

Initiatives

Service Features

Core Capabilities

Stakeholder Goals

Desired Outcomes

- A department does not need to run its own AD or Azure AD.
- I can share data using Microsoft-based services.
- I can provide Microsoft-based services.
- UW NetIDs are available for use with Microsoft technology.
- UW Groups are available for use with Microsoft technology.
- I can easily manage my devices.
- I can use cloud based technologies that require Microsoft infrastructure.
- Data in Microsoft technologies is secure.

Authentication & Credential Mgmt

Collaboration & Application Mgmt

Device Mgmt

Information Security

Enable Cloud

Windows Domain Services
Azure AD Services

Credential Mgmt
Windows Authentication
Federated Authentication
2 Factor Authentication

App Integration & Mgmt
Software Deployment
Microsoft License Mgmt

Device Integration
Device Mgmt
Device Name Registration & Resolution

Authorization
Data Protection
Auditing

Cloud Based Infrastructure
Hybrid Cloud

NETID Active Directory
UW Azure AD

AD gMSAs
NETID AD Kerberos & NTLMv2
NETID AD Trusts
UW AAD OIDC & SAML
UW AAD 2FA (Duo, Azure MFA)

AAD Applications
Campus KMS
AAD group-based licensing

AD computer join
AAD device registration
Delegated OUs
Domain-based DFS
LAPS & Bitlocker
AD Certificate Services
clients.uw.edu DDNS

AAD Conditional Access
UW Groups integration
AAD OAuth2 services
Microsoft Information Protection
MS Defender for Identity

AAD Connect
NETID Hybrid join
AAD B2B
Microsoft Graph

AuthN & Credential Mgmt
FY21 - Unfederate AAD
FY22 - ADFS retirement
FY22 - Inactive User Refactor

Information Security
FY22 - UW Groups integration refactor
FY22 - Administrative Units (basic)
FY23 - PIM and PAM for admins
FY23 - Azure Info Protection Expansion

FY21 - NETID DCs via Azure VNET