

AFFIDAVIT OF MINA CHING

1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.
2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.
3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.
4. The archived data made viewable and browseable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.
5. The Internet Archive assigns a URL on its site to the archived files in the format `http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]` aka an "extended URL". Thus, the extended URL `http://web.archive.org/web/19970126045828/http://www.archive.org/` would be the URL for the record of the Internet Archive home page HTML file (`http://www.archive.org/`) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.

MICROSOFT CORP.
EXHIBIT 1022





archive.org

6. Attached hereto as Exhibit A are true and accurate copies of browser screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each screenshot.
7. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATE: 10/14/2025



Mina Ching

**Please see attached
All Purpose
Jurat form
for additional
Notary Events**



EXHIBIT A



<https://web.archive.org/web/20160419012327/https://azure.microsoft.com/en-us/documentation/articles/active-directory-identityprotection/?rnd=1>



Search for docs 🔍

- ▶ Overview
- ▶ Managing applications
- ▶ Integrating on-premises identities
- ▶ Get started
- ▶ Tell me how it works
- ▶ Develop applications
- ▶ What's next
- ▶ Troubleshooting

See more ▶

Azure Active Directory Identity Protection



By Markus Vilcinskis

Updated: 03/18/2016

Contributors: [Edit on GitHub](#)

Azure Active Directory Identity Protection is a security service that provides a consolidated view into risk events and potential vulnerabilities affecting your organization's identities. Microsoft has been securing cloud-based identities for over a decade, and with Azure AD Identity Protection, Microsoft is making these same protection systems available to enterprise customers. Identity Protection leverages existing Azure AD's anomaly detection capabilities (available through Azure AD's Anomalous Activity Reports), and introduces new risk event types that can detect anomalies in real-time.

Limitations of the current preview

This section lists limitations that apply to the current preview of Azure Active Directory Identity Protection.

Country or Region limitation

The preview of Azure Active Directory Identity Protection is currently available only for directories with a **Country or Region** value of **United States**.

Remediation

Identity Protection and federated domains

The preview of Azure Active Directory Identity Protection has the following limitations in conjunction with federated domains:

- Security policies do not work for federated domains
- Risk events are only detected for apps federating with Azure Active Directory

Getting Started

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. Attackers have become increasingly effective at leveraging third party breaches, and using sophisticated phishing attacks. Once an attacker gains access to even a low privileged user account, it is relatively straightforward for them to gain access to important company resources through lateral movement. It is therefore essential to protect all identities and, when an identity is compromised, proactively prevent the compromised identity from being abused.

Discovering compromised identities is no easy task. Fortunately, Identity Protection can help: Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised.

Using this data, Identity Protection generates reports and alerts that enables you to investigate these risk events and take appropriate remediation or mitigation action.

But Azure Active Directory Identity Protection more than a monitoring and reporting tool. Based on risk events, Identity Protection calculates a user risk level for each user, enabling you to configure risk-based policies to automatically protect the identities of your organization. These risk-based policies, in addition to other conditional access controls provided by Azure Active Directory and EMS, can automatically block or offer adaptive remediation actions that include password resets and multi-factor authentication enforcement.

[Explore Identity Protection's capabilities](#)



Detecting risk events and risky accounts:

- Detecting 6 risk event types using machine learning and heuristic rules
- Calculating user risk levels
- Providing custom recommendations to improve overall security posture by highlighting vulnerabilities

Investigating risk events:

- Sending notifications for risk events
- Investigating risk events using relevant and contextual information
- Providing basic workflows to track investigations
- Providing easy access to remediation actions such as password reset

Risk-based conditional access policies:

- Policy to mitigate risky sign-ins by blocking sign-ins or requiring multi-factor authentication challenges.
- Policy to block or secure risky user accounts
- Policy to require users to register for multi-factor authentication

Detection and Risk

Risk events

Risk events are events that were flagged as suspicious by Identity Protection, and indicate that an identity may have been compromised. For a complete list of risk events, see [Types of risk events detected by Azure Active Directory Identity Protection](#).

Some of these risk events have been available through the Azure AD Anomalous Activity reports in the Azure Management Portal. The table below lists the various risk event types and the corresponding **Azure AD Anomalous Activity** report. Microsoft is continuing to invest in this space, and plans to continuously improve the detection accuracy of existing risk events and add new risk event types on an ongoing basis.

