
- ✓ Creating and configuring users
- ✓ Deleting and recovering users
- ✓ Security and auth-related configuration

# Important User Settings



User Name

A few important items...



Usage  
location



Authentication  
contact info

## Creating users with PowerShell

### Connect-AzureAD

```
$PasswordProfile = New-Object  
-TypeName.Open.AzureAD.Model.PasswordProfile  
$PasswordProfile.Password = "P@ssw0rd1!"  
New-AzureADUser -DisplayName "New User" `  
-PasswordProfile $PasswordProfile `  
-UserPrincipalName "NewUser@contoso.com" -AccountEnabled $true `  
-MailNickName "Newuser"
```



Home > Kineteco > Users - All users > Allan Deyoung - Authentication methods

## Allan Deyoung - Authentication methods

User

Manage

- Profile
- Assigned roles
- Groups
- Applications
- Licenses
- Devices
- Azure resources
- Authentication methods**

Activity

- Sign-ins
- Audit logs

Reset password Require re-register MFA Revoke MFA sessions Save Discard

Authentication methods are the ways your users sign into Azure AD. Here, you can set the phone numbers and email addresses that users use to perform multi-factor authentication and self-service password reset, and reset a user's password.

### Authentication contact info

Phone

Alternate phone

Email

Alternate email

Home > Kineteco > Users - All users > Allan Deyoung - Assigned roles

## Allan Deyoung - Assigned roles

User

Manage

- Profile
- Assigned roles**
- Groups
- Applications
- Licenses
- Devices
- Azure resources
- Authentication methods

Activity

- Sign-ins
- Audit logs

+ Add assignment X Remove assignment Refresh

### Administrative roles

Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search  Type

Role	Description	Resource N...
No directory roles assigned.		

Home > Kineteco > Users - All users > Allan Deyoung - Audit logs

### Allan Deyoung - Audit logs

User

Manage

- Profile
- Assigned roles
- Groups
- Applications
- Licenses
- Devices
- Azure resources
- Authentication methods

Activity

- Sign-ins
- Audit logs**

Download Refresh Columns Got feedback?

Date: Last 1 month Show dates as: Local Service: All Category: All Activity: All Add filters

Date	Service	Category	Activity	Status	Status Re...	Target(s)	Initiated ...
10/31/2019, 7:...	Core Directory	RoleManage...	Add eligible ...	Success		AllanD@M36...	MS-PIM
10/31/2019, 7:...	Core Directory	RoleManage...	Remove mem...	Success		AllanD@M36...	MS-PIM
10/31/2019, 7:...	PIM	RoleManage...	Remove mem...	Success	First Time Set...	Global Admin...	Pete Zerger
10/28/2019, 9:...	Core Directory	RoleManage...	Remove eligi...	Success		AllanD@M36...	MS-PIM
10/28/2019, 7:...	PIM	RoleManage...	Add member ...	Success	Make perman...	62e90394-69f...	Azure AD
10/28/2019, 5:...	Core Directory	RoleManage...	Add eligible ...	Success		AllanD@M36...	MS-PIM
10/28/2019, 5:...	PIM	RoleManage...	Remove mem...	Success	First Time Set...	Global Admin...	Pete Zerger
10/28/2019, 4:...	PIM	RoleManage...	Add eligible ...	Success	User already ...	Global Admin...	Pete Zerger
10/28/2019, 4:...	PIM	RoleManage...	Add member ...	Success	User already ...	Global Admin...	Pete Zerger

Home > Kineteco > Users - Deleted users

### Users - Deleted users

Kineteco - Azure Active Directory

Delete permanently Restore user Bulk restore Refresh Columns

Restore user

Users are permanently deleted automatically 30 days after they are deleted.

Name

Search by name or email

Name	User name	User type	Source	Deletion date	Permanent deletion ...
<input checked="" type="checkbox"/> Alex Wilbe	AlexW@M365x39...	Member	Azure Active Dire...	10/31/2019, 4:08:25 PM	11/30/2019, 3:08:25 PM
<input type="checkbox"/> Provisionir	provisioninguser0...	Member	Azure Active Dire...	10/22/2019, 11:00:43 ...	11/21/2019, 10:00:43 ...
<input type="checkbox"/> Provisionir	provisioninguser1...	Member	Azure Active Dire...	10/22/2019, 11:00:43 ...	11/21/2019, 10:00:43 ...
<input type="checkbox"/> Provisionir	provisioninguser2...	Member	Azure Active Dire...	10/22/2019, 11:00:43 ...	11/21/2019, 10:00:43 ...
<input type="checkbox"/> Provisionir	provisioninguser3...	Member	Azure Active Dire...	10/22/2019, 11:00:44 ...	11/21/2019, 10:00:44 ...
<input type="checkbox"/> Provisionir	provisioninguser4...	Member	Azure Active Dire...	10/22/2019, 11:00:44 ...	11/21/2019, 10:00:44 ...

# For the Exam

Focus on the aspects of user management related to authentication, access, and automation.

