Azure Multi-Factor Authentication- Adoption Kit

Version: 2.0
For the latest version, please check https://aka.ms/aadadoptionkits

Contents

Awareness

This section helps you to analyze the benefits of Azure Active Directory (Azure AD) Multi-Factor Authentication. You will learn about the ease of use, pricing and licensing model, as well as customer stories about how it helped improve their business. You will also receive up-to-date announcements and access to blogs that discuss ongoing improvements.

Business Overview

> The following adoption kit is specific to Azure Multi-Factor Authentication and does not cover the Multi-Factor Authentication (MFA) server. For information on the MFA server, see Getting started with the Azure Multi-Factor

Azure AD Multi-Factor Authentication (MFA) helps safeguard access to data and applications while meeting user demand for a simple sign-on process. It delivers strong authentication via a range of easy verification options—phone call, text message, or mobile app notification and one-time passwords—allowing users to choose the method they prefer. It can be used both on-premises and in the cloud to add security for accessing Microsoft online services, Azure AD-connected SaaS applications, line of business applications, and remote access applications. Refer to What does Azure Multi-Factor Authentication mean for me?

Before you can decide where and how to deploy Azure MFA, you need to answer the following three basic questions:

- What am I trying to secure?
- Where are the users located?
- What features do I need?

Refer to Frequently asked questions about Azure Multi-Factor Authentication about common questions on using Azure MFA service.

Pricing and Licensing Requirements

Microsoft offers basic two-step verification features to Office 365 and Azure AD administrators for no extra cost. If you want to upgrade the features for your admins or extend two-step verification to the rest of your users, you can buy Azure MFA. Refer to How to get Azure Multi-Factor Authentication to help you understand the different ways to buy Azure MFA.

For specific details about pricing and billing, refer to Azure MFA Pricing.

Key Benefits

The key benefits of Azure MFA are:

Easy to Set Up
Azure Multi-Factor Authentication is designed for administrators to set up, use, and monitor.

Scalable

Azure Multi-Factor Authentication can be implemented for any number of users or groups and integrates with Active Directory and on-prem applications as well as cloud-based applications.

Always Protected
Azure Multi-Factor Authentication provides strong authentication using standard industry practices.

Reliable
Microsoft guarantees 99.9% availability of Azure Multi-Factor Authentication.

Intuitive User Experience
Users likely already use MFA with personal and other accounts, and their experience with Azure MFA is easy to activate and use. The extra protection that comes with Azure Multi-Factor Authentication allows users to manage their own devices.

Customer stories/Case studies

Discover how most organizations have come to understand the need for securing cloud identities with a second layer of authentication like Azure MFA. The following featured stories demonstrate these needs.

Wipro Limited – Wipro drives mobile productivity with Microsoft cloud security tools to improve customer engagements. The IT team uses a combination of single sign-on capabilities and Azure MFA to support conditional access, including device state conditional access.

Orica – Explosives provider simplifies business and improves data access with SAP S/4HANA on Azure. "We use Azure services for additional protection, such as automatically requiring anyone seeking access to our software and service applications to verify their identity through a mobile app, phone call, or text message. With Azure Active Directory and Multi-Factor Authentication, we know that people are who they say they are."

Coty – Cloud technology supports Coty in drive to celebrate beauty. "Enabling highly secure modern work environments is part of our overall vision to create an effortless end-user experience for our employees. We are using Office 365 Advanced Threat Protection and Microsoft Advanced Threat Analytics to improve the depth and breadth of our security capabilities, and we will use Microsoft Azure Multi-Factor Authentication for all Office apps and services."

To learn more about customer and partner experiences on Azure MFA, visit - See the amazing things people are doing with Azure.

Announcements/Blogs

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, refer to What's new in Azure Active Directory?

