Microsoft Azure Multi-Factor Authentication- Adoption Kit

Version: 3.0
For the latest version, please check https://aka.ms/aadadoptionkits

Contents

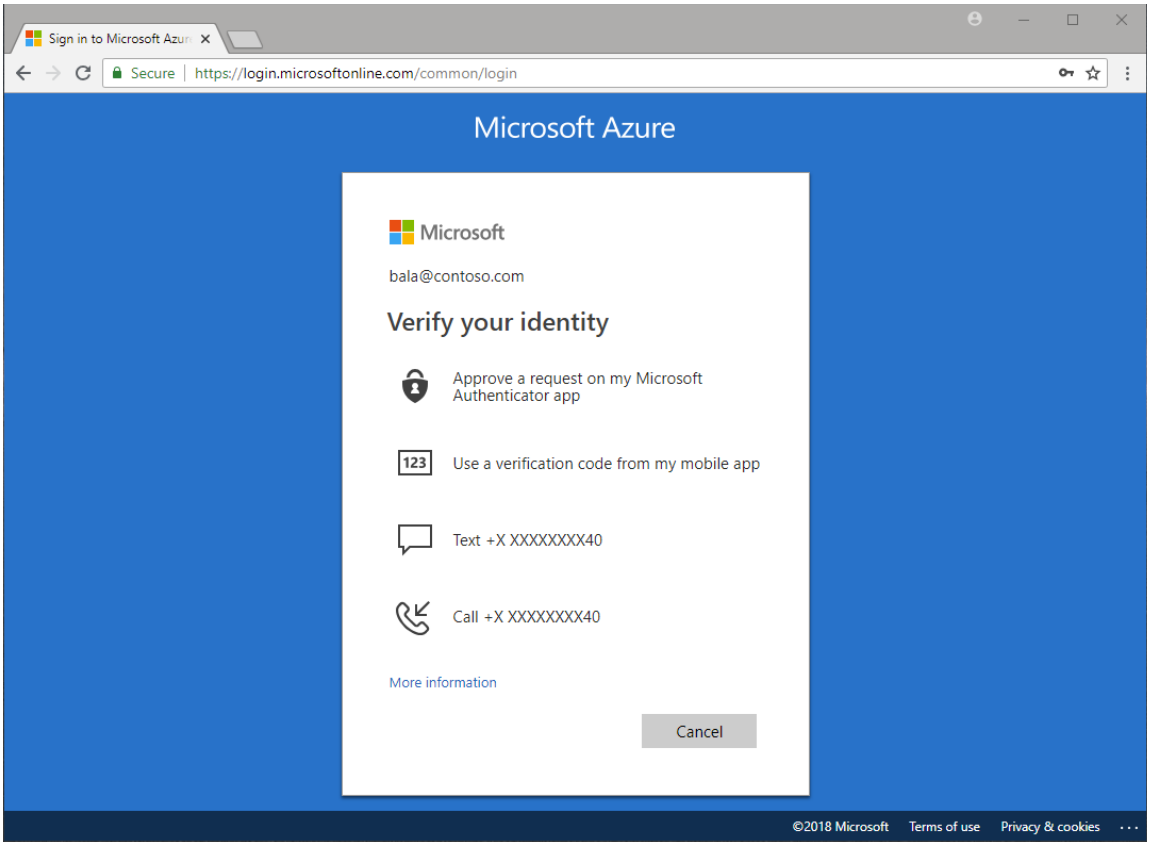
Awareness

This section helps you to analyze the benefits of Microsoft Azure Multi-Factor Authentication. You will learn about the ease of use, benefits, pricing, and licensing model. You can also access up-to-date announcements and blogs that discuss ongoing improvements.

Business overview

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

Multi-Factor Authentication 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, mobile app notification, or 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 Frequently asked questions about Multi-Factor Authentication for general, billing models, user experiences, and troubleshooting questions.

Key benefits

Using Multi-Factor Authentication gives you the following benefits:

Easy to set up
Your applications or services do not need to make any changes to use Multi-Factor Authentication. The verification prompts are part of the Azure AD sign-in event, which automatically requests and processes the Multi-Factor Authentication challenge when required. It is designed for administrators to easily set up, use, and monitor.

Scalable
Basic Multi-Factor Authentication features are available at no extra cost. You can upgrade to scale for a greater number of users or groups. You can integrate with Active Directory and on-prem applications as well as cloud-based applications.

Always protected
To enable protection for specific sign-in events, you can configure Conditional Access policies. Coupling Conditional Access with Azure AD Identity Protection which detects anomalies and suspicious events, allows you to require Multi-Factor Authentication when sign-in risk is medium or high.

Reliable
Microsoft guarantees 99.9% availability of Multi-Factor Authentication. This feature is especially dependable for accounts with privileged access to resources.

Intuitive user experience
Users likely already use Multi-Factor Authentication with personal and other accounts, and their experience is that it is simple to activate and use. The extra protection that comes with Multi-Factor Authentication allows users to manage their own devices.

Pricing and licensing requirements

Choose features and licenses for Multi-Factor Authentication depending on your organization’s needs. For more information on pricing and billing, see Azure AD pricing.

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 AD?

Training/learning resources

The following resources are a good start to learn about Multi-Factor Authentication. They include level 100 concepts, videos by our experts, books, link to online courses, and useful whitepapers for reference.

Level 100 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 AD?
- Know the five steps to securing your identity infrastructure.
- Understand identity and device access configurations.

