



Microsoft Azure Administrator Associate Training

Secure Identities



Agenda



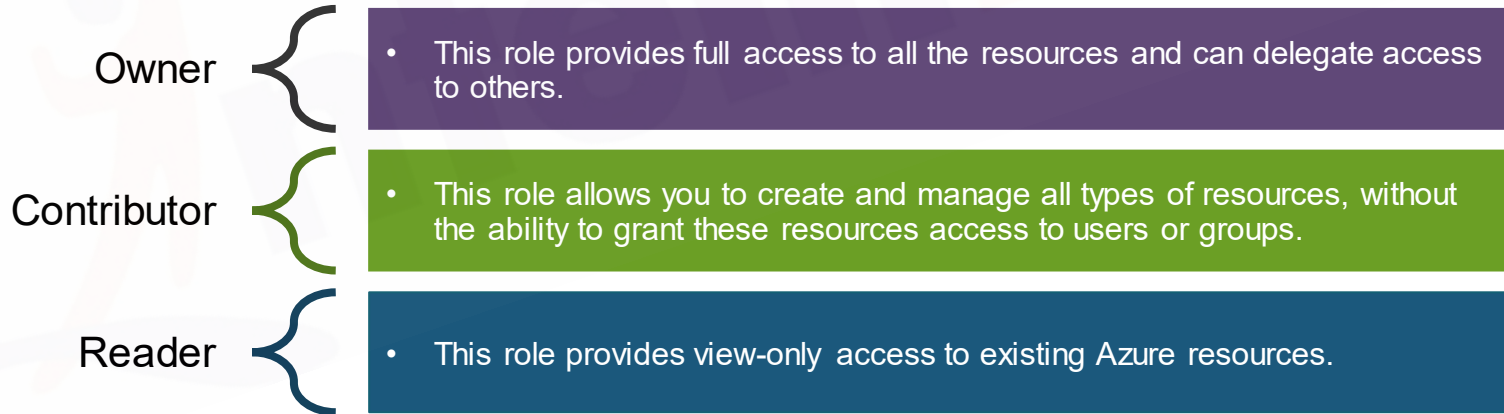
- ☐ Manage role based access control (RBAC)
- ☐ Multi-factor authentication (MFA)
- ☐ Directory Synchronization
- ☐ Implement Azure Active Directory (AD) Privileged Identity Management (PIM)
- ☐ Hands-On Lab

Manage Role Based Access Control (RBAC)

Manage Role Based Access Control (RBAC)



- ❑ RBAC enables fine-grained access management for resources that exist in an Azure subscription.
- ❑ By using RBAC, you can implement delegated management of cloud resources.
- ❑ For example, you can allow your development team to create their own virtual machines, but limit virtual networks to which those machines can be connected.
- ❑ RBAC has three basic built-in roles that apply to all resource types:



Multi-Factor Authentication (MFA)

- ❑ Azure Multi-Factor Authentication adds an additional security layer in the authentication process by requiring more than one method of authentication to identify user identity.
- ❑ Usernames and passwords are still required to sign in to access data and applications, but an additional access method can be added as a second factor of authentication.
- ❑ Multi-factor authentication combines something that you know, such as a password or a PIN.



- You can authenticate via a phone call.
- You can authenticate via a text message.
- You can authenticate using a third-party OAuth token.

Directory Synchronization



Directory synchronization involves copying selected user, group, contact between on-premises Active Directory and Azure AD.

In its simplest form, you install a directory synchronization component on a server with direct connectivity to your AD DS domain controllers.

After the initial synchronization completes, objects representing all on-premises user accounts, groups, contacts that are not built-in from AD DS will then automatically appear in Azure AD.

