Microsoft

Swiss Post
Cybersecurity

Introduction to Microsoft Entra

Microsoft
Solutions Partner

Security

Specialist
Threat Protection

Learning path agenda

- Describe the function and identity types of Microsoft Entra ID.

- Describe the authentication capabilities of Microsoft Entra ID.

- Describe the access management capabilities of Microsoft Entra.

- Describe the identity protection and governance capabilities of Microsoft Entra.

LAB Setup

- **Connect to XtremLabs**
- **Add you Codes to intiate the Labs**

https://tinyurl.com/Azurewien

Launch the Lab environment

Lab to do:

- [SC-900T00-A-CEP-L0] Lab setup
- [SC-900T00-A-CEP-L01] Explore Microsoft Entra ID User Settings
- [SC-900T00-A-CEP-L03] Microsoft Entra Conditional Access
- [SC-900T00-A-CEP-L04] Explore Privileged Identity management.
- [SC-900T00-A-CEP-L05] Explore Azure Network Security Groups (NSGs)

Lab Title: [SC-900T00-A-CEP-L0] Lab setup
Duration: 120 minutes
Status :   Not Initiated

Take Lab
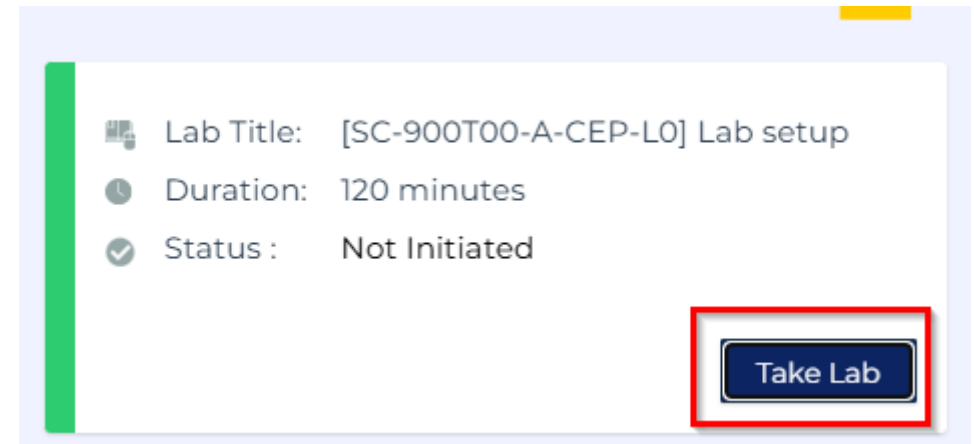
Learning path summary
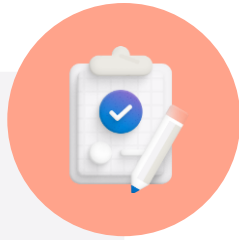
Describe the capabilities of Microsoft Entra.

In this learning path, you have:

- Learned about Microsoft Entra ID and the services and identity types it supports.

- Explored the authentication capabilities of Microsoft Entra and MFA.

- Explored the access management capabilities of Microsoft Entra, with Conditional Access and Microsoft Entra RBAC.

- Described identity protection and governance capabilities of Microsoft Entra, including PIM and access reviews.

- Learned about the capabilities of Microsoft Entra Identity Protection.

Knowledge check

An organization has completed a full migration to the cloud and has purchased devices for all its employees. All employees sign in to the device through an organizational account configured in Microsoft Entra ID. Select the option that best describes how these devices are set up in Microsoft Entra ID.

A. These devices are set up as Microsoft Entra ID registered.
B. These devices are set up as Microsoft Entra ID joined.
C. These devices are set up as Hybrid Microsoft Entra ID joined.

After hearing of a breach at a competitor, the security team wants to improve identity security within their organization. What should they implement to provide the greatest protection to user identities?

A. Multifactor authentication.
B. Require security questions for all sign-ins.
C. Require strong passwords for all identities.

Knowledge check continued

An organization plans to implement Conditional Access. What do admins need to do?

A. Create policies that enforce organizational rules.
B. Check that all users have multi-factor authentication enabled.
C. Amend your apps to allow Conditional Access.

An organization has recently conducted a security audit and found that four people who have left were still active and assigned global admin roles. The users have now been deleted but the IT organization has been asked to recommend a solution to prevent a similar security lapse happening in future. Which solution should they recommend?

A. Entitlement management.
B. Identity Protection.
C. Privileged Identity Management.