Managing user identities and secure access at Microsoft

Managing identities and network access at Microsoft encompasses all the processes and tools used throughout the identity life cycle for employees, supplier staff, and partners. As a cloud-first company, Core Services Engineering and Operations (CSEO) uses features in the Microsoft Enterprise Mobility + Security suite, powered by Microsoft Azure, along with on-premises identity and access management solutions to enable our users to be securely productive, from anywhere.

Microsoft is on a multi-year journey of transforming into a truly cloud-first, mobile-first enterprise. Though we operate in a hybrid cloud environment today, we’re moving on-premises identity technologies to the cloud, giving employees the flexibility they need. Plus, application owners can use the power of Microsoft Graph to effectively manage access to applications and resources.

Unifying the environment

To enable a single user identity for authentication and offer a unified experience, we integrated on-premises Windows Server Active Directory forests with Azure Active Directory (Azure AD). Our geographically distributed Active Directory environment uses Windows Server 2016. We use Azure AD Connect and Active Directory Federation Services (AD FS) when an Azure-based application needs user attributes—for example, their location, organization, or job title. User information is available if the service has the right permissions to query for those attributes.

As shown in Figure 1, our identity and access environment is hybrid, federated, and cloud-synched.

Figure 1. A high-level overview of the Microsoft identity and access environment

The Microsoft identity environment includes:

- 131,300 employees
- 303,000 global identities
- 488,000 partner identities
- 10,400 privileged identities that have some level of elevated access
- 15 million authentication requests per month
- 1.6 million cloud applications—99 percent of our apps—using Azure Active Directory (Azure AD)
- 3,000 applications using Active Directory Federation Services (AD FS)

Azure AD Connect

Azure AD Connect integrates on-premises directories with Azure AD. It gives users a single identity in Office 365, Azure, and software as a service (SaaS) applications that are integrated with Azure AD. Azure AD Connect consists of three main components:

- **Synchronization services.** Azure AD Connect sync services creates users, groups, and other objects. It makes sure that the on-premises identity for users and groups matches the cloud identity.
- **AD Federation Services.** Federation is an optional part of Azure AD Connect that’s used to configure hybrid environments using an on-premises AD FS infrastructure. It supports single sign-on and enforces Active Directory sign-on policy with smart card or third-party, multifactor authentication.
- **Health Monitoring.** Azure AD Connect Health offers a central location in the Azure portal to monitor system health.

Enabling identity models in Office 365

Microsoft Office 365 supports three identity models that support a variety of identity scenarios. Depending on how you manage identities, you can use a cloud identity model, federated identity model, or the synchronized identity model.

We use the federated model where we synchronize on-premises directory objects with Office 365 and manage our users on-premises. The users have the same password on-premises and in the cloud, and they do not have to sign in again to use Office 365. The user password is verified by AD FS—the password hash doesn’t need to be synchronized to Azure AD, and the user doesn’t have to sign in again to use Office 365.

Enabling users

Every employee, supplier staff, or partner that needs access to the corporate network receives an email address to sign in to their primary account. That primary account is synced to Azure AD and gives the user access to corporate resources, Office 365, Microsoft SaaS, and corporate business unit and third-party SaaS and platform as a service (PaaS) applications (such as apps for expenses or travel).

Strong authentication

We require multifactor authentication to verify a user’s identity before giving them access to corporate resources when they’re not connected to the corporate network. People use multifactor authentication in a few ways, including certificate-backed virtual and physical smart cards, Windows Hello for Business with PIN or biometric sign in, and Azure Multi-Factor Authentication (MFA) that uses a phone or the Microsoft Authenticator app. On domain-joined devices that we manage, multifactor authentication has become almost transparent to users.

Currently, the use rate for each authentication method is approximately:

- Certificate-based using virtual or physical smart cards—21 percent.
- Windows Hello for Business—25 percent.
- Azure MFA using phone authentication or an authenticator app—54 percent.
Certificate-based
For many years, certificated-based physical and virtual smart cards were the main method of multifactor authentication. As the other options have been enabled, smart card use has been declining.