## External Identity Scenarios

**There are four approaches to external identities in Azure Active Directory (Azure AD) you should be familiar with:**

1. External identities

When collaborating with partner organizations **with an Azure AD tenant**

2. External identities with social IdP

For partners, contractors, or customers **with a social identity** (Google, Facebook, etc.)

## External Identity Scenarios

3. External identities with direct federation

For organizations **without an Azure AD** but have a service that supports the SAML or WS-Federation protocols

4. External identities OTP (one-time password) with email

When other means, such as Azure AD, Microsoft account (MSA), or social identity providers are not an option

# Tenants in the External Identity Scenarios



**Resource tenant**  
(where the app or resource is)



**Account tenant**  
(where the account is)

**You have two tenants to think about when approaching the topic of external identities.**

**You will be the **resource tenant admin** in most exam scenarios.**

## Process Flow for External Identity Scenarios

1. Resource tenant admin creates invitation for external user.
2. User object is created for external user (when invite is accepted).
3. External user accesses resources for the first time.
4. Home Realm Discovery (HRD)
5. HRD configuration is looked up, then authentication sequence takes place.



Dashboard > Lumagate Inc | Overview ...

Azure Active Directory

Overview Preview features Diagnose and solve problems

Manage

- Users
- Groups
- External Identities ✓
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses

Overview Monitoring Tutorials

Search your tenant

Basic information

Name	Lumagate Inc	Users	258
Tenant ID		Groups	2,227
Primary domain	lumagatena.com	Applications	177
License	Azure AD Premium P2	Devices	65

My feed

**Pete Zerger**  
Global administrator and 3 other roles  
[More info](#)

**TLS 1.0, 1.1 and 3DES deprecation**  
Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Dashboard > Lumagate Inc > External Identities

External Identities | All identity providers ...

Lumagate Inc - Azure Active Directory

Search (Ctrl+/)

Get started

All identity providers ✓

External collaboration settings

Diagnose and solve problems

Self-service sign up

- Custom user attributes
- All API connectors
- User flows

Subscriptions

- Linked subscriptions

Lifecycle management

- Terms of use
- Access reviews

Troubleshooting + Support

+ Google + Facebook + New SAML/WS-Fed IdP | Got feedback?

Configured identity providers

Name
Azure Active Directory
Microsoft Account
Email one-time passcode
Facebook
Google

SAML/WS-Fed identity providers

Search

Search by domain name

Domain	Protocol	Issuer
You have not added a SAML/WS-Fed identity provider		

Dashboard > Lumagate Inc > External Identities

## External Identities | All identity providers

Lumagate Inc - Azure Active Directory

Search (Ctrl+/)

+ Google + Facebook + New SAML/WS-Fed IDP

Get started

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

User flows

Subscriptions

Linked subscriptions

### Configured identity providers

Name
Azure Active Directory
Microsoft Account
Email one-time passcode
Facebook
Google

### SAML/WS-Fed identity providers

Search

### Configure identity provider

Delete

You must configure credentials at Google APIs first to get the client ID and client secret. →

Name

Google

Client ID \*

672088824373-ph4e1ni26qtda1lt19m5int1gomt9b8d.apps.googleusercontent.com

Client secret \*

\*\*\*\*\*

Dashboard > Lumagate Inc > External Identities

## External Identities | All identity providers

Lumagate Inc - Azure Active Directory

Search (Ctrl+/)

+ Google + Facebook + New SAML/WS-Fed IDP

Get started

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

User flows

Subscriptions

Linked subscriptions

Lifecycle management

### Configured identity providers

Name
Azure Active Directory
Microsoft Account
Email one-time passcode
Facebook
Google

### SAML/WS-Fed identity providers

Search

Search by domain name

### New SAML/WS-Fed IDP

You must configure the federating identity provider first. [Learn more](#)

Identity provider protocol \*

SAML

Domain name of federating IdP \*

fabrikam.com

Select a method for populating metadata \*

Select method



# External Identity Scenarios in Azure AD

## **Recap of some fundamental concepts you will want to remember for the exam:**

Resource tenant (where the app or resource is) owns the user lifecycle

Account tenant own the credentials

Flow for each scenario is the same, but authentication technique changes

Resource tenant admin must configure social, direct federation, or email OTP in advance

## **For the Exam**

Know the use cases for external identities and the tasks the resource tenant admin must complete.

### 1.5 Manage administrative unit

## **What Are Administrative Units?**

**Containers of users and groups and serve as a boundary for delegation of administration**

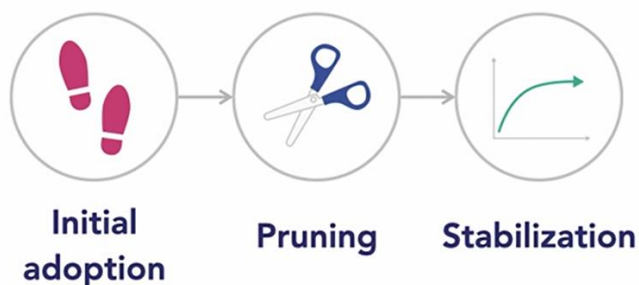
**Azure AD Premium P1 or P2** license for each administrative unit administrator

**Azure AD Free** licenses for administrative unit members

**Assign** delegate users to an Azure AD role with a scope that's limited to one or more administrative units

**Automation/command line** using AzureAD

## Phases of Adoptions



**In most organizations, use of administrative units will evolve over time.**

## Supported Roles

Members of Global Administrator or Privileged Role Administrator roles can create AUs, add or remove members, and delegate to IT staff.

