Digital Workspace | Cloud-Managed Windows Endpoints

IMPLEMENTATION DELIVERABLES

- Microsoft Endpoint Management & Security Build Intent Workshop Delivery
- Deploy Cloud Kerberos Trust
- Deploy Intune Certificate Connector/NDES/SCEP
- Configure Windows Autopilot for Entra ID joined devices
- Configure Microsoft Intune for Windows device management
- Review Intune Group Policy Analytics tool
- Deploy Windows 10/11 Security Baseline
- Deploy three Windows Applications
- Configure Windows Device Compliance Policy
- Configure Windows Update for Business or Windows Autopatch
- Deploy up to ten pilot Entra ID joined Windows devices via Windows Autopilot/Intune

ASSUMPTIONS

- User identities are already being synchronized from an existing on-premises Windows Server Active Directory to Microsoft Entra ID.
- Microsoft Entra ID is not federated with another identity provider for authentication.
- All Windows Server Active Directory Domain Controllers are running either:
    - Windows Server 2016 with KB3534307 installed
    - Windows Server 2019 with KB4534321 installed
    - Windows Server 2022
- All pilot users are licensed for at least Microsoft Intune and Entra ID Premium Plan 1 or higher.
- Customer has an existing, functional Microsoft certificate authority deployed if certificate distribution to Entra ID joined clients is required.
- The User Principal Name (UPN) assigned to users in Windows Server Active Directory must be routable.
- Users that are direct or indirect members of privileged built-in security groups in Windows Server Active Directory won't be able to use cloud Kerberos trust and Windows Hello for Business.

NON-DELIVERABLES

- Any remediations to the Customers Windows Server Active Directory or Entra ID environment to meet pre-requisites requirements.
- MacOS, Android, iOS, iPadOS device management is not in-scope.
- Direct end user support. CDI will provide tier-3 support to the Customers IT staff only.
- Enrollment of pilot user devices via Windows Hello for Business and Microsoft Intune.
- Migration of group policy settings to device configuration profiles in Microsoft Intune.
- Manual enrollment of corporate owned Windows 10/11 devices in Windows Autopilot service.
- Additional configuration of Microsoft Intune or Active Directory group policy beyond what's necessary for deploying Windows Hello for Business for pilot devices.
- Production deployment to users/devices beyond the pilot user scope (maximum 20 users).
- Integration, configuration, or deployment of Microsoft Defender for Endpoint.