

Azure Active Directory **Multi-Factor Authentication** Deployment Plan

**How to use this plan**

This step-by-step plan walks through the implementation of Multi-Factor Authentication in a five-step process. The links below take you to each of those steps.



**1**

**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Plan)**

[Your project](#_Plan)

**3**

**[Design](#_Design)**

[Policies and integration](#_Design)

**5**

**[Manage](#_Operational_Doc)**

[Your implementation](#_Operational_Doc)



**4**

**[Implement](#_Implementation)**

[Your design](#_Implementation)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

These are general recommendations, and you should only implement if they apply to your specific enterprise needs.

Table of Contents

[Business Value of Multi-Factor Authentication 3](#_Toc515947891)

[Planning Deployment of Multi-Factor Authentication 4](#_Toc515947892)

[Stakeholders and Sign-off 4](#_Toc515947893)

[Project Scope 5](#_Toc515947894)

[Pre-requisites 5](#_Toc515947895)

[In scope 5](#_Toc515947896)

[Out of scope 5](#_Toc515947897)

[Planning Your Deployment 6](#_Toc515947898)

[General Planning 6](#_Toc515947899)

[Planning Deployment for the Azure Multi-Factor Authentication Service 7](#_Toc515947900)

[Planning Deployment for On-Premises Integration with Azure Multi-Factor Authentication 13](#_Toc515947901)

[Planning Decision Summary Sheet 15](#_Toc515947902)

[Implementing Your Solution 16](#_Toc515947903)

[Implementing the Azure Multi-Factor Authentication Service 16](#_Toc515947904)

[Implementing Azure MFA Verification Options 16](#_Toc515947905)

[Implementing Azure MFA App Passwords 16](#_Toc515947906)

[Implementing User Communication 17](#_Toc515947907)

[Implementing Named Locations or Trusted IPs 17](#_Toc515947908)

[Implementing Remember MFA 18](#_Toc515947909)

[Implementing Azure MFA Registration Policy 18](#_Toc515947910)

[Implementing Conditional Access 19](#_Toc515947911)

[Implementing On-Premises Integration with Azure Multi-Factor Authentication 20](#_Toc515947912)

[Implementing Azure MFA With Legacy Apps 20](#_Toc515947913)

[Implementing Azure MFA With On-Premises AD FS Apps 20](#_Toc515947914)

[Implementing Azure MFA With On-Premises RADIUS Apps 21](#_Toc515947915)

[Manage Your Solution 23](#_Toc515947916)

[Monitoring and Logging 23](#_Toc515947917)

[Reports for Azure MFA 23](#_Toc515947918)

[Information Logged in AD FS when Azure MFA is Used 23](#_Toc515947919)

[Maintenance Tasks 23](#_Toc515947920)

[Renew and Manage AD FS Azure MFA Certificates 23](#_Toc515947921)

[Prepare NPS for users that aren't enrolled for MFA 25](#_Toc515947922)

# Business Value of Multi-Factor Authentication

Traditional password-based authentication is not strong enough in the current security landscape. Users tend to choose bad passwords, store them in plain view or are easily tricked by social engineering attacks

Now, more than ever, users are increasingly connected. With smart phones, tablets, laptops, and PCs, users have multiple options to access their accounts and applications from anywhere and stay connected at any time

Azure Multi-Factor Authentication (MFA) is an easy to use, scalable, and reliable solution that provides a second method of authentication to protect your users. Azure MFA 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 verification methods, including phone call, text message, or mobile app verification

|  |  |
| --- | --- |
| **Figure 1** |  |
| |  |  | | --- | --- | | A picture containing clipart  Description generated with high confidence | **Easy to Use**  Azure Multi-Factor Authentication is simple to set up and use. The extra protection that comes with Azure Multi-Factor Authentication allows users to manage their own devices. Best of all, in many instances it can be set up with just a few simple clicks | | A picture containing clipart  Description generated with very high confidence | **Scalable**  Azure Multi-Factor Authentication uses 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**  Microsoft guarantees 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process verification requests for the two-step verification | |  |

# Planning Deployment of Multi-Factor Authentication

## Stakeholders and Sign-off

The following roles will be involved in delivering this project. To see a full list of responsibilities and delivery items, see [Implementation Steps and Stakeholders](#_Implementation_Steps_and)

* Action Required:
  + SO = Sign-off on this project
  + R = Review this project and provide input
  + I = Informed of this project

|  |  |  |
| --- | --- | --- |
| Name | Area | Action |
| <Enter name and email> | **IT Support Manager**  *A representative from the IT support organization who can provide input on the supportability of this change from a helpdesk perspective* | SO |
| <Enter name and email> | **Identity Architect or Azure AD Global Administrator**  *A representative from the identity management team who owns defining how this change aligns with the core identity management infrastructure in the customer’s organization* | SO |
| <Enter name and email> | **Business Owner**  *A representative colleague who can provide input on the user experience and usefulness of this change from an end-user’s perspective and owns the overall business aspect of the application, which may include managing access* | SO/I |
| <Enter name and email> | **Security Owner**  *A representative from the security team that can sign off that the plan will meet the security requirements of your organization* | SO/R |
| <Enter user groups and communications channel> | **End Users**  *All users who will be subject to the use of Multi-Factor Authentication* | I |