Identity Protection Risk Event Type	Corresponding Azure AD Anomalous Activity Report
Leaked credentials	Users with leaked credentials
Impossible travel to atypical locations	Irregular sign-in activity
Sign-ins from infected devices	Sign-ins from possibly infected devices
Sign-ins from anonymous IP addresses	Sign-ins from unknown sources
Sign-ins from IP addresses with suspicious activity	Sign-ins from IP addresses with suspicious activity
Signs in from unfamiliar locations	-
Lockout events (not in public preview)	-

The following Azure AD Anomalous Activity reports are not included as risk events in Azure AD Identity Protection, and will therefore not be available through Identity Protection. These reports are still available in the Azure Management Portal however they will be deprecated at some time in the future as they are being superseded by risk events in Identity Protection.

- Sign-ins after multiple failures
- Sign-ins from multiple geographies

Risk level

The Risk level for a risk event is an indication (High, Medium, or Low) of the severity of the risk event. The risk level helps Identity Protection users prioritize the actions they must take to



reduce the risk to their organization. The severity of the risk event represents the strength of the signal as a predictor of identity compromise, combined with the amount of noise that it typically introduces.

- **High:** High confidence and high severity risk event. These events are strong indicators that the user's identity has been compromised, and any user accounts impacted should be remediated immediately.
- **Medium:** High severity, but lower confidence risk event, or vice versa. These events are potentially risky, and any user accounts impacted should be remediated.
- **Low:** Low confidence and low severity risk event. This event may not require an immediate action, but when combined with other risk events, may provide a strong indication that the identity is compromised.

Risk Level

Risk events are either identified in **real-time**, or in post-processing after the risk event has already taken place (offline). Currently most risk events in Identity Protection are computed offline, and show up in Identity Protection within 2-4 hours. While evaluated in real-time, the real-time risk events will show up in the Identity Protection Console within 5-10 minutes.

Several legacy clients do not currently support real-time risk event detection and prevention. As a result, sign-ins from these clients cannot be detected or prevented in real-time.

Investigation

Your journey through Identity Protection typically starts with the Identity Protection dashboard.

Remediation

The dashboard gives you access to:

- Reports such as **Users flagged for risk**, **Risk events** and **Vulnerabilities**
- Settings such as the configuration of your **Security Policies**, **Notifications** and **multi-factor authentication registration**

It is typically your starting point for investigation, which is the process of reviewing the activities, logs, and other relevant information related to a risk event to decide whether remediation or mitigation steps are necessary, and how the identity was compromised, and understand how the compromised identity was used.

You can tie your investigation activities to the [notifications](#) Azure Active Directory Protection sends per email.

The following sections provide you with more details and the steps that are related to an investigation.

What is a user risk level?

A user risk level is an indication (High, Medium, or Low) of the likelihood that the user's identity has been compromised. It is calculated based on the user risk events that are associated with the user's identity.

The status of a risk event is either **Active** or **Closed**. Only risk events that are **Active** contribute to the user risk calculation.

The user risk level is calculated using the following inputs:

- Active risk events impacting the user
- Risk level of these events
- Whether any remediation actions have been taken

User risks

You can use the user risk levels to create conditional access policies to block risky users from signing in, or force them to securely change their password.

Closing risk events manually

In most cases, you will take remediation actions such as a secure password reset to automatically close risk events. However, this might not always be possible.



automatically close risk events. However, this might not always be possible.

This is, for example, the case, when:

- A user with Active risk events has been deleted
- An investigation reveals that a reported risk event has been performed by the legitimate user

Because risk events that are **Active** contribute to the user risk calculation, you may have to manually lower a risk level by closing risk events manually.