Dashboard > Lumagate Inc

## Lumagate Inc | Administrative units

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

**Administrative units**

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

Learn more

Add

Delete

Refresh

Preview features

Search administrative units

	Name	Description
<input type="checkbox"/>	Brantford	
<input type="checkbox"/>	Houston	

Dashboard > Lumagate Inc > Groups >

## New Group ...

Group type \* ⓘ

Security

Group name \* ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group ⓘ

Yes No

Membership type \* ⓘ

Assigned

Owners

No owners selected

Members

No members selected

# For the Exam

Familiarize yourself with administrative units for delegation, and check documentation for the latest supported scenarios.

## 1.5 Quiz

Question 1 of 5

Administrative units in Azure AD can contain users, groups, and devices.

☒ FALSE  
Correct

Administrative units can contain only users and groups.

☐ TRUE

Question 2 of 5

Whenever possible, Microsoft recommends using which type of managed identity?

☒ system-assigned  
Correct

Because a system-assigned identity eliminates need for managing password and identity lifecycle, it is the preferred option.

☐ app registration

☐ user-assigned

☐ service principal

Question 3 of 5

You can create new users in Azure AD with the Create-AzureADUser cmdlet.

☐ TRUE

☒ FALSE  
Correct

This is false. The New-AzureADUser cmdlet is used to create new users in Azure AD.

Question 4 of 5

The object for external users is created in your Azure AD tenant appears \_\_\_\_.

☒ after the user accepts the invitation

**Correct**

The object for the external user is fully created in your directory once they accept your invitation for access.

☐ after you send the invitation to the user

**Incorrect**

☐ after the external user accesses a resource

Question 5 of 5

Security Groups and Office 365 groups can both be used to secure Azure resources.

☒ TRUE

**Correct**

Office 365 groups can be used to secure resources, just like Security groups. Office 365 also include additional functionality.

☐ FALSE

## 2. Manage Secure Access by Using Azure AD

### 2.1 Privileged access for Privileged Identity Management



Microsoft Azure

Search resources, services, and docs (G+/)

**Azure services**

Create a resource

Azure AD Privileged

Azure Active Directory

Subscriptions

Resource groups

Groups

Multi-Factor Authentication

All resources

**Azure AD Privileged Identity Management**

View

**Description**

Protect your organization from the risk of compromised permanent privileged user accounts by managing, controlling, and monitoring your privileged identities. Privileged Identity Management provides you a way to enable on-demand time limited access for administrative tasks.

**TYPE**

Subscription

Resource group

Resource groups

All resources

Dashboard

Home > Privileged Identity Management > Azure AD roles - Directory roles audit history

**Azure AD roles - Directory roles audit history**

Filter Refresh Export

Sort: Time Action Role

Time	Requestor	Action	Member	Role	Reasoning
10/30/2019, 10:56...	Pete Zerger	Assign	Pete Zerger admin@kineteco.us	Billing Administrator	-
10/28/2019, 7:00:...	Azure AD	Added	Allan Deyoung AllanD@M365x390295.O...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Nestor Wilke NestorW@M365x39029...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Isaiah Langer IsaiahL@M365x390295...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Lidia Holloway LidiaH@M365x390295.O...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Provisioning User provisioninguser0@M36...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Provisioning User provisioninguser1@M36...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Provisioning User provisioninguser2@M36...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Provisioning User provisioninguser3@M36...	Global Administrator	Make perman
10/28/2019, 7:00:...	Azure AD	Added	Provisioning User provisioninguser4@M36...	Global Administrator	Make perman

My requests

Approve requests

Review access

**Manage**

Roles

Members

Alerts

Access reviews

Wizard

Settings

**Activity**

Directory roles audit history

My audit history

Troubleshooting + Support

Home > Privileged Identity Management > Azure AD roles - Alerts

### Azure AD roles - Alerts

Kinectico

My requests  
Approve requests  
Review access

Manage

- Roles
- Members
- Alerts**
- Access reviews
- Wizard
- Settings

Activity

- Directory roles audit history
- My audit history

Scan now

Alert name	Severity
Roles are being assigned outside of PIM	High
There are too many global administrators	Low

Home > Privileged Identity Management > Azure AD roles - Wizard

### Azure AD roles - Wizard

Kinectico

My requests  
Approve requests  
Review access


Manage

- Roles
- Members
- Alerts
- Access reviews
- Wizard**
- Settings

- 1 Discover privileged roles
- 2 Convert members to eligible
- 3 Review the changes to your members in privileged roles

Discover privileged roles

Kinetico



Review this list of privileged roles that exist in your directory. Select each role to see permanent or eligible users in roles.