Refer to the following links to get started with Multi-Factor Authentication:

- Read the Azure Multi-Factor Authentication overview
- Learn about authentication and verification methods available in Azure AD
- Learn how Azure Multi-Factor Authentication works?
- Understand Conditional Access policies and security defaults.
- Understand risk detection and remediation using Azure AD Identity Protection
- Find which Multi-Factor Authentication version is right for your organization
- Know about Multi-Factor Authentication for Microsoft 365
- Learn to optimize reauthentication prompts and understand session lifetime for Multi-Factor Authentication
- Frequently asked questions (FAQs) about Azure Multi-Factor Authentication

For more information, deep-dive into Authentication documentation.

Training resources

Videos

Video	Description
How to get started with identity security	Learn about identity security, why is it important, and what you can do to get it more secure.
How to improve your identity security posture with Secure Score	Get a walk-through of the identity secure score in the Azure AD portal.
Introduction to Azure Multi Factor Authentication	Get a Multi-Factor Authentication walkthrough by Microsoft Virtual Academy.
How to choose the right authentication option in Azure AD	Learn how to choose the right authentication option when setting up your identity in Azure AD, based on the needs of the organization.
How to upgrade your security with Azure Multi-Factor Authentication	Get an overview of Multi-Factor Authentication, learn how to use Multi-Factor Authentication with Conditional Access, and learn best practices.

How to register your security information in Azure Active Directory	Learn how to register the security information through Azure AD for security features like Multi-Factor Authentication and Self-Service Password Reset. End users will also learn how to view and manage their security methods in Azure AD.

Books

Source: Microsoft Press - Modern Authentication with Azure Active Directory for Web Applications (Developer Reference) 1st Edition.

Learn the essentials of authentication protocols and get started with Azure AD. Refer to 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).

Online courses

Refer to the following courses on Multi-Factor Authentication at pluralsight.com:

Course	Description
Implementing and managing Azure Multi-Factor Authentication	This course demonstrates how to integrate Multi-Factor Authentication with on-premises and cloud-based systems.
Microsoft Azure Authentication scenarios for developers	This course provides guidance for Multi-Factor Authentication, Azure Business to consumers (B2C), certificate-based authentication, and SQL server authentication.

Whitepaper

Whitepaper	Description
Create a resilient access control management strategy with Azure Active Directory	Get an understanding on strategies an organization might adopt to provide resilience and reduce the risk of lockout during unforeseen disruptions. For example, implement Multi-Factor Authentication using Conditional Access rather than per-user Multi-Factor Authentication.
Zero Trust Deployment Guide for Microsoft Azure Active Directory	This guidance is to assist you if you are engaging in Microsoft's Zero Trust security strategy.

Plan and change management

In this section, you deep-dive into planning and deploying Multi-Factor Authentication in your organization.

Deployment plan

Planning your Multi-Factor Authentication deployment is critical to make sure you achieve the required authentication strategy for your organization.

Refer to Multi-Factor Authentication Deployment Plan - a comprehensive guide to plan and implement Multi-Factor Authentication in your organization. It includes the following sections:

Sections	Description
Prerequisites	Get prepared for the deployment
Plan user rollout	Determine your roll out plan, and communication strategies.
Deployment considerations	Determine how to define your network- Will you use Conditional Access and Named Locations, or Trusted IPs?
Plan authentication methods	Choose the authentication methods for the users.
Plan registration policy	Determine how to configure your Multi-Factor Authentication Registration policies.
Plan Conditional Access policies	Determine how to configure other Conditional Access policies to implement Multi-Factor Authentication.
Plan integration with on-premises systems	Determine how you will integrate legacy and on-premises applications
Implement your plan	Step-by-step instructions to implement your plan
Manage your solution	View Azure Multi-Factor Authentication reports
Troubleshoot Multi-Factor Authentication issues	Collect information to ease troubleshooting and follow the instructions

Quickstarts

Follow the step-by-step guidance to:

- Set up Multi-Factor Authentication
- Enable Security defaults
- Secure user sign-in events with Azure Multi-Factor Authentication
- Use risk detections for user sign-ins to trigger Azure Multi-Factor Authentication or password changes

End-user readiness and communication

Download Multi-Factor Authentication rollout materials and customize them with your organization's branding. You can distribute the readiness material to your users during Multi-Factor Authentication rollout, educate them about the feature, and remind them to register.

Combined registration with Self-Service Password Reset

We recommend that you enable combined security information registration in Azure AD for SSPR and Multi-Factor Authentication.

Before enabling the new experience, review the article combined security information registration to ensure you understand the functionality and effects of this feature. In case of issues, refer to Troubleshooting combined security information registration.

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 Multi-Factor Authentication.

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 Multi-Factor Authentication to support conditional access, including device-state conditional access.

Orica – Explosives provider simplifies business and improves data access with SAP S/4HANA on Azure. Orica uses Azure services for additional protection, such as automatically requiring anyone seeking access to the software and service applications to verify their identity through Multi-Factor Authentication.

Aramex delivery limited - Global logistics and transportation company creates cloud-connected office with identity and access management solution. Ensuring secure access was especially difficult with Aramex's remote employees. The company is now applying conditional access to let these remote employees access their SaaS applications from outside the network. The conditional access rule will decide whether to enforce Multi-Factor Authentication, giving only the right people the right access.

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

Support and feedback

How can we improve Multi-Factor Authentication? 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 AD 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 Multi-Factor Authentication Server (PhoneFactor) support.

Next steps

- Learn about Conditional Access
- Learn more about Identity Protection