CDI

an AHEAD Company

Digital Workspace | Passwordless Authentication

IMPLEMENTATION DELIVERABLES

- Verify all pre-requisites are in place for implementation of Windows Hello for Business
- Define Customers Windows Hello for Business/FIDO2 Authentication Policy
- If applicable, Plan FIDO2 Security Key Lifecycle
- Configure Hybrid-Joined Windows Clients (Pilot Group)
- Implement Cloud Kerberos Trust for Windows Server Active Directory
- If applicable, Enable FIDO2 Security Key Authentication in Microsoft Entra ID
- Prepare Pilot Users for Windows Hello for Business/FIDO2 login
- If applicable, Enable Support for FIDO2 Security Keys on Windows 10 clients (up to twenty devices)
- Deploy Windows Hello for Business Policies to the Pilot Group (Up to twenty users)
- Modify Windows Hello for Business Policies/Settings based on Feedback
- Review Next Steps and Perform Final Knowledge Transfer

ASSUMPTIONS

- 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
- Windows 10/11 Client Requirements:
    - All Windows 10 clients are running Windows 10 version 21H2 or later with KB5010415
    - All Windows 11 clients are running Windows 11 version 21H2 or later with KB5010414
    - All Windows 10/11 clients all have a Trusted Platform Module (TPM) version 2.0 or later
    - Windows 10/11 endpoints enabled for Windows Hello for Business/FIDO2 logon will be physical devices and not virtualized. Remote Desktop Protocol (RDP), virtual desktop infrastructure (VDI), and Citrix scenarios will not be supported.
    - Windows 10/11 endpoints enabled for Windows Hello for Business/FIDO2 logon will either be joined to Windows Server Active Directory or Microsoft Entra ID joined clients managed by a modern device management solution capable of deploying configuration service provider (CSP) profiles.
- Customer is not using Microsoft Active Directory Federated Services for authentication to Microsoft Entra ID
- 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.
- Customer does not have an existing key trust or certificate trust deployment configured with Microsoft Entra ID.

NON-DELIVERABLES

- Direct end user support. CDI will provide tier-3 support to the Customers IT staff only.
- Enrollment of devices in any device management solutions such as Microsoft Intune
- 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).