

Episode Title: Configure and manage Windows Defender Credential Guard and SmartScreen

Objectives:

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

1. Define Windows Defender Credential Guard
2. Deploy Credential Guard using Group Policy
3. Explain SmartScreen

Key Points:

Key Point 1

Credential Guard isolates the credentials in a separate memory space on the machine to prevent credential theft. It requires Secure Boot to be enabled and is not recommended on Domain Controllers.

Key Point 2

SmartScreen identifies potentially malicious websites and downloads. It will block access or prevent the app from running if detected.

Key Point 3

The Protected Users group is a built-in Active Directory group. Adding a user account to the group disabled NTLM authentication and limits Kerberos tickets to 4 hours.

- 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:

- Configure Credential Guard
: <https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/configure>
- Protected Users security group
: <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group>