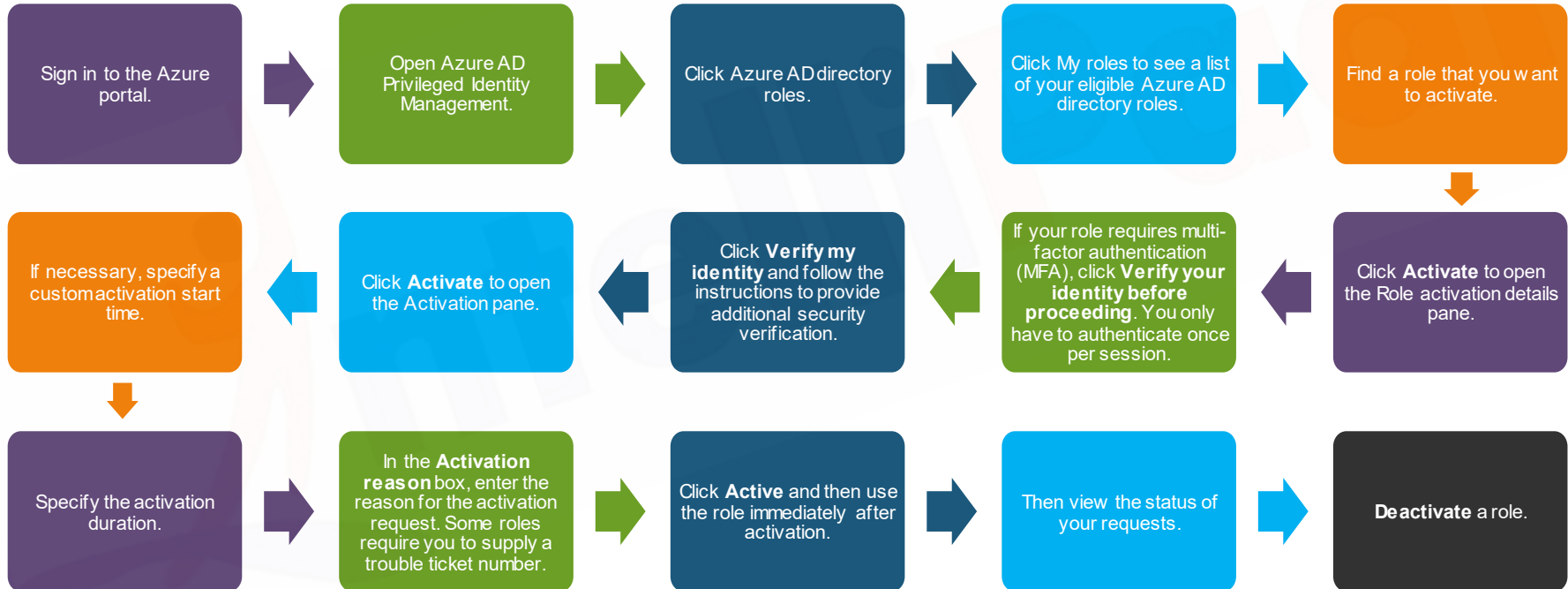
This way, AD DS users can authenticate and access Azure resources by using the same credentials as those they use to sign in to their on-premises computers.

Implement Azure Active Directory (AD) & Privileged Identity Management (PIM)