[Learn more about privileged roles;](#)


ROLES

Role	Permanent	Eligible	
Global Administrator	10	2	>
Security Administrator	1	0	>
Privileged Role Administrator	1	0	>
Billing Administrator	0	1	>

Home > Privileged Identity Management > Azure AD roles - Wizard > Discover privileged roles > Global Administrator

## Discover privileged roles

Kineteco

 Review this list of privileged roles that exist in your directory. Select each role to see permanent or eligible users in roles.  
[Learn more about privileged roles.](#)











ROLES

Role	Permanent	Eligible	
Global Administrator	10	2	>
Security Administrator	1	0	>
Privileged Role Administrator	1	0	>
Billing Administrator	0	1	>

[Next](#)

### Global Administrator

Permanent

-  Allan Deyoung  
AllanD@M365x390295.O...
-  Isaiah Langer  
IsaiahL@M365x390295.O...
-  Lidia Holloway  
LidiaH@M365x390295.O...
-  Nestor Wilke  
NestorW@M365x390295....
-  Pete Zerger  
admin@kineteco.us
-  Provisioning User  
provisioninguser0@M36...
-  Provisioning User  
provisioninguser1@M36...
-  Provisioning User  
provisioninguser2@M36...
-  Provisioning User  
provisioninguser3@M36...
-  Provisioning User  
provisioninguser4@M36...

Microsoft Azure

Search resources, services, and docs (G+)

Home > Privileged Identity Management > Azure AD roles - Wizard > Convert members to eligible

### Convert members to eligible

Kineteco

Global Administrator	
<input type="checkbox"/>	Pete Zerger admin@kineteco.us
<input checked="" type="checkbox"/>	Allan Deyoung AllanD@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Isaiah Langer IsaiahL@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Lidia Holloway LidiaH@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Nestor Wilke NestorW@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Provisioning User provisioninguser4@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Provisioning User provisioninguser3@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Provisioning User provisioninguser2@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Provisioning User provisioninguser1@M365x390295.OnMicrosoft.com
<input checked="" type="checkbox"/>	Provisioning User provisioninguser0@M365x390295.OnMicrosoft.com

Privileged Role Administrator	
<input type="checkbox"/>	Pete Zerger admin@kineteco.us

Security Administrator	
------------------------	--

Next

Home > Privileged Identity Management > Azure AD roles - Wizard > Review changes

## Review changes

Kineteco

Review the changes to your members in privileged roles. You can go to Step 2 to make changes.

Member	ASSIGNMENT
<b>Global Administrator</b>	
Allan Deyoung AllanD@M365x390295.OnMicrosoft.com	Eligible
Isaiah Langer IsaiahL@M365x390295.OnMicrosoft.com	Eligible
Lidia Holloway LidiaH@M365x390295.OnMicrosoft.com	Eligible
Nestor Wilke NestorW@M365x390295.OnMicrosoft.com	Eligible
Provisioning User provisioninguser4@M365x390295.OnMicrosoft.com	Eligible
Provisioning User provisioninguser3@M365x390295.OnMicrosoft.com	Eligible
Provisioning User provisioninguser2@M365x390295.OnMicrosoft.com	Eligible
Provisioning User provisioninguser1@M365x390295.OnMicrosoft.com	Eligible
Provisioning User provisioninguser0@M365x390295.OnMicrosoft.com	Eligible

3 assignments will remain permanent, 9 assignments will be able to activate roles as needed

OK



Search resources, services, and docs (G+)

Home > Privileged Identity Management > Azure AD roles - Roles > Global Administrator - Members

### Global Administrator - Members

[+ Add member](#)
[X Remove member](#)
[Access reviews](#)
[Export](#)
[Refresh](#)

Assignment type: All

Search:

Member	Email	Assignment type	Expiration
<input type="checkbox"/> Adele Vance	AdeleV@kineteco.us	Eligible	-
<input type="checkbox"/> Pete Zerger	admin@kineteco.us	Permanent	-
<input type="checkbox"/> Nestor Wilke	NestorW@M365x390295.On...	Eligible	-
<input type="checkbox"/> Isaiah Langer	IsaiahL@M365x390295.Gl...Mi...	Eligible	-
<input type="checkbox"/> Provisioning User	provisioninguser4@M365x3...	Eligible	-
<input type="checkbox"/> Megan Bowen	MeganB@kineteco.us	Eligible	-
<input type="checkbox"/> Provisioning User	provisioninguser3@M365x3...	Eligible	-

Manage

- Members
- Description
- Troubleshooting + Support
- Troubleshoot
- New support request

# For the Exam

There is no substitute for hands-on experience with Privileged Identity Management.

## 2.2 Implement Conditional Access Policies, including MFA

Dashboard > Contoso Electronics >

# Security | Getting started

Search (Ctrl+ /)

**Getting started**

**Protect**

- Conditional Access ✓
- Identity Protection
- Security Center

**Manage**

- Identity Secure Score
- Named locations
- Authentication methods
- MFA

**Report**

- Risky users
- Risky sign-ins
- Risk detections

**Documentation**

Azure Active Directory offers a range of security features to protect y

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multi Factor Authentication (MFA)

**Security guidance**

For a strong security posture, we recommend the following:

- 5 steps to secure your identity infrastructure
- Azure AD Password Guidance
- Azure AD Data Security Whitepaper
- How Password Hash Sync (PHS) works

---

Dashboard > Contoso Electronics > Security >

## Conditional Access | Policies

Azure Active Directory

+ New policy | What If | Got feedback?