**Table 1**

## Project Scope

### Pre-requisites

#### Assumptions

The following are assumptions that are in place today:

* Azure AD Connect is deployed so that user identities are synchronized from the on-premises Active Directory Forest to the Azure Active Directory tenant ([Reference](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect))
* Azure Active Directory Application Proxy is deployed for scenarios where on-premises applications will be published to users for cloud access ([Reference](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy))
* Active Directory Federation Services is deployed for scenarios where the Azure Active Directory tenant is federated and a requirement for securing on-premises resources with Azure Multi-Factor Authentication is desired ([Reference](https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services))
* An existing Network Policy Server is deployed for scenarios where Azure Multi-Factor Authentication is desired for use in combination with RADIUS authentication such as VPN or Remote Desktop Gateway ([Reference](https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top))

### In scope

The following is in scope for this project:

**Enabling Azure Multi-Factor Authentication**

* Azure Multi-Factor Authentication Service Configuration
* User Communications
* Configuration of Azure Multi-Factor Authentication Registration Policy using Azure Identity Protection (optional)
* Configuration of Azure Conditional Access Policies for the enforcement of Azure Multi-Factor Authentication (optional)

### Out of scope

The following is out of scope for this project:

* Deployment of Azure AD Connect
* Assigning Licenses to Users
* Deployment of Azure Active Directory Application Proxy
* Deployment of Active Directory Federation Services
* Providing Disaster Recovery plans for Active Directory Federation Services
* Deployment of Network Policy Server and infrastructure for RADIUS authentication
* Providing Disaster Recovery plans for Network Policy Server

## Planning Your Deployment

### General Planning

#### Environments and Project Stages

Project stages depend on environments that are available. If you have a non-production Azure tenant, you can complete a proof of concept (POC) outside of your production environment if desired.

In the **Table 2**, document the Azure AD and AD environments and stages of your project

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

**Table 2**

#### Deployment Considerations

The following are deployment considerations for deploying Multi-Factor Authentication with Azure Active Directory:

* **Microsoft recommends** If you have access to Azure Active Directory Identity Protection through Azure Active Directory P2 licenses, configure a Multi-Factor registration policy through Identity Protection that enforces end-user registration for MFA. Azure Active Directory Identity Protection is only available with Azure Active Directory P2 licenses. Refer to the licensing references below.
* **Microsoft recommends** Combine Azure MFA with Azure Conditional Access so that you have greater control over the times when the challenge for a second authentication factor occurs. Implementing Azure MFA in the per-user model of enforcement leads to an “always on” implementation that may impact user productivity. See the [Azure Active Directory Conditional Access Deployment Plan](http://aka.ms/conditionalaccessdeploymentplan) for more information

#### Licenses

Azure Multi-Factor Authentication is bundled with [Azure Active Directory Premium](https://azure.microsoft.com/en-us/pricing/details/active-directory/), [Enterprise Mobility Suite](https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility), and [Enterprise Cloud Suite](https://www.microsoft.com/en-us/licensing/licensing-programs/enterprise.aspx#tab=3)

For more information, refer to the Azure Multi-Factor Authentication pricing page [here](https://azure.microsoft.com/en-au/pricing/details/multi-factor-authentication/)

**Table 3** provides an overview of the Azure Active Directory security features that work together with Multi-Factor Authentication. For a full list of license options and features, refer to the Azure Active Directory [pricing page](https://azure.microsoft.com/en-us/pricing/details/active-directory/)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Azure AD License Type | | |
|  | **FREE/BASIC** | **PREMIUM P1** | **PREMIUM P2** |
| Multi-factor Authentication | LIMITED | Requires minimum P1 | |
| Conditional Access | NOT Available | Requires minimum P1 | |
| Identity Protection |  |  | Requires P2 |

**Table 3**

### Planning Deployment for the Azure Multi-Factor Authentication Service

The decisions and activities you will need to consider for deployment of the Azure Multi-Factor Authentication Service are captured in the flow-chart shown in **Figure 2**



**Figure 2**

Before you deploy Azure MFA to your organization, you must choose the authentication methods for your users. In addition, there are other service configuration options you may need to consider, depending on whether you intend to use Azure MFA on its own or in combination with Azure Conditional Access Policies

To change Azure MFA Service Configuration –

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Users**
3. At the top of the Users blade, click **Multi-Factor Authentication**. This will open the Azure MFA management portal
4. Click **service settings**

On this page, you may modify the Azure MFA service settings (**Figure 2**, References **2.1, 2.2, 2.5** and **2.6**)

#### Planning Azure MFA Verification Options (Figure 2, Ref 2.1)

You can choose the verification methods that you wish to make available for your users. It is important to allow more than a single verification method so that users can authenticate in different scenarios