During the course of investigation, you can choose to take any of these actions to change the status of a risk event:

Actions


- **Resolve** - If after investigating a risk event, you took an appropriate remediation action outside Identity Protection, and you believe that the risk event should be considered closed, mark the event as Resolved. Resolved events will set the risk event's status to Closed and the risk event will no longer contribute to user risk.
- **Mark as false-positive** - In some cases, you may investigate a risk event and discover that it was incorrectly flagged as a risky. You can help reduce the number of such occurrences by marking the risk event as False-positive. This will help the machine learning algorithms to improve the classification of similar events in the future. The status of false-positive events is to **Closed** and they will no longer contribute to user risk.
- **Ignore** - If you have not taken any remediation action, but want the risk event to be removed from the active list, you can mark a risk event Ignore and the event status will be Closed. Ignored events do not contribute to user risk. This option should only be used under unusual circumstances.
- **Reactivate** - Risk events that were manually closed (by choosing **Resolve**, **False positive**, or **Ignore**) can be reactivated, setting the event status back to **Active**. Reactivated risk events contribute to the user risk level calculation. Risk events closed through remediation (such as a secure password reset) cannot be reactivated.

To open the related configuration dialog:

1. On the **Azure AD Identity Protection** blade, click **Users flagged for risk**.

 Manual password reset

2. Right-click the affected user.

 Manual password reset

Remediating user risk events

A remediation is an action to secure an identity or a device that was previously suspected or known to be compromised. A remediation action restores the identity or device to a safe state, and resolves previous risk events associated with the identity or device.

To remediate user risk events, you can:

- Perform a secure password reset to remediate user risk events manually
- Configure a user risk security policy to mitigate or remediate user risk events automatically
- Re-image the infected device

Manual secure password reset

A secure password reset is an effective remediation for many risk events, and when performed, automatically closes these risk events and recalculates the user risk level. You can use the Identity Protection dashboard to initiate a password reset for a risky user.

The related dialog provides two different methods to reset a password:

Reset password - Select **Require user to reset password** to allow the user to self-recover if the user has registered for multi-factor authentication. During the user's next sign-in, the user will be required to solve a multi-factor authentication challenge successfully and then, forced to change the password. This option isn't available if the user account is not already registered multi-factor authentication.

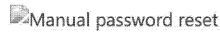
Temporary password - Select **Generate a temporary password** to immediately invalidate the existing password, and create a new temporary password for the user. Send the new temporary password to an alternate email address for the user or to the user's manager. Because the password is temporary, the user will be prompted to change the password upon sign-in.



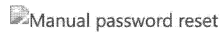


To open the related configuration dialog:

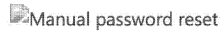
1. On the Azure AD Identity Protection blade, click **Users flagged for risk**.



2. Click the affected user

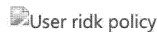


3. Click **Reset password**



User risk security policy

A user risk security policy is a conditional access policy that evaluates the risk level to a specific user and applies remediation and mitigation actions based on predefined conditions and rules.



Azure AD Identity Protection helps you manage the mitigation and remediation of users flagged for risk by enabling you to:

- Set the users and groups the policy applies to:



- Set the user risk level threshold (low, medium, or high) that triggers a password change:



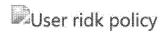
- Set the user risk level threshold (low, medium, or high) that triggers blocking a user:



- Switch the state of your policy:



- Review and evaluate the impact of a change before activating it:



Choosing a **High** threshold reduces the number of times a policy is triggered and minimizes the impact to users. However, it excludes **Low** and **Medium** users flagged for risk from the policy, which may not secure identities or devices that were previously suspected or known to be compromised.

When setting the policy,

- Exclude users who are likely to generate a lot of false-positives (developers, security analysts)
- Exclude users in locales where enabling the policy is not practical (for example no access to helpdesk)
- Use a **High** threshold during initial policy roll out, or if you must minimize challenges seen by end users.
- Use a **Low** threshold if your organization requires greater security. Selecting a **Low** threshold introduces additional user sign-in challenges, but increased security.

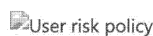
The recommended default for most organizations is to configure a rule for a **Medium** threshold to strike a balance between usability and security.

For an overview of the related user experience, see:

- [Compromised account recovery flow.](#)
- [Compromised account blocked flow.](#)

To open the related configuration dialog:

1. On the Azure AD Identity Protection blade, click **Settings**.



2. In the **Security Policies** section, click **User risk**.



Mitigating user risk events

Administrators can set a user risk security policy to block users upon sign-in depending on the risk level.

Blocking a sign-in:

- Prevents the generation of new user risk events for the affected user
- Enables administrators to manually remediate the risk events affecting the user's identity and restore it to a secure state

What is a sign-in risk level?

