Desired Outcomes

- UW NetIDs & UW Groups are available for use with Microsoft technology
- I can share data using Microsoft-based services
- My application can be integrated with Microsoft technology
- My unit can easily manage its Windows devices
- Access to Microsoft technologies can be provisioned or deprovisioned when needed
- Data in Microsoft technologies is secure
- I can use cloud technologies that require Microsoft infrastructure
- A unit doesn’t need its own AD or Azure AD

Stakeholder Goals

- Authentication & Credential Mgmt
- Collaboration & Application Mgmt
- Device Mgmt
- Information Security
- Enable Cloud

Core Capabilities

- Active Directory services
- Azure AD services
- Credential Mgmt - Microsoft Authentication - Multi-factor Authentication
- App Integration & Mgmt - Software Deployment - Microsoft License Mgmt
- Device Integration - Device Mgmt - Device Name Registration & Resolution
- Provisioning - Authorization - Data Protection - Auditing
- Azure AD Connect NETID Hybrid Join Azure AD External Users (Federation, B2B & Guests) Hybrid Cloud

Future Initiatives

- Strong AuthN for Windows (PRJ1408099)
- Azure MFA replaces Duo
- Expanded Azure AD app integration documentation
- UW Shibboleth proxies authentication to Azure AD
- UW Shibboleth replaced with UW Azure AD
- Supervisor data in NETID AD and Azure AD
- Azure AD Guest lifecycle - Privileged Identity Mgmt (PIM) - Renewed inactive user lifecycle - Expanded use of Azure AD Access Reviews
- Improved guidance and practices for Azure AD tenants

Future Outcomes

- Windows Hello for Business
- FIDO2 token authentication
- Use of Azure MFA for ‘UW 2FA for the Web’
- UW saves ~$170K annually not duplicatively paying for two MFA products; simplification for many users
- Customers can self-service integrate their applications more easily
- Unified UW web sign in experience
- All enterprise web apps gain risk-based and fraud detection security capabilities; web app integration capabilities are modernized & UW-IT saves ~$80K annually not supporting a custom IdP
- Workflows and business processes requiring supervisor are enabled
- Unredeemed guest invites are deleted
- Guest deletion after 1y of inactivity
- Automated loss of privileges for users with Azure AD roles with lack of use
- NETID AD and Azure AD users who are inactive are disabled and deleted
- Automated of loss of entitlements for resources whose access is tied to an Azure AD group; this moves us past custom category & subscription system for automated deprovisioning of access
- Cost savings, operational excellence, and regulatory alignment

Key

*italics*
Future possibility, no solid plans yet