

Episode Title: Implement and manage Microsoft Defender for Identity

Objectives:

At the end of this episode, I will be able to:

1. Understand licensing requirements for Defender for Identity
2. Deploy the sensor to domain controllers
3. Configure monitoring and alert policies for threats

Key Points:

Key Point 1

Defender for Identity requires an E5 license type, either Microsoft 365 E5 or the Enterprise Mobility + Security E5 suite.

Key Point 2

The sensor that is used with Defender for Identity should be installed on all Domain Controller and Active Directory Federation Services computers in the domain.

Key Point 3

You can create custom policies based on sensitivity levels for authentication that occurs in the domain.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- What is Microsoft Defender for Identity?
: <https://learn.microsoft.com/en-us/defender-for-identity/what-is>