**Policies**

- Insights and reporting
- Diagnose and solve problems
- Manage**
- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Classic policies
- Troubleshooting + Support
- New support request

**Baseline Protection policies are a legacy experience which have been deprecated. They are no longer being enforced, can't be enabled, and will disappear from the Azure Portal soon. If you're looking to enable a security policy for your organization, we recommend enabling Security defaults or configuring Conditional Access policies.**

Policy Name	State
Baseline policy: Require MFA for admins (Preview)	Off
Baseline policy: End user protection (Preview)	Off
Baseline policy: Block legacy authentication (Preview)	Off
Baseline policy: Require MFA for Service Management (Preview)	Off
Require MFA for Delegate Admins	On
MFA Pilot	On

## MFA Pilot

Conditional access policy

 Delete

make decisions, and enforce organizational policies. [Learn more](#)

users, directory roles, or external guest users  
[Learn more](#)

Name \*

MFA Pilot

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Assignments

Users and groups ⓘ

Specific users included >

Cloud apps or actions ⓘ

1 app included >

Conditions ⓘ

0 conditions selected >

Access controls

Grant ⓘ

Select >

1 user



Megan Bowen  
MeganB@mycontoso.us



Enable policy

Report-only

On

Off

Save

## MFA Pilot

Conditional access policy

Delete

Name

MFA Pilot

### Assignments

Users and groups ⓘ

Specific users included

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

### Access controls

Grant ⓘ

1 control selected

Session ⓘ

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Select

Microsoft Azure Management

MA Microsoft Azure Management  
7974846-ba00-4fd7-ba43-dac1f8f63013

⚠ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.  
[Dismiss this warning if you're sure.](#)

Enable policy

Report-only

On

Off

Save

# MFA Pilot

Conditional access policy

 Delete

Name	Not configured	
Assignments	Sign-in risk	
Users and groups	Not configured	
Specific users included	Device platforms	
Cloud apps or actions	Not configured	
1 app included	Locations	
Conditions	Not configured	
0 conditions selected	Client apps (Preview)	
Access controls	Not configured	
Grant	Device state (Preview)	
1 control selected		
Session		

**Include**   **Exclude**

☐ Any location

☐ All trusted locations

☐ Selected locations

Select

None

Enable policy

Report-only   **On**   Off

Save


Microsoft Azure

Search resources, services, and documentation

Dashboard > Contoso Electronics > Security > Conditional Access

## MFA Pilot

Conditional access policy

 Delete

### Assignments

Users and groups ⓘ

Specific users included

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

### Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

### Enable policy

Report-only

On

Off

Save

Grant

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy (Preview) ⓘ  
[See list of policy protected client apps](#)

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

Select

LinkedIn Learning




Here

## Session

Control user access based on session controls to enable limited experiences within specific cloud applications.

[Learn more](#)

☐ Use app enforced restrictions ⓘ



This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

☐ Use Conditional Access App Control ⓘ

☐ Sign-in frequency ⓘ

☐ Persistent browser session ⓘ

## Exam Tip

Know Azure AD Conditional Access well.

# Privileged Identity Management

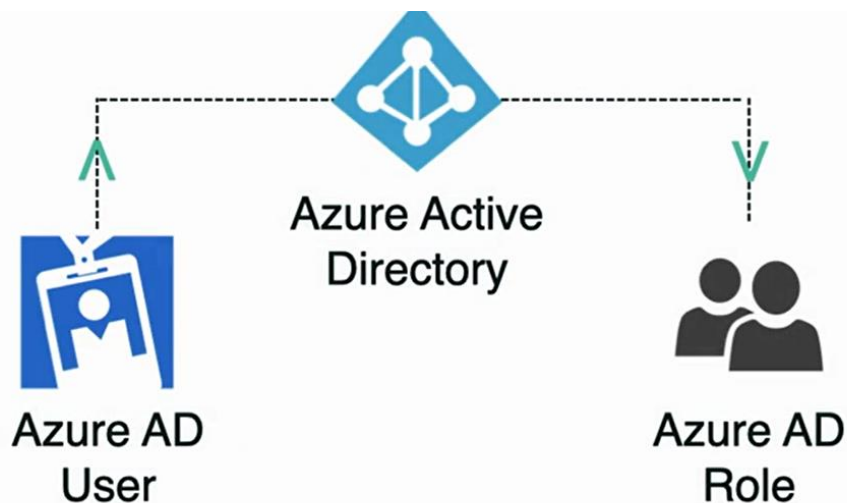
**Simplifies management of privileged access**