Blogs by the Tech Community and Microsoft Identity Division:

- February 20, 2019, Azure AD Ignite Recap 3: start your journey to password-less!
- October 23, 2018, Hardware OATH tokens in Azure MFA in the cloud are now available
- September 26, 2018, Announcing password-less login, identity governance, and more for Azure Active Directory
- June 06, 2018, More #AzureAD MFA Coolness – selectable verification methods and more OATH!

Compete Information, Independent Research

Azure MFA is compatible with the third-party MFA solutions using custom controls. These controls allow the use of certain external or custom services as conditional access controls, and generally extend the capabilities of Conditional Access.

For more information, refer to Custom controls.

Training/Learning Resources

The section provides concepts, role-based guidance, and lists the various training resources available on Azure MFA.

Level 100 Knowledge/Concepts

Microsoft understands that some organizations have unique environment requirements or complexities. If yours is one of these organizations, use these recommendations as a starting point. However, most organizations can implement these recommendations as suggested.

- Find "What is the identity secure score in Azure Active Directory?"
- Know the "'Five steps to securing your identity infrastructure"
- Understand "Identity and device access configurations"

Refer to the links below to learn how Azure MFA helps safeguard access to data and applications:

- Watch this short video – "Windows Azure Multi-Factor Authentication"
- Learn "How it works: Azure Multi-Factor Authentication"
- Learn "When to use an Azure Multi-Factor Authentication Provider"
- Follow "Frequently asked questions about Azure Multi-Factor Authentication"
- Know "Security guidance for using Azure Multi-Factor Authentication with Azure AD accounts"
- Understand "Which version of Azure MFA is right for my organization?"
- Do "Feature comparison of versions"

Role-Based Guidance

IT Administrator Staff

Enabling Azure MFA for your administrators adds a second layer of security to user sign-ins and transactions. Refer to Enforce multi-factor authentication (MFA) for subscription administrators

Users who have been assigned the Global Administrator role in Azure AD Tenants can enable two-step verification for their Azure AD Global Admin accounts at no additional cost.

- If you are using a Microsoft Account, refer to About two-step verification.
- If you are NOT using a Microsoft Account, refer to How to require two-step verification for a user or group.

Here are some additional links to help you get started:

- Understand Supportability for using Azure AD MFA.
- Get a step-by-step Azure MFA deployment plan.
- Get details about which version to deploy
- Learn When to use an Azure Multi-Factor Authentication Provider?
- Configure Azure Multi-Factor Authentication settings
- Manage user settings with Azure Multi-Factor Authentication in the cloud.
- Follow this Tutorial: How to turn on Azure Multi-Factor Authentication for Azure AD Administrators
- Follow Frequently asked questions about Azure Multi-Factor Authentication for general, installation, and operation related questions.

Help Desk Staff

- Search Frequently asked questions about Azure Multi-Factor Authentication.
- Search the Microsoft Support Knowledge Base for solutions to common technical issues.
- Search for and browse technical questions and answers from the community, or ask your own question in the Azure Active Directory forums.
- Contact Azure Multi-Factor Authentication Server (PhoneFactor) support.

Training

On-Demand Webinars

Reserve here - Secure your identities with Azure Multi-Factor Authentication

Videos

- Azure videos - How to get started with Azure MFA the right way
- Azure videos - Windows Azure Multi-Factor Authentication
- Azure videos - Multi-Factor Authentication for Azure AD
- YouTube - Introduction to Azure Multi Factor Authentication MFA
- Azure videos - Microsoft Azure Multi-Factor Authentication Deep Dive: Securing Access on Premises and in the Cloud

Online Courses

- PluralSight.com- Implementing and Managing Azure Multi-Factor Authentication
  "This course teaches you how to integrate Azure MFA with on-premises and cloud-based systems."

- SkillUp.Online- Securing Identities

"This course focuses on three key areas in defending against attackers who target security vulnerabilities, focused on credential theft and compromised identities: Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Azure Active Directory Privileged Identity Management (PIM)."

- PluralSight.com- Microsoft Azure Authentication Scenarios for Developers
  "This course provides guidance for Azure MFA, B2C, certificate-based authentication, and SQL Server authentication."