Windows Hello for Business
With the deployment of Windows 10, we enabled **Windows Hello for Business**, which can replace passwords with strong two-factor authentication that combines an enrolled device with a PIN or biometric (fingerprint or facial recognition) to sign in. Windows Hello was easily implemented within our existing identity infrastructure, by extending certificates to include the use of a PIN or biometrics as an enterprise credential; plus, it allows remote access. Users can sign in to their Microsoft account, an Active Directory account, or an Azure AD Premium account.

Azure MFA
Although Windows Hello has become the preferred method for our Windows 10 domain-joined devices, we support access using mobile platforms such as iOS and Android. Azure MFA is the best solution for securing our users and data on these platforms, and it integrates seamlessly with our existing AD FS infrastructure.

Enabling partner access
For Microsoft partners, we’ve started using [Microsoft Azure Active Directory business-to-business (B2B) collaboration](https://azure.microsoft.com/en-us/services/active-directory-b2b/). Azure AD B2B collaboration make it easier to enable single sign-on access to Microsoft extranet applications and collaboration spaces.

Invitation lists are created using manually exported lists in the form of comma-separated value (.csv) files. We’re working on automating the process to reduce the potential for error and increase our speed.

Enabling mobile access
As a cloud-first company, many of our corporate resources are in the cloud. People can use multifactor authentication to securely access their work from anywhere. To enable mobile access to on-premises resources, we use a couple of remote access solutions:

- We help ensure the security of cloud resources and remote access at Microsoft by validating who the user is through multifactor authentication.
- We check system health to ensure that the user accesses corporate resources on a device that’s managed through System Center Configuration Manager or Microsoft Intune, and that the device has all the latest updates installed.

We introduced Conditional Access in Windows 10 Anniversary Update. To help ensure that users sign in from a healthy device with strong authentication, we also configure device management policies for remote access.

Role and user attribute access roles
We’ve started to implement role-based and user attribute–based access. We created a couple of dynamic groups that set up parameters for variable access to resources based on device, location, and type of user. We’ve focused on large user categories—such as employees and supplier staff—but we’re working on adding more specific roles.

Self-service
Cloud services gave us the ability to introduce more self-service capabilities for identity and access management. These services have helped reduce manual administrative tasks and Helpdesk support calls for help with password and identity management changes.
• **Password management.** Microsoft employees can change their passwords using an internal, cloud-based, self-service password management solution. We integrated Azure MFA, including verification with a phone call or mobile app, as part of the process. Users are prompted to answer verification questions when they change a password. When users need to change their password, they do so without calling Helpdesk.

• **Security and distribution group management.** Tools like Office 365 Teams help users manage their teams without going through an administrator or Helpdesk to create and manage their groups. Group owners can set up access policies to user groups rather than individual.

• **Azure AD Join.** At Microsoft, we support bring your own device (BYOD) scenarios; many employees do part of their work on their personal device. In Windows 10, our users can add an Azure AD account, and their device will be enrolled in mobile device management through Microsoft Intune.

### Managing the service

To manage on-premises and cloud identity services and enable day-one productivity for new users, we use established processes for provisioning and deprovisioning user identities, and to monitor and audit account usage.

### User account life cycle management

User account life cycle management includes all processes for provisioning and deprovisioning user identities for both full-time employees (FTEs) and supplier staff. New identities are created in our accounts provisioning system and in Active Directory. After an account is created, user sync enables it in Azure AD. Account provisioning is the same for both FTE and supplier staff identities, but they are granted different levels of access. For example, by default, FTEs are granted remote access, but it’s granted for supplier staff only upon manager approval.

#### Provisioning

To provision an active user account:

1. A business manager or Human Resources employee submits a provisioning request, which includes information such as the legal name of the user, the domain, their physical location, and if they have an office number or are a mobile worker.

2. After the request is submitted, the data is consumed by SAP, which generates a unique employee ID number for each person. New employee data automatically goes through the SAP web service to the accounts provisioning service.

3. The accounts service receives the employee ID from the SAP web service, with an action to provision the user account. We create the user identity, alias, and a temporary password. We also create the mailbox where the mailbox object is stamped in Active Directory.

4. The user employee ID number and provisioned alias are provided as a key pair back to the SAP web service.
   - SAP publishes the data through an HC01 feed, which gives the user identity access to Human Resources productivity sites, including finance and benefits.
   - In parallel, the accounts service sends account details (alias, temporary password, and mailbox) to the manager, sponsors, and other designated recipients identified in the original provisioning request.