**Just-in-Time  
(JIT) Access**

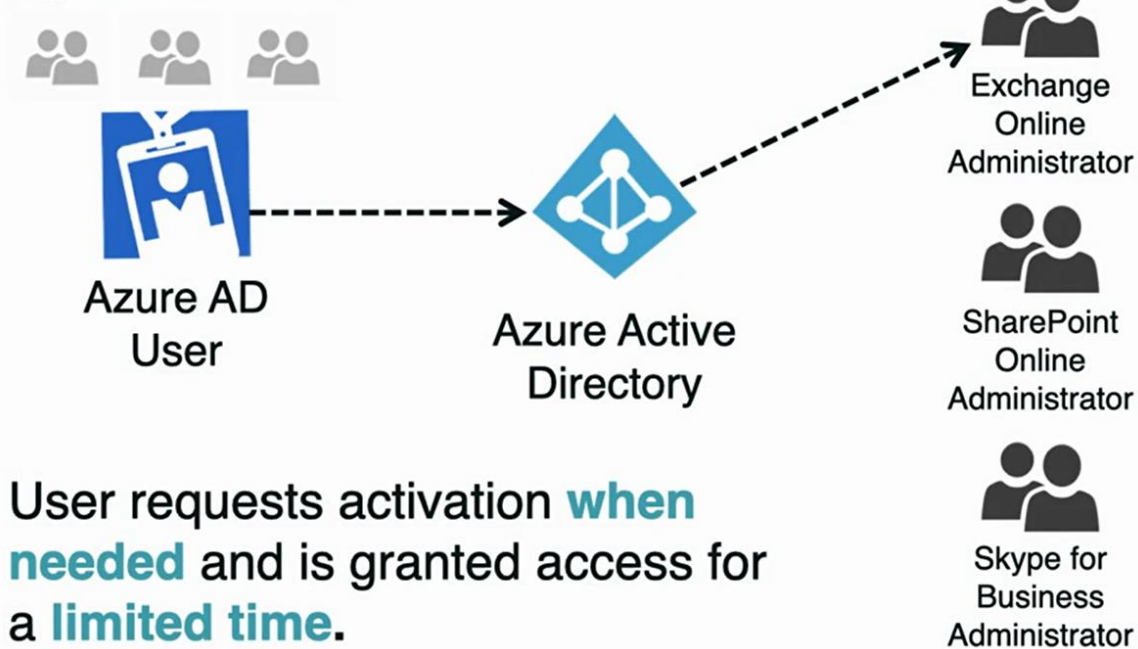


**Just Enough  
Access (JEA)**



**Activate the role** when you need to perform **privileged actions** ... for a limited time.

Eligible Azure AD Roles



## Enabling Azure AD PIM

You'll use the Azure AD PIM app in the Azure portal to request role activation...



Even if operating in another portal



Or using PowerShell for bulk admin tasks

# Activation Requirements

There can be multiple requirements for your activation request to succeed:



Some roles require **multi-factor authentication**.



All require **reason for activation** request.



Some roles require a **help desk ticket number**.

The screenshot shows the 'My roles - Azure AD roles' page in the Azure portal. The left sidebar includes links for 'Activate', 'Azure AD roles', 'Azure AD custom roles (Preview)', 'Azure resources', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main content area has tabs for 'Eligible roles' and 'Active roles'. Below the tabs is a table with columns: Role name, Status, Pending requests, and Action. The table lists the 'Billing Administrator' role with a status of 'Not active' and '0 pending request(s)'. The 'Action' column for this role contains a blue 'Activate' button, which is circled in blue in the image.

Role name	Status	Pending requests	Action
Billing Administrator	Not active	0 pending request(s)	<a href="#">Activate</a>

Home > Privileged Identity Management > My roles - Azure AD roles > Billing Administrator > Verify my identity

### Billing Administrator

Role activation details

☐ Activate ☐ Deactivate

**Verify your identity before proceeding** →

NAME  
Pete Zerger

EMAIL  
admin@kineteco.us


ACTIVATION  
Eligible

EXPIRATION  
-

### Verify my identity

Billing Administrator

Before you activate this role, verify your identity with Azure Multi-Factor Authentication. If you haven't registered with Azure MFA yet, we'll help you do that.

 Verify my identity

Azure AD roles - Quick start

Kineteco

Overview

Quick start

Tasks


- My roles
- My requests
- Approve requests
- Review access

Manage

- Roles
- Members
- Alerts
- Access reviews
- Wizard
- Settings

## Azure AD Privileged Identity Management


Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)



### Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary


[Assign eligibility](#)



### Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

[Activate your role](#)



### Approve

View and approve all activation request for specific Azure AD roles that you are configured to approve

[Approve requests](#)



Home > Privileged Identity Management > Azure AD roles - Settings > Roles > Billing Administrator

### Roles

Kineticco

- Default for all roles
- Application Administrator
- Application Developer
- Authentication Administrator
- Azure DevOps Administrator
- B2C IEF Keyset Administrator
- B2C IEF Policy Administrator
- B2C User Flow Administrator
- B2C User Flow Attribute Administrator
- Billing Administrator**
- Cloud Application Administrator
- Cloud Device Administrator
- Compliance Administrator
- Compliance Data Administrator
- Conditional Access Administrator
- CRM Service Administrator
- Customer LockBox Access Approver
- Desktop Analytics Administrator