A sign-in risk level is an indication (High, Medium, or Low) of the likelihood that for a specific sign-in, someone else is attempting to authenticate with the user's identity. The sign-in risk level is evaluated at the time of a sign-in and considers risk events and indicators detected in real-time for that specific sign-in.

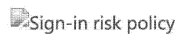
Mitigating sign-in risk events

A mitigation is an action to limit the ability of an attacker to exploit a compromised identity or device without restoring the identity or device to a safe state. A mitigation does not resolve previous sign-in risk events associated with the identity or device.

You can use conditional access in Azure AD Identity Protection to automatically mitigate sign-in risk events. Using these policies, you consider the risk level of the user or the sign-in to block risky sign-ins or require the user to perform multi-factor authentication. These actions may prevent an attacker from exploiting a stolen identity to cause damage, and may give you some time to secure the identity.

Sign-in risk security policy

A sign-in risk policy is a conditional access policy that evaluates the risk to a specific sign-in and applies mitigations based on predefined conditions and rules.

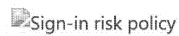


Azure AD Identity Protection helps you manage the mitigation of risky sign-ins by enabling you to:

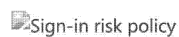
- Set the users and groups the policy applies to:



- Set the sign-in risk level threshold (low, medium, or high) that triggers a multi-factor authentication challenge for the affected sign-ins:



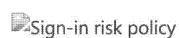
- Set the sign-in risk level threshold (low, medium, or high) that blocks the affected sign-ins:



- Switch the state of your policy:



- Review and evaluate the impact of a change before activating it:



Choosing a **High** threshold reduces the number of times a policy is triggered and minimizes the impact to users.

However, it excludes **Low** and **Medium** sign-ins flagged for risk from the policy, which may not block an attacker from exploiting a compromised identity.

When setting the policy,



- Exclude users who do not/cannot have multi-factor authentication
- Exclude users in locales where enabling the policy is not practical (for example no access to helpdesk)
- Exclude users who are likely to generate a lot of false-positives (developers, security analysts)
- Use a **High** threshold during initial policy roll out, or if you must minimize challenges seen by end users.
- Use a **Low** threshold if your organization requires greater security. Selecting a **Low** threshold introduces additional user sign-in challenges, but increased security.

The recommended default for most organizations is to configure a rule for a **Medium** threshold to strike a balance between usability and security.

The sign-in risk policy is:

- Applied to all browser traffic and sign-ins using modern authentication.
- Not applied to applications using older security protocols by disabling the WS-Trust endpoint at the federated IDP, such as ADFS.

The **Risk Events** page in the Identity Protection console lists all events:

- This policy was applied to
- You can review the activity and determine whether the action was appropriate or not

For an overview of the related user experience, see:

- [Risky sign-in recovery](#)
- [Risky sign-in blocked](#)
- [Multi-factor authentication registration during a risky sign-in](#)

To open the related configuration dialog:

1. On the **Azure AD Identity Protection** blade, click **Settings**.



2. In the **Security Policies** section, click **Sign-in risk**.



Multi-factor authentication registration policy

Azure Multi-factor authentication is a method of verifying who you are that requires the use of more than just a username and password. It provides a second layer of security to user sign-ins and transactions.

We recommend that you require Azure Multi-Factor Authentication for user sign-ins because it:

- Delivers strong authentication with a range of easy verification options
- Plays a key role in preparing your organization to protect and recover from account compromises

For more details, see [What is Azure Multi-Factor Authentication?](#)

Azure AD Identity Protection helps you manage the roll-out of multi-factor authentication registration by configuring a policy that enables you to:

- View the current registration status:



- Set the users and groups the policy applies to:



- Define how long they are allowed to skip registration:



- Switch the state of your policy:



For an overview of the related user experience, see:



- [Multi-factor authentication registration flow.](#)
- [Multi-factor authentication registration during a risky sign-in.](#)

To open the related configuration dialog:

1. On the **Azure AD Identity Protection** blade, click **Settings**.



2. In the **Multi-Factor Authentication** section, click **Registration**.



See also

- [Channel 9: Azure AD and Identity Show: Identity Protection Preview](#)
- [Types of risk events detected by Azure Active Directory Identity Protection](#)
- [Vulnerabilities detected by Azure Active Directory Identity Protection](#)
- [Azure Active Directory Identity Protection notifications](#)
- [Azure Active Directory Identity Protection flows](#)
- [Azure Active Directory Identity Protection playbook](#)
- [Azure Active Directory Identity Protection glossary](#)

