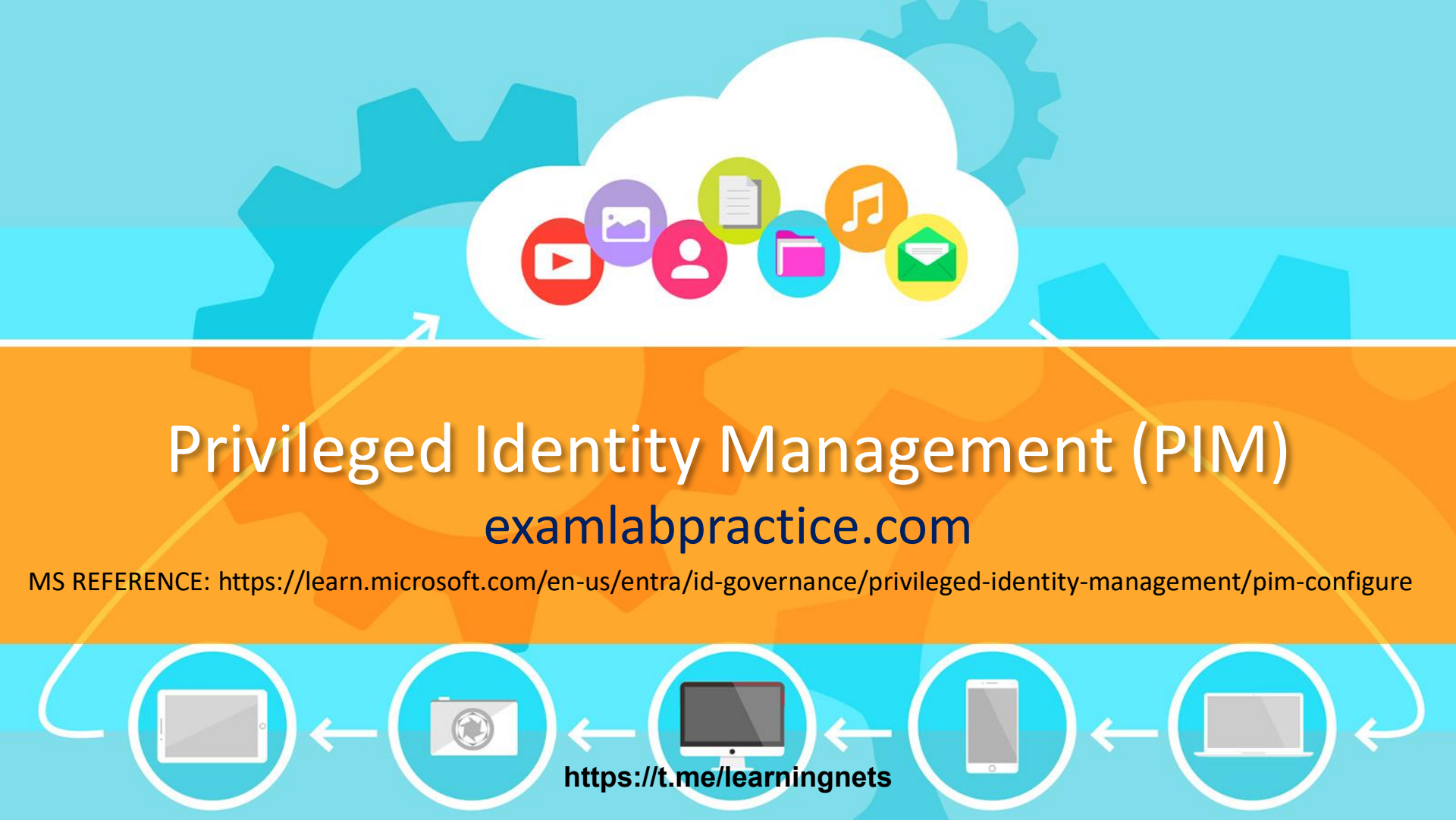

Privileged Identity Management (PIM)

examlabpractice.com

MS REFERENCE: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

What is PIM?

Privileged Identity Management (PIM) is a technology that allows you to manage, control, and monitor access to resources in your organization. These resources include resources in Microsoft Entra ID (formerly Azure AD), Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Licensing Privileged Identity Management

The following licenses will provide PIM in your organizations:

- Microsoft Entra ID P2
- Microsoft Entra ID Governance

MORE INFO: https://learn.microsoft.com/en-us/entra/id-governance/licensing-fundamentals

Key Features of PIM

- Set up **just-in-time** privileged access to Entra ID and Azure resources
- Create **time-bound** access to resources using start and end dates
- Enforce **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate a role
- Utilize **justification** to understand why users activate
- Receive **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit

Roles Required for Managing PIM

- Only a user who has the Privileged role administrator or Global administrator role can manage assignments for other administrators.
- You can grant access to other administrators to manage Privileged Identity Management.
- Global Administrators, Security Administrators, Global readers, and Security Readers can also view assignments to roles in Privileged Identity Management.

Terminology

Term or concept	Role assignment category	Description
eligible	Type	A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.
active	Type	A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role.
activate		The process of performing one or more actions to use a role that a user is eligible for. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
assigned	State	A user that has an active role assignment.
activated	State	A user that has an eligible role assignment, performed the actions to activate the role, and is now active. Once activated, the user can use the role for a preconfigured period-of-time before they need to activate again.

Terminology

Term or concept	Role assignment category	Description
permanent eligible	Duration	A role assignment where a user is always eligible to activate the role.
permanent active	Duration	A role assignment where a user can always use the role without performing any actions.
expire eligible	Duration	A role assignment where a user is eligible to activate the role within a specified start and end date.
expire active	Duration	A role assignment where a user can use the role without performing any actions within a specified start and end date.
just-in-time (JIT) access		A model in which users receive temporary permissions to perform privileged tasks, which prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it.
principle of least privilege access		A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform. This practice minimizes the number of Global Administrators and instead uses specific administrator roles for certain scenarios