### Billing Administrator

Save Discard

**Activations**

Maximum activation duration (hours) ⓘ

☐ 0

**Notifications**

Send email notifying admins of activation ⓘ

Enable **Disable**

**Incident/Request ticket**

Require incident/request ticket number during activation ⓘ

Enable **Disable**

**Multi-Factor Authentication**

Require Azure Multi-Factor Authentication for activation ⓘ

Enable Disable

**Require approval**

Require approval to activate this role ⓘ

**Require approval**

Require approval to activate this role ⓘ

**Enable** **Disable**



# For the Exam

Explore Privileged Identity Management before you take the exam.

## 2.4 Configure Azure AD Identity Protection

### Passwordless Authentication Options

**Azure includes three passwordless authentication options that integrate with Azure Active Directory (Azure AD):**

#### **Windows Hello for Business**

Biometric and PIN credentials that are directly tied to the user's PC, which prevents access from anyone other than the owner

### Passwordless Authentication Options

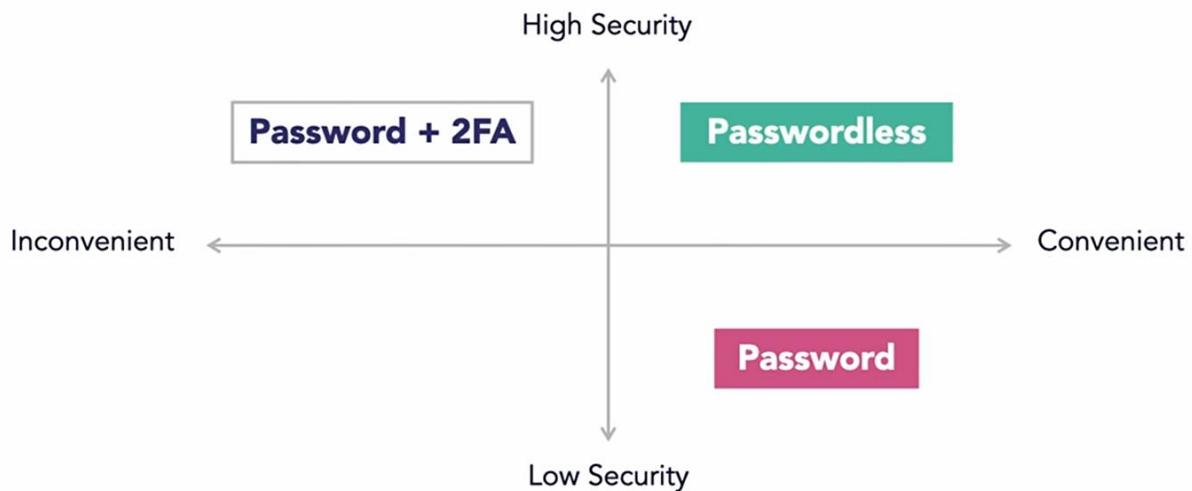
#### **Microsoft Authenticator app**

Allows your employee's phone to become a passwordless authentication method, widely used as an MFA option but works for passwordless also

#### **FIDO2 (Fast IDentity Online) security keys**

Typically USB devices but could also use Bluetooth or NFC; great option in sensitive scenarios or when mobile (Authenticator app) is not an option

# Relative Security of Authentication Options



## Passwordless authentication options for Azure Active Directory

06/28/2021 • 11 minutes to read • +16

Features like multi-factor authentication (MFA) are a great way to secure your organization, but users often get frustrated with the additional 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.

Authentication	Something you have	Something you are or know
Passwordless	Windows 10 Device, phone, or security key	Biometric or PIN

Is this page helpful?

Yes No

In this article ✓

[Windows Hello for Business](#)

[Microsoft Authenticator App](#)

[FIDO2 security keys](#)

[Supported scenarios](#)

[Choose a passwordless method](#)

[Next steps](#)

Use the following table to choose which method will support your requirements and users.

Persona	Scenario	Environment	Passwordless technology
Admin	Secure access to a device for management tasks	Assigned Windows 10 device	Windows Hello for Business and/or FIDO2 security key
Admin	Management tasks on non-Windows devices	Mobile or non-windows device	Passwordless sign-in with the Microsoft Authenticator app
Information worker	Productivity work	Assigned Windows 10 device	Windows Hello for Business and/or FIDO2 security key
Information worker	Productivity work	Mobile or non-windows device	Passwordless sign-in with the Microsoft Authenticator app
Frontline worker	Kiosks in a factory, plant, retail, or data entry	Shared Windows 10 devices	FIDO2 Security keys

### 3.5 Configure access Reviews

Home > Privileged Identity Management - Quick start

## Privileged Identity Management - Quick start

Privileged Identity Management

Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Azure AD roles
- Azure AD custom roles (Preview)
- Azure resources