#### Deprovisioning

When we receive a deprovisioning request from a business manager or Human Resources, we terminate and disable the user account from corporate access, including alternate and elevated access credentials. We reset the user’s network password and disable remote access, Office Web Access, and Skype for Business.
Automating our processes
Since August 2016, we’ve automated our core service scenarios to help ensure an active user account is provisioned before an employee’s start date, so employees will be productive on their first day. This includes provisioning scenarios for new hires, rehires, new supplier staff, and supplier staff to FTE conversions. We plan to automate additional post-provisioning activities, such as renaming aliases, domain moves, and remote access requests. We also plan to migrate the service to a third-party platform that will provide increased efficiency, integration, and provide more identity-related self-service capabilities.

Auditing and monitoring
Auditing identities is like other services—we collect event types in our central log management system. For monitoring identity events, we coordinate with the engineering team to define use cases and the monitoring conditions that would alert us. Those correlated conditions could come from any of the different monitoring pipelines, including Microsoft Cloud App Security.

Network monitors and endpoint monitoring, like Windows Defender Advanced Threat Protection (ATP), feed in to our security and information event management (SIEM) solution. When we get an alert, the service operations team determines whether the alert is valid and if it needs to be opened for investigation. If we determine that it’s a real alert, we use the information in the SIEM and in the Defender ATP console to begin investigating. Depending on the severity of the alert, it could be escalated to the incident response team, the legal department, or even law enforcement.

To help us deal with the number of alerts, we use a third-party behavioral analytics tool that helps reduce event noise and helps us better identify real events.

Cloud-enabled protection
Our traditional approach was to protect all the assets on the corporate network. Because we’ve moved most of our assets to the cloud, we now focus on security at the user level. We do that by introducing better user and admin accountability with security and governance, including:

- Controlling access to resources.
- Requiring strong user authentication.
- Responding to advanced threats by monitoring for specific risk-based scenarios.
- Mitigating administrative risks.
- Governance of on-premises and cloud identities.

Using privileged identities to manage elevated access
Privileged identity management is an important part of a larger effort within CSEO to secure high-value corporate assets. Of the roughly 303,000 identities that we manage, approximately 10,000 on-premises and 400 Azure AD users need elevated access to data and services. We have other tools and a process for the subset of users that have administrative—or elevated—access to data and services at Microsoft.

One important way we protect elevated access accounts is through just in time (JIT) access. Rather than have separate credentials or a persistent admin session, JIT elevates access for a specific duration. Access expires at the end of that time.

We also protect elevated accounts by requiring on-premises admins to sign in on secure access workstations, and we plan to expand that requirement to cloud admins.
Best practices

As our identity and access management solution has evolved, we’ve discovered a few best practices, including:

- If your Human Resources systems are primarily on-premises, you can use a hybrid approach to create user identities in Active Directory and sync them to the cloud.
- Assess your environment honestly to determine how to best use the cloud to reduce complexity for on-premises process points. Migrating to the cloud offers an opportunity to reassess existing processes and identify ways that the cloud can make your identity infrastructure more efficient. The scalability of Azure solutions offer advantages that can help modernize processes and technology dependencies.
- Identity is the new security perimeter. Azure provide the ability through it’s security products to help protect those identities much more effectively than traditional network/datacenter monitoring.

Looking ahead

We’re exploring other changes to identity management, including eliminating time-bound password expiration by moving to a system where passwords stop working only when triggered by specific risks or user behaviors.

Beyond that, we look forward to a future where our identities are in the cloud and there are no passwords. Within the next few years, we hope to move to a purely cloud-based service model, rather than our current, cloud-enabled state. Windows Hello for Business was our first step toward a future where biometrics replace passwords.

Also, we’re deploying Azure Information Protection at Microsoft. Azure Information Protection integrates with cloud identities to help protect corporate data. We continually look for ways that we can be more efficient as we move to cloud-only solutions for identity and access management.

For more information

IT Showcase

microsoft.com/ITShowcase

No more passwords: the relentless commitment to creating a password-less world at Microsoft

Implementing strong user authentication with Windows Hello for Business

Active Directory and Azure Active Directory

Connect domain-joined devices to Azure AD for Windows 10 experiences

Azure AD Join on Windows 10 devices

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.