Activate Azure AD directory roles in PIM



To Activate a role



Assign Azure resource roles in PIM



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

•Owner

User Access
Administrator

Contributor

Security Admin

Security Manager, and
more

Assign Azure resource roles in PIM



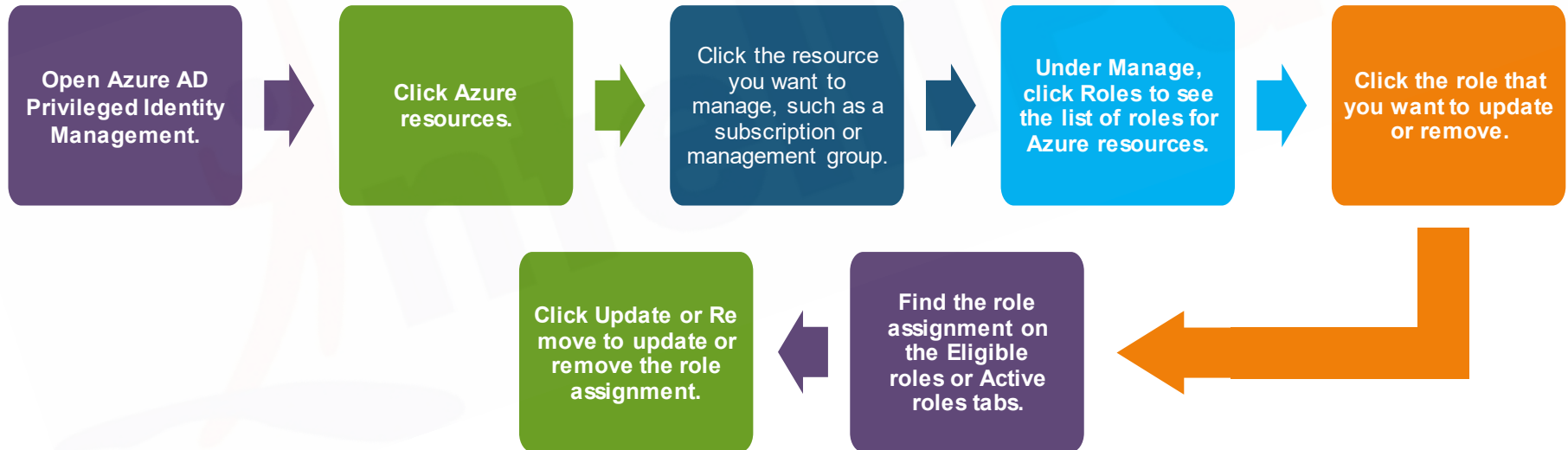
To Assign a role, follow these steps to make a user eligible for an Azure resource role:



Assign Azure resource roles in PIM continued....



To update or remove an existing role assignment, Follow these steps to update or remove an existing role assignment.



Approve/Deny requests for Azure AD directory roles in PIM



Microsoft Azure

Search resources, services, and docs

Home > Privileged Identity Management > Azure AD directory roles - Approve requests

Privileged Identity Management

Azure AD directory roles - Approve requests

default directory

Quick start

TASKS

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

MANAGE

- Azure AD directory roles
- Azure resources

Overview

Quick start

TASKS

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

MANAGE

- Roles
- Members

Approve Deny Refresh

ROLE	REQUESTOR	REASON
Application Administrator	Isabe... isabe...	Configure a n
Security Reader	Ann ... ann...	Review securi

Approve/Deny requests for Azure AD directory roles in PIM



Approve Requests

1. Select the requests you want to approve and then click **Approve** to open the Approve selected requests pane.

1. In the **Approve reason** box, type a reason.

1. Click **Approve**.

A screenshot of the 'Approve requests' pane in the Azure AD PIM console. The pane has a dark header with a star icon. Below the header, there are three buttons: 'Approve' (checked), 'Deny', and 'Refresh'. The main area contains a table with columns: ROLE, REQUESTOR, REASON, START TIME, and END TIME. The first row shows 'Application Administrator' requested by 'Isabe...' for 'Configure a new appli...'. The second row, which is highlighted in light blue, shows 'Security Reader' requested by 'Ann ...' for 'Review security reports'. A red box highlights the 'Approve' button in the top left of the pane.

ROLE	REQUESTOR	REASON	START TIME	END TIME
Application Administrator...	Isabe... isabe...	Configure a new appli...	8/29/2018,...	8/29/2018,...
<input checked="" type="checkbox"/> Security Reader	Ann ... ann...	Review security reports	Upon appr...	4 hours aft...

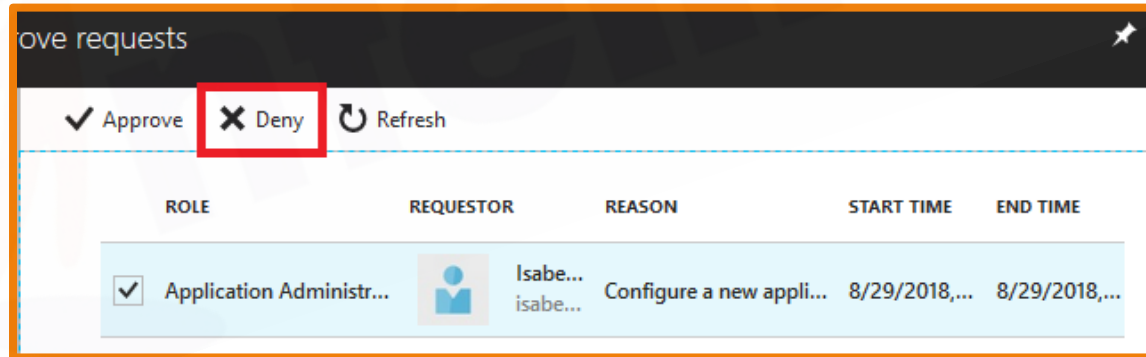
Approve/Deny requests for Azure AD directory roles in PIM