Activity

- My audit history

Introduction

Secure your organization by managing and restricting privileged access

[Azure AD Privileged Identity Management](#)  
[Azure AD Privileged Identity Management PowerShell module](#)  
[Azure AD Privileged Identity Management for Azure resource roles](#)

### What's new in Privileged Identity Management

- ☒ All services
- ☒ Azure Active Directory
- ☒ Azure resources

**Feature update**

Azure Active Directory

Improved activation experience

Friday, March 22, 2019

**New feature**

Azure Active Directory

[New alert on potential stale accounts in a privileged directory](#)

Home > Privileged Identity Management > Azure AD roles - Quick start

## Azure AD roles - Quick start

Kineticco

Overview

Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Roles
- Members
- Alerts
- Access reviews**
- Wizard
- Settings

Activity

## Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more

**Assign**

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

[Assign eligibility](#)

**Activate**

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

[Activate your role](#)

**Approve**

View and approve all act request for specific Azur roles that you are config approve

[Approve requests](#)

Home > Privileged Identity Management > Azure AD roles - Access reviews > Create an access review

### Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name \*  ✓

Description ⓘ

Start date \*  📅

Frequency  ⚙️

Duration (in days) ⓘ

End ⓘ

Number of times \*

End date \*

Users

Scope ☒ Everyone

One time

One time

Weekly


Monthly



Quarterly


Semi-annually

Annually


## Create an access review

Frequency Quarterly 

Duration (in days)   25

End  Never End by Occurrences

Number of times \* 0

End date \* 11/29/2019 

Users

Scope ☒ Everyone


---

\*Review role membership >

Select privileged role(s)

---

Reviewers

Reviewers Selected users 

---

\*Select reviewers >

Start



Home > Privileged Identity Management > Azure AD roles - Access reviews > Create an access review

### Create an access review

Frequency: Quarterly

Duration (in days): 25

End: Never End by Occurrences

Number of times: 0

End date: 11/29/2019

Users Scope: Everyone

\*Review role membership  
Select privileged role(s)

Reviewers  
Reviewers: Selected users

\*Select reviewers

Start

### Review membership

- ☐ Directory Readers
- ☐ Directory Writers
- ☐ Exchange Administrator
- ☐ External Identity Provider Administrator
- ☒ Global Administrator
- ☐ Global reader
- ☐ Guest Inviter
- ☐ HelpDesk Administrator
- ☐ Information Protection Administrator
- ☐ Intune Service Administrator
- ☐ Kaizala Administrator

Select

Pick all the roles you want to review.

\*Review role membership  
Billing Administrator and 1 other

Reviewers  
Reviewers: Members (self)

Upon completion settings

Advanced settings

Start



Home > Privileged Identity Management > Azure AD roles - Access reviews

### Azure AD roles - Access reviews

Kineteco

Overview

Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Roles
- Members
- Alerts
- Access reviews**
- Wizard
- Settings

New Filter Group Settings

Access reviews for Azure AD directory roles

Search

ROLE	OWNER	START DATE	END DATE	STATUS
<b>Privileged Access Review</b>				
Billing Administrator	Pete Zenger admin@kineteco.us	10/31/2019	11/29/2019	Initializing
Global Administrator	Pete Zenger admin@kineteco.us	10/31/2019	11/29/2019	Initializing
<b>Billing Administrator</b>				
Billing Administrator	Pete Zenger admin@kineteco.us	10/30/2019	11/6/2019	Active

# Recommendation

Walk through the steps of PIM access review to learn the configuration options.

## 3.6 Quiz

Question 1 of 5

You can configure access reviews in Privileged Identity Management to be self-completed by the eligible members of the privileged roles.

☒ TRUE  
Correct

Yes, you can assign designated reviewers, owners, or eligible role members.

☐ FALSE

Question 2 of 5

You can activate an eligible privileged identity profile \_\_\_\_\_.

☐ in the properties of your Office 365 user profile

☒ via the Azure Privileged Identity app in the Azure portal.

**Correct**

This is correct. Activating a profile is performed within the Azure AD PIM app in the Azure portal.

☐ all of these answers

☐ via the Microsoft Authenticator App

Question 3 of 5

Azure AD Privileged Identity Management (PIM) supports which of the following features when users request to activate a privileged identity profile?

☒ all of these answers

**Correct**

Azure AD Privileged Identity Management supports all three of these options, alone or in any combination.

☐ an explanation of why they need to activate

☐ approval by an admin

☐ a ticket number in ServiceNow

[Next question](#)

Question 4 of 5

Microsoft Azure AD Identity Protection evaluates risk associated with

☒ users and sign-ins

**Correct**

Azure AD Identity Protection evaluates risk associated to users and sign-in attempts.

☐ users

☐ users and devices

☒ users, sign-ins, and devices.

**Incorrect**

Azure AD Identity Protection does not evaluate devices.

Question 5 of 5

You can configure access reviews in Privileged Identity Management to be self-completed by the eligible members of the privileged roles

☐ FALSE

☒ TRUE

**Correct**

Yes, you can assign designated reviewers, owners, or eligible role members.

## References

<https://www.linkedin.com/learning/instructors/pete-zerger?u=86261762>