Books

Source: Microsoft Press - Modern Authentication with Azure Active Directory for Web Applications (Developer Reference) 1st Edition. "This book will guide you through the essentials of authentication protocols, decipher the disparate terminology applied to the subject, tell you how to get started with Azure AD, and then present concrete examples of applications that use Azure AD for their authentication and authorization, including how they work in hybrid scenarios with Active Directory Federation Services (ADFS)."

Tutorials

- Tutorial: Complete an Azure Multi-Factor Authentication pilot roll out
  In this tutorial, you walk you through configuring a conditional access policy enabling Azure Multi-Factor Authentication (Azure MFA) when logging in to the Azure portal.

- Use risk events to trigger Multi-Factor Authentication and password changes
  In this tutorial, you will configure risk-based policies that automatically respond to risky behaviors. These policies, can either automatically block or initiate remediation, including requiring password changes and enforcing Multi-Factor Authentication.

Whitepaper

Published October 17, 2018, Architect scalable e-commerce web app.

The e-commerce website includes simple order processing workflows with the help of Azure services (Including MFA). Using Azure Functions and Web Apps, developers can focus on building personalized experiences and let Azure take care of the infrastructure.

FAQ

Refer to Frequently asked questions about Azure Multi-Factor Authentication for general, billing models, user experiences, and troubleshooting questions.

End-user Readiness and Communication

This section provides customizable posters and email templates to roll out Azure MFA to your organization.

You can distribute the readiness material to your users during MFA rollout, educate them about the feature, and remind them to register.

- Download Multi-Factor Authentication rollout materials and customize them with your organization's branding.
- To register for Azure MFA, watch How to register for Azure Multi-Factor Authentication.
- See Converged registration for self-service password reset and Azure Multi-Factor Authentication (public preview)-
- Disable Azure AD converged registration (Public preview)

Planning and Change Management

This section provides the resource links to Azure MFA deployment plan and topology to help you determine your MFA strategies, and document your decisions and configurations to prepare for implementation.

Deployment Plan

Refer to the step-by-step Azure MFA Deployment Plan. The decisions and activities that you will need to consider for Azure MFA deployment are:

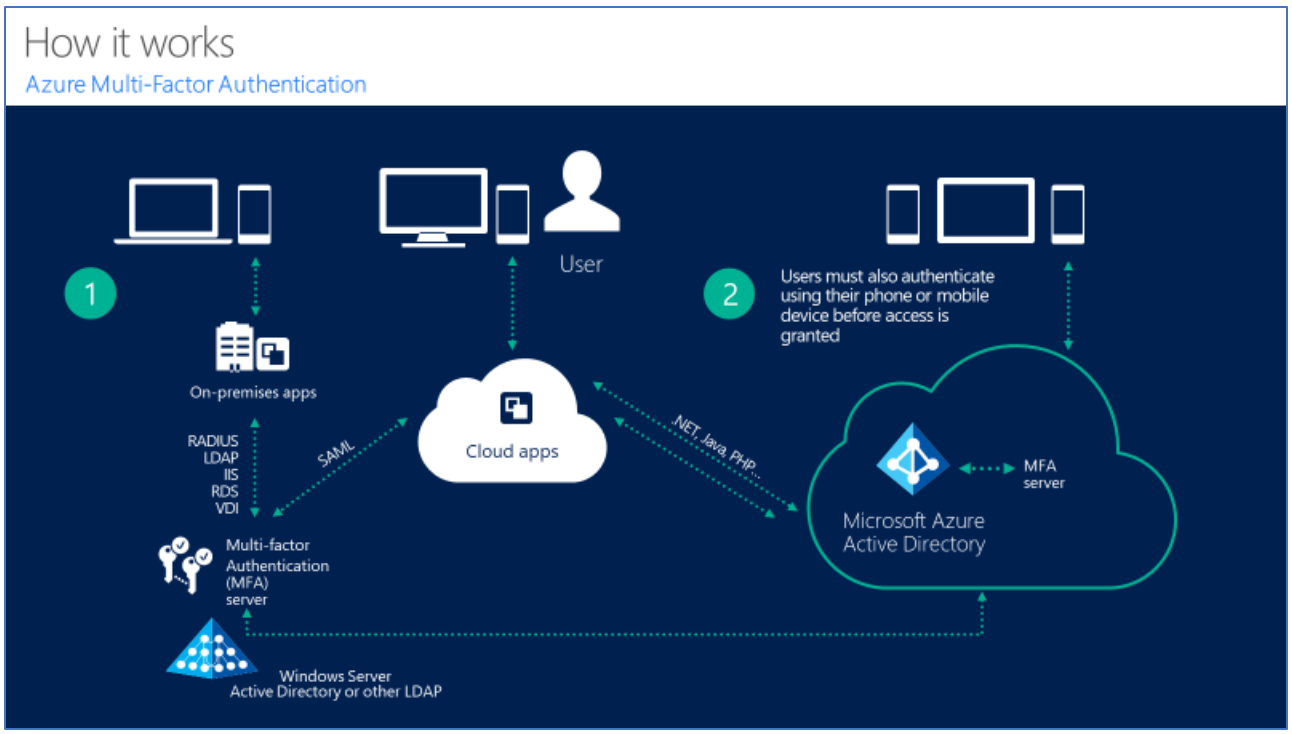
- Choose the authentication methods for the users.
- Determine whether to use Conditional Access with MFA.
- Determine how to define your network- Will you use Conditional Access and Named Locations, or Trusted IPs?
- Determine how to configure your MFA Registration policies.
- Determine your roll out plan, and communication strategies.

Architecture Plan/Topology

How does Azure MFA work?

The security of two-step verification lies in its layered approach. Azure MFA works by requiring two or more of the following authentication methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)



Testing

This section provides the plan to test the functionality of Azure MFA in a sandbox or test lab environment before the customer rolls it into production.

Project stages depend on environments that are available. If you have a non-production Azure tenant, it is a beneficial activity to complete a proof of concept (POC) outside of your production environment.

Follow the instructions under "General Planning Considerations" section in the Azure MFA Deployment Plan.

Deployment

How can I get Azure MFA deployed in my environment? This section provides resource links to help with implementation of your solution.

Deployment

To set up and use Azure MFA, follow the guidance under "Implementing Your Solution" section in the Azure MFA Deployment Plan.

You can also refer to the following links:

- Deploy cloud-based Azure Multi-Factor Authentication
- How to require two-step verification for a user

Readiness Checklist

Follow the readiness checklist under "Implementing Your Solution" section in the Azure MFA Deployment Plan.

Design Template

Follow the design template under "Implementing Your Solution" section in the Azure MFA Deployment Plan.

Operations

How do I manage and maintain Azure MFA? This section provides troubleshooting info, Azure MFA operation and management details, and other important references.

Operations

Follow the guidance under "Manage Your Solution" section in Azure MFA Deployment Plan.

Monitoring

Refer to the following links:

- Configure Azure Multi-Factor Authentication settings
- Reports in Azure Multi-Factor Authentication
- Manage user settings with Azure Multi-Factor Authentication in the cloud

Troubleshooting

Refer to Frequently asked questions about Azure Multi-Factor Authentication for troubleshooting questions.

References

What Does Azure Multi-Factor Authentication mean for me?

Manage Multi-Factor Authentication settings in the Azure portal, to help you to get the most out of Azure Multi-Factor Authentication.

Support and Feedback

How can we improve Azure AD MFA? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our Technical Community, a platform to Microsoft Azure Active Directory users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try StackOverflow or visit the MSDN Azure AD forums.

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - feedback.azure.com or contact a support professional through Azure Multi-Factor Authentication Server (PhoneFactor) support.