Using Azure Multi-Factor Authentication at Microsoft to enhance security

To address the increasing security risk of phishing emails and fake web pages that are designed to harvest user names and passwords, Microsoft IT accelerated the adoption of Azure Multi-Factor Authentication for all users at Microsoft. We already had multi-factor authentication for remote access and virtual private network (VPN), in the form of virtual and physical smart cards. But to improve security and better support mobile productivity, we needed an option that provided:

- Additional security for federated identities that are used to access on-premises resources and cloud-based services.
- Multi-factor authentication capability for approximately 190,000 users and over 300,000 mobile devices that are not set up to use smart cards, or when a user does not have their smart card.

Integrating on-premises identities

To enable a single user identity for authentication and a unified experience when accessing resources in the cloud and on-premises, we integrated our on-premises Active Directory forests with Azure Active Directory (Azure AD). Our geographically distributed Active Directory environment includes both Windows Server 2016 and Windows Server 2012 R2. We use Azure AD Connect and Active Directory Federation Services (AD FS), so when an Azure-based application needs user attributes—for example, their location, organization, or job title—that information is available as long as the service has the right permissions to query for those attributes.

Setting up Azure Multi-Factor Authentication

To further secure user identities, we enabled Azure Multi-Factor Authentication as an additional verification method that is sent to the user. Our verification options include a phone call or mobile app notification, and the user can select the preferred option at the time of enrollment. The user experience is based on the connectivity type, so when the user connects remotely they are prompted for a second verification. For critical services, we require multi-factor authentication for access, even for connections within the corporate network.

Enrolling users

For our sign-in experience, we have enabled signing in with mobile phone and signing in with mobile app notification. Our corporate policies required that the user identity be validated for enrollment. The enrollment process used a portal designed to enable users to validate their phone number automatically when they sign in with a smart card during registration. The identity of users without smart cards is validated using a workflow that requires their manager’s approval.

Customizing a user-friendly sign-in screen

We enabled Azure Multi-Factor Authentication in a phased manner, and gathered feedback from our early adopters through Yammer communities and from user support about the experience. Based on feedback, we chose to customize the AD FS sign-in page to create an intuitive and self-guided user experience before deploying to the rest of our users. Early feedback helped us improve the experience where additional clarity was needed to guide users, such as which sign-in option to select or which certificate to choose for authentication.

We were able to combine sign-in screens and update them to drive preferred user behavior. While our default option for the user is to sign in with a smart card, in cases where username and password was selected we achieved the strong authentication with Azure Multi-Factor Authentication. The interface is also updated to detect and display only valid authentication options. If a user is on a device that can only support phone or app verification, the user will not
see physical smart card as their primary option to sign in. The option to sign on with a username and password using phone verification as the second factor is available on the screen but is a smaller option that needs to be purposefully selected.

Figure 1. Customized sign-in screen

More self-help options are provided in the sign-in failure screen to guide users through the steps to resolve their issue. If none of the steps resolve the user’s issue, then they are given contact information for the global helpdesk.

Figure 2. Customized sign-on failure screen to help users troubleshoot their issue

Learn more about customizing AD FS sign-in pages at [Customizing the AD FS Sign-in Pages](#).
Additional scenarios

We enabled a few additional scenarios to help improve the experience for our users, reduce the amount of helpdesk calls, and improve the performance of the service.

Securing remote access

For remote access, our VPN infrastructure has long required a physical or virtual smart card to sign in securely. With the addition of Azure Multi-Factor Authentication, we can integrate with our existing VPN/RADIUS infrastructure and users can also use phone or mobile app verification to sign in. This includes making this option available within our Connection Manager—a component of Microsoft Windows Server-based VPN client. We were able to give users the choice of using their preferred strong authentication method for remote access. This has helped users gain remote access faster in locations where it takes a long time to get smart cards.

Changing passwords

Microsoft users can now change their passwords using an internal, cloud-based, self-service password management solution. We have integrated Azure Multi-Factor Authentication, including verification with a phone call or mobile app, as part of the process. Users are prompted to answer additional verification questions when they change a password. When users need to change their password, they can now do so without having to call the global helpdesk.

Enabling performance and high availability

Our Azure Multi-Factor Authentication servers are configured with Windows Server 2012 R2 AD FS. To provide high availability and redundancy, we do not direct authentication traffic to the primary Multi-Factor Authentication server. This helps ensure that the server can make updates without having performance issues.

