



# Identity Services

Enterprise Single Sign-On  
Platform SSO



# Introduction to Identity Services

Lecture



# Kerberos SSO

- ✦ Extensible single sign-on extension via MDM.
- ✦ Support for on-prem Windows Active Directory domain services.
- ✦ Does NOT support cloud-based authentication (Entra ID).
- ✦ Devices must have network access via LAN or VPN to the domain controller.
- ✦ Acquires a TGT from Active Directory and then uses that to sign into websites, apps, file servers, etc.



# Enterprise SSO

- ✦ Modern authentication using web-based protocols like SAML 2.0, OAuth 2.0, and Open ID Connect.
- ✦ Supports multi-factor authentication.
- ✦ Configuration is done via MDM payload.
- ✦ Apps and devices that support Kerberos SSO work with Enterprise SSO.
- ✦ Devices can use a combination of authentication methods depending on resources and network topology.



# Platform SSO

- Next generation single sign-on for Mac. Requires macOS 13 or later. Still technically in beta.
- Payload for configuring Platform SSO requires an MDM.
- Extends the Mac login window functionality to your Identity Provider.
  - Keeps local and IdP account in sync.
  - Allows for authentication to the Mac using cloud hosted IdP like Microsoft Entra ID.
  - Provides support for password-less authentication.



# Kerberos Single Sign-On

Practical Exercise



# Enterprise Single Sign-On

Practical Exercise



# Platform SSO

Practical Exercise