Go Social

- Facebook
- Twitter
- Rss
- Newsletter

Microsoft Azure

- [Services](#)
- [Regions](#)
- [Case Studies](#)
- [Pricing](#)
- [Member Offers](#)
- [Calculator](#)
- [Documentation](#)
- [Downloads](#)
- [Samples](#)
- [Marketplace](#)
- [Azure in China](#)
- [Azure Government](#)

Community

- [Blog](#)
- [Service Updates](#)
- [Forums](#)
- [Events](#)
- [Careers](#)

Support

- [Forums](#)
- [Azure Status Dashboard](#)
- [Support](#)

Account

- [Subscriptions](#)
- [Profile](#)
- [Preview Features](#)
- [Microsoft Azure portal](#)

Trust Center

- [Security](#)
- [Privacy](#)
- [Compliance](#)

Hello from **Seattle**.

English (US) ▼

USD ▼

[Contact Us](#) [Feedback](#) [Trademarks](#) [Privacy & Cookies](#)

Microsoft
© 2016 Microsoft



<https://web.archive.org/web/20160314054531/https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/>



Search for docs

- Overview
 - What is Azure Multi-Factor Authentication?
 - How it Works
- Get Started
- Develop Applications
- How to Manage
- How do we use multi-factor authentication?
- Common IT Scenarios
- Troubleshooting

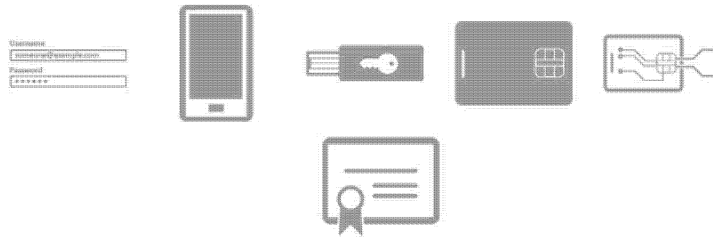
See more ▶

What is Azure Multi-Factor Authentication?

By Bill Mathers
Updated: 03/03/2016 Contributors: +1 [Edit on GitHub](#)

Multi-factor authentication (MFA) is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions. It works by requiring any two or more of the following verification 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)



Azure Multi-factor authentication is a method of verifying who you are that requires the use of more than just a username and password. It provides a second layer of security to user sign-ins and transactions.

Azure Multi-Factor Authentication helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of easy verification options—phone call, text message, or mobile app notification or verification code and 3rd party OATH tokens.

For an overview of how Azure Multi-Factor Authentication works see the following video.

Why use Azure Multi-Factor Authentication?

Today, now more than ever, people are increasingly connected. With smart phones, tablets, laptops, and PCs, people have several different options on how they are going to connect and stay connected at any time. People can access their accounts and applications from anywhere and this means that they can get more work done and serve their customers better.

Azure Multi-Factor Authentication is an easy to use, scalable, and reliable solution that provides a second method of authentication so your users are always protected.



Easy to use Scalable Always Protected Reliable

- **Easy to Use** - Azure Multi-Factor Authentication is simple to setup and use. The additional protection that comes with Azure Multi-Factor Authentication allows users to use and manage their own devices and, in many instances, it can be setup with just a few simple clicks.
- **Scalable** - Azure Multi-Factor Authentication utilizes the power of the cloud and integrates with your on-premises AD and custom apps. This protection is even extended to your high volume mission critical scenarios.
- **Always Protected** - Azure Multi-Factor Authentication provides strong authentication using



the highest industry standards.

- **Reliable** - We guarantee 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process authentication requests for the multi-factor authentication.

For additional information on why use Azure Multi-Factor Authentication see the following video.

How Azure Multi-Factor Authentication works

The security of multi-factor authentication lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the trusted device. Should the user lose the device, the person who finds it won't be able to use it unless he or she also knows the user's password.



Azure Multi-Factor Authentication helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It provides additional security by requiring a second form of authentication and delivers strong authentication via a range of easy verification options:

- phone call
- text message
- mobile app notification—allowing users to choose the method they prefer
- mobile app verification code
- 3rd party OATH tokens

For additional information oh how it works see the following video.