Deny Requests

1. Select the requests you want to deny and then click Deny to open the Deny selected requests pane.


1. In the Deny reason box, type a reason.

1. Click **Deny**.



Approve requests

✓ Approve **✗ Deny** ↻ Refresh

ROLE	REQUESTOR	REASON	START TIME	END TIME
<input checked="" type="checkbox"/> Application Administr...	 Isabe... isabe...	Configure a new appli...	8/29/2018,...	8/29/2018,...

Little Glance to PIM



To start using PIM in your directory, you must first enable PIM.

Sign in to the Azure portal as a **Global Administrator** of your directory.

Click **All services** and find the **Azure AD Privileged Identity Management service**.

Click to **open** the PIM QuickStart.

In the list, click **Consent** to PIM.

Click **Verify** my identity to verify your identity with Azure MFA. You'll be asked to pick an account.

Once you have completed the verification process, click the **Consent button**.

In the message that appears, click **Yes** to consent to the PIM service.

Sign up PIM for Azure AD roles

1. Open **Azure AD Privileged Identity Management**. Click **Azure AD roles**.

Click **Sign up**. In the message that appears, click **Yes** to sign up PIM to manage Azure AD roles.

Navigate to your tasks.

Add a PIM tile to the dashboard.

1. Sign in to the Azure portal. Click **All services** and find the **Azure AD Privileged Identity Management service**.

Click to open the PIM QuickStart. Check **Pin blade to dashboard** to pin the PIM QuickStart blade to the dashboard.

Hands-On

Hands-On

- ☐ Configure Azure AD
- ☐ Create user in Azure AD
- ☐ Login via Azure AD
- ☐ Enable MFA



Quiz 1

RBAC is _____?

- A** Role based authorization and configuration
- B** Role based authorization and controlling
- C** Retention based access control
- D** Role based access control



Answer 1

RBAC is _____?

- A** Role based authorization and configuration
- B** Role based authorization and controlling
- C** Retention based access control
- D** Role based access control



Quiz 2

Basic built-in roles that apply to all resources types?

- A Owner
- B Contributor
- C Reader
- D All of the above



Answer 2

Basic built-in roles that apply to all resources types?

A

Owner

B

Contributor

C

Reader

D

All of the above



Quiz 3

Which statement is correct about Multi-factor authentication (MFA)?

A

MFA removes the additional security layer in the authentication by enabling only one method of authentication to identify user's identity

B

MFA adds an additional security layer in the authentication by enabling more than one method of authentication to identify user's identity

C

MFA keeps the same security layer in the authentication and enhances its security by enabling more only one method of authentication to identify user's identity

D

All of the above



Answer 3

Which statement is correct about Multi-factor authentication (MFA)?

A

MFA removes the additional security layer in the authentication by enabling only one method of authentication to identify user's identity

B

MFA adds an additional security layer in the authentication by enabling more than one method of authentication to identify user's identity

C

MFA keeps the same security layer in the authentication and enhances its security by enabling more only one method of authentication to identify user's identity

D

All of the above



Quiz 4

Directory Synchronization involves copying?

- A** User
- B** Group
- C** Contact
- D** All of the above



Answer 4

Directory Synchronization involves copying?

A

User

B

Group

C

Contact

D

All of the above



Quiz 5

Which one of them are the important roles in PIM?

A

Owner

B

User Access Administrator

C

Contributor

D

All of the above



Answer 5

Which one of them are the important roles in PIM?

A

Owner

B

User Access Administrator

C

Contributor

D

All of the above





India : +91-7847955955

US : 1-800-216-8930 (TOLL FREE)



sales@intellipaate.com



24X7 Chat with our Course Advisor