Our distributed secondary Multi-Factor Authentication servers store a read-only copy of the Multi-Factor Authentication configuration database from the primary server. They connect to and synchronize data with the primary server, provide fault tolerance, and load balance access requests. Since Azure Multi-Factor Authentication Server is not running on the same servers as AD FS, we have installed the Multi-Factor Authentication adapter for AD FS locally on servers running AD FS. Each virtual adapter is configured for certificate authentication to the web service SDK on the Multi-Factor Authentication server.

For load balancing, we use a combination of DNS round robin and hardware. To learn more about steps to install Azure Multi-Factor Authentication Server see Getting started with the Azure Multi-Factor Authentication Server.

Monitoring service health

To monitor service health and performance, we developed a synthetic client flow through the Multi-Factor Authentication and AD FS infrastructures. We used a test account without any rights to live applications or resources on the corporate network to run synthetic transactions that tested the end-to-end client flow. Using a constant stream of synthetic transactions per day, we can quickly identify degradations in the service and get them fixed before users are affected. We use Azure AD Connect Health for detailed monitoring, reporting, and alerts for our AD FS servers. Azure AD Connect Health, a feature of Azure Active Directory Premium helps monitor and secure cloud and on-premises identity infrastructure. Using Azure AD Connect Health with AD FS has more information about Azure AD Connect Health.

We also use real-time metrics in Visual Studio Application Insights to analyze request load, server performance counters, and response times across dependencies. It helps us diagnose exceptions and failed requests, correlate them with events and traces, and get multi-dimensional analyses over standard metrics. Visual Studio Application Insights helps us determine the cause of any performance behavior through ad hoc queries. Learn more about how to detect, triage, and diagnose issues in your web apps and services with Visual Studio Application Insights.

www.microsoft.com/ITShowcase

June 2016
The fraud alert feature has been configured and set up so that our users can report fraudulent attempts when trying to access resources. When a fraudulent attempt is reported, we have the ability to investigate and take immediate action, such as locking out an account, which is included in our service reports.

We consolidated the text-based logging from the Multi-Factor Authentication servers into a single database, and the support team uses scripts to query against those reports. We also created Microsoft SQL Server Reporting Services reports for the support team to look at bigger issues.

Reporting provides a view into what kinds of issues are occurring and what can be done to provide a better user experience. Reports were used by service management to help them spot trends during the rollout. After the rollout, service managers monitored the user experience service health reports for telemetry about how many people were using the phone call for phone authentication, and how many people were using the mobile application. The service health report also lets service managers know how many users have authenticated on a given day and how the service is performing.

Conditional access control

We have the ability to provide conditional access to applications with AD FS rules. We can vary the granularity of how we enforce multi-factor authentication, at an application level. AD FS is flexible and allows us to designate people or groups that can access an application, and how they have to authenticate when they are on the corporate network or off. Most users that access applications on the corporate network are allowed single authentication, and applications that are accessed from the internet require multi-factor authentication. Some applications are so important that they require multi-factor authentication even when the user accesses them from the corporate network.

Upgrading to Windows Server 2016

Moving from AD FS on Windows Server 2012 R2 to AD FS on Windows Server 2016 has gotten much easier. Now you can simply add a new Windows Server 2016 server to a Windows Server 2012 R2 farm, and the farm will act at the Windows Server 2012 R2 farm behavior level, so it looks and behaves just like a Windows Server 2012 R2 farm. Then, add new Windows Server 2016 servers to the farm, verify the functionality and remove the older servers from the load balancer. Once all farm nodes are running Windows Server 2016, you are ready to upgrade the farm behavior level to 2016 and begin using the new features.

Best practices

- Improve manageability. Common reporting with other services and integration into a reporting dashboard provides an end-to-end view of all services.
- Focus on the user experience. This is particularly important when it comes to security initiatives and supporting broad adoption. Leadership and users can be resistant to change if there is a perception that new security measures may degrade the user experience.
- Use synthetic transactions to regularly test the performance of your Azure Multi-Factor Authentication environment. This will help identify any degradations in the service early enough to address them before users are affected.
- Create test accounts for synthetic transactions. By using accounts that do not have access to live applications or resources, you can help keep information secure while testing service performance of your environment.
- Communicate broadly about upcoming changes and make them as minimally intrusive as possible for users. User awareness and readiness is key to change management. We used a combination of social channels on Yammer, an email campaign, print collateral, posters, and digital signage.
For more information

Microsoft IT

Microsoft.com/ITShowcase

Microsoft Azure Multi-Factor Authentication

© 2016 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.