Methods available for multi-factor authentication

When a user signs in, an additional verification is sent to the user. The following are a list of methods that can be used for this second verification.

Verification Method	Description
Phone Call	A call is placed to a user's smart phone asking them to verify that they are signing in by pressing the # sign. This will complete the verification process. This option is configurable and can be changed to a code that you specify.
Text Message	A text message will be sent to a user's smart phone with a 6 digit code. Enter this code in to complete the verification process.



Mobile App Notification	A verification request will be sent to a user's smart phone asking them complete the verification by selecting Verify from the mobile app. This will occur if you selected app notification as your primary verification method. If they receive this when they are not signing in, they can choose to report it as fraud.
Verification code with Mobile App	A verification code will be sent to the mobile app that is running on a user's smart phone. This will occur if you selected a verification code as your primary verification method.

Available versions of Azure Multi-Factor Authentication

Azure Multi-Factor Authentication is available in three different versions. The table below describes each of these in more detail.

Version	Description
Multi-Factor Authentication for Office 365	This version works exclusively with Office 365 applications and is managed from the Office 365 portal. So administrators can now help secure their Office 365 resources by using multi-factor authentication. This version comes with an Office 365 subscription.
Multi-Factor Authentication for Azure Administrators	The same subset of Multi-Factor Authentication capabilities for Office 365 will be available at no cost to all Azure administrators. Every administrative account of a Azure subscription can now get additional protection by enabling this core multi-factor authentication functionality. So an administrator that wants to access Azure portal to create a VM, a web site, manage storage, mobile services or any other Azure Service can add multi-factor authentication to his administrator account.
Azure Multi-Factor Authentication	Azure Multi-Factor Authentication offers the richest set of capabilities. It provides additional configuration options via the Azure Management portal, advanced reporting, and support for a range of on-premises and cloud applications. Azure Multi-Factor Authentication comes as part of Azure Active Directory Premium.

Feature comparison of versions

The following table below provides a list of the features that are available in the various versions of Azure Multi-Factor Authentication.

Feature	Multi-Factor Authentication for Office 365 (included in Office 365 SKUs)	Multi-Factor Authentication for Azure Administrators (included with Azure subscription)	Azure Multi-Factor Authentication (included in Azure AD Premium and Enterprise Mobility Suite)
Administrators can protect accounts with MFA	*	*(Available only for Azure Administrator accounts)	*
Mobile app as a second factor	*	*	*
Phone call as a second factor	*	*	*
SMS as a second factor	*	*	*
App passwords for clients that	*	*	*



don't support
MFA

Admin control over authentication methods	(Public Preview)	(Public Preview)	*
PIN mode			*
Fraud alert			*
MFA Reports			*
One-Time Bypass			*
Custom greetings for phone calls			*
Customization of caller ID for phone calls			*
Event Confirmation			*
Trusted IPs			*
Remember MFA for trusted devices	*	*	*
MFA SDK			*
MFA for on-premises applications using MFA server			*

How to get Azure Multi-Factor Authentication

If you would like the full functionality offered by Azure Multi-Factor Authentication instead of just those provided for Office 365 users and Azure administrators, there are several options to get it:

1. Purchase Azure Multi-Factor Authentication licenses and assign them to your users.
2. Purchase licenses that have Azure Multi-Factor Authentication bundled within them such as Azure Active Directory Premium, Enterprise Mobility Suite or Enterprise Cloud Suite and assign them to your users.
3. Create an Azure Multi-Factor Authentication Provider within an Azure subscription. If you don't already have an Azure subscription, you can sign up for an Azure trial subscription. Trial subscriptions will need to be converted to regular subscriptions prior to trial expiration.

When using an Azure Multi-Factor Authentication Provider there are two usage models available that are billed through your Azure subscription:

- **Per User.** Generally for enterprises that want to enable multi-factor authentication for a fixed number of employees who regularly need authentication.
- **Per Authentication.** Generally for enterprises that want to enable multi-factor authentication for a large group of external users who infrequently need authentication.

Azure Multi-Factor Authentication provides selectable verification methods for both cloud and server. This means that you can choose which methods are available for your users to use with multi-factor authentication. This feature is currently in public preview for the cloud version of multi-factor authentication. For additional information see [selectable verification methods](#).

For pricing details see [Azure MFA Pricing](#).

Choose the per-seat or consumption-based model that works best for your organization. Then to get started see [Getting Started](#).



Choose the multi-factor security solution for you

Because there are several flavors of Azure Multi-Factor Authentication we must determine a couple of things in order to figure out which version is the proper one to use. Those things are:

- What am I trying to secure
- Where are the users located

The following sections will provide guidance on determining each of these.

What am I trying to secure?

In order to determine the correct multi-factor authentication solution, first we must answer the question of what are you trying to secure with a second method of authentication. Is it an application that is in Azure? Or is it a remote access system for example. By determining what we are trying to secure, we will see to answer the question of where multi-factor authentication needs to be enabled.

What are you trying to secure	Multi-Factor Authentication in the cloud	Multi-Factor Authentication Server
First party Microsoft apps	*	*
SaaS apps in the app gallery	*	*
IIS applications published through Azure AD App Proxy	*	*
IIS applications not published through Azure AD App Proxy		*
Remote access such as VPN, RDG		*

Where are the users located

Next, depending on where are users are located, we can determine the correct solution to use, whether it is multi-factor authentication in the cloud or on-premises using the MFA Server.

User Location	Solution
Azure Active Directory	Multi-Factor Authentication in the cloud
Azure AD and on-premises AD using federation with AD FS	Both MFA in the cloud and MFA Server are available options
Azure AD and on-premises AD using DirSync, Azure AD Sync, Azure AD Connect - no password sync	Both MFA in the cloud and MFA Server are available options
Azure AD and on-premises AD using DirSync, Azure AD Sync, Azure AD Connect - with password sync	Multi-Factor Authentication in the cloud
On-premises Active Directory	Multi-Factor Authentication Server

The following table is a comparison of the features that are a with Multi-Factor Authentication in the cloud and with the Multi-Factor Authentication Server.

	Multi-Factor Authentication in the cloud	Multi-Factor Authentication Server
Mobile app notification as a second factor	•	•
Mobile app verification code as a second factor	•	•
Phone call as second factor	•	•
One-way SMS as second factor	•	•



Two-way SMS as second factor		•
Hardware Tokens as second factor		•
App passwords for clients that don't support MFA	•	
Admin control over authentication methods	(Public Preview)	•
PIN mode		•
Fraud alert	•	•
MFA Reports	•	•
One-Time Bypass		•
Custom greetings for phone calls	•	•
Customizable caller ID for phone calls	•	•
Trusted IPs	•	•
Remember MFA for trusted devices	•	
Conditional access	•	•
Cache		•

Now that we have determined whether to use cloud multi-factor authentication or the MFA Server on-premises, we can get started setting up and using Azure Multi-Factor Authentication. Select the icon that represents your scenario!



MFA in the cloud



MFA on-premises

Go Social

- Facebook
- Twitter
- Rss
- Newsletter

Microsoft Azure

- Services
- Regions
- Case Studies
- Pricing
- Member Offers
- Calculator
- Documentation
- Downloads
- Samples
- Marketplace
- Azure in China
- Azure Government

Community

- Blog
- Service Updates
- Forums
- Events
- Careers

Support

- Forums
- Azure Status Dashboard
- Support

Account

- Subscriptions
- Profile
- Preview Features
- Microsoft Azure portal

Trust Center

- Security
- Privacy
- Compliance

Hello from Seattle.
English (US) ▾
USD ▾
Contact Us Feedback Trademarks Privacy & Cookies

© 2016 Microsoft





JURAT ATTACHMENT

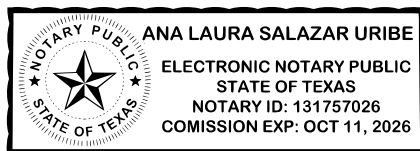
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF Texas }

COUNTY OF Harris }

The foregoing instrument was subscribed and sworn before me this date of 10/14/2025 , by Mina Ching

This notarial act was an online notarization.



Document Notarized using a Live Audio-Video Connection

(Notary Seal)

Notary's Signature Ana Laura Salazar Uribe

Registration No.: 131757026

Commission Expiration Date: October 11, 2026