* **Microsoft recommends** You should enable "Notification through mobile app", "Call to phone", and "Verification code from mobile app"
* Push notifications through the mobile app provide the best user experience
* A voice call to phone is important because it persists through a phone handset upgrade, allowing the user to register the mobile app on the new device
* Verification code from mobile app can be used when the phone has no data connection or cellular signal

Choose your authentication methods using **Table 4**

|  |  |  |
| --- | --- | --- |
| Method | Description | Selected |
| Call to phone | Places an automated voice call. The user answers the call and presses # in the phone keypad to authenticate. The phone number is not synchronized to on-premises Active Directory |  |
| Text message to phone | Sends a text message that contains a verification code. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS. Two-way SMS means that the user must text back a particular code. Two-way SMS is deprecated and not supported after November 14, 2018. Users who are configured for two-way SMS are automatically switched to call to phone verification at that time |  |
| Notification through mobile app | Sends a push notification to your phone or registered device. The user views the notification and selects **Approve** to complete verification. The Microsoft Authenticator app is available for [Windows Phone](http://go.microsoft.com/fwlink/?Linkid=825071), [Android](http://go.microsoft.com/fwlink/?Linkid=825072), and [iOS](http://go.microsoft.com/fwlink/?Linkid=825073) |  |
| Verification code from mobile app | The Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The Microsoft Authenticator app is available for [Windows Phone](http://go.microsoft.com/fwlink/?Linkid=825071), [Android](http://go.microsoft.com/fwlink/?Linkid=825072), and [iOS](http://go.microsoft.com/fwlink/?Linkid=825073) |  |

**Table 4**

#### Planning Azure MFA App Passwords (Figure 2, Ref 2.2)

Some applications, like Office 2010 or earlier and Apple Mail for iOS versions below 11, don't support two-step verification. The apps aren't configured to accept a second verification. To use these applications, take advantage of the app passwords feature

* **Microsoft recommends** It is strongly recommended that you **do not** use Azure MFA App Passwords and that you only work with applications that use modern protocols supporting MFA

For more information about “App Passwords”, refer to guidance [here](https://docs.microsoft.com/en-au/azure/active-directory/authentication/howto-mfa-mfasettings#app-passwords)

Use **Table 5** to record your choice to allow app passwords

|  |
| --- |
| Allow App Passwords – Yes/No |
|  |

**Table 5**

#### Planning User Communication (Figure 2, Ref 2.3)

Communicate to your users the changes that will be coming. You can use the documentation [here](https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/multi-factor-authentication-end-user) to notify and inform them about Azure MFA requirements and how they should respond

You may also direct users to the [Azure MFA Proof-up](https://aka.ms/proofup) page to sign up directly

#### Planning Named Locations or Azure MFA Trusted IPs (Figure 2, Ref 2.4)

Trusted IPs under Azure MFA Service Configuration need only be configured when you are not using [Azure Conditional Access Policies](#_Planning_Azure_Conditional). The Trusted IPs feature is used by administrators of a managed or federated tenant to bypass two-step verification for users who sign in from the company intranet

Trusted IP ranges need only be defined when the Azure Active Directory tenant is managed (i.e. not federated with Active Directory Federation Services)

For more information about “Trusted IPs”, refer to guidance [here](https://docs.microsoft.com/en-au/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips)

* **Microsoft recommends** It is strongly recommended that you use Azure Conditional Access which includes the “Named Locations” feature. “Named Locations” provides the same (plus more) functionality compared with “Trusted IPs”. The use of “Named Locations” is covered under the [Azure Conditional Access Deployment Plan](http://aka.ms/conditionalaccessdeploymentplan)

Use **Table 6** to plan your use of Trusted IPs or Named Locations

|  |  |
| --- | --- |
| Design Decision | Yes/No |
| IP ranges must be defined (no AD FS) |  |
| Named Locations will be used (Conditional Access used) |  |
| Trusted IPs feature required (no Conditional Access) |  |
| **IP Range Name** | **IP Range Definition** |
| <name> | <subnet> |
| <name> | <subnet> |
| Etc. |  |

**Table 6**

#### Planning Configure Remember Multi-Factor Authentication (Figure 2, Ref 2.5)

The “remember Multi-Factor Authentication” feature allows users to bypass subsequent verifications for a specified number of days, following a successful sign-in to a device by using Multi-Factor Authentication. The feature enhances usability by minimizing the number of times a user must perform two-step verification on the same device but if an account or device is compromised, remembering Multi-Factor Authentication for trusted devices can affect security

* **Microsoft recommends** Do not use “remember Multi-Factor Authentication”. Instead use [Azure Conditional Access](http://aka.ms/conditionalaccessdeploymentplan) policies to control the requirement for an additional authentication factor

For more information about “remember multi-factor authentication”, refer to guidance [here](https://docs.microsoft.com/en-au/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication-for-trusted-devices)

Use **Table 7** to plan your use of “remember Multi-Factor Authentication”

|  |
| --- |
| Remember Multi-Factor Authentication – Yes/No |
|  |

**Table 7**

#### Planning Azure MFA Registration Policy (Figure 2, Ref 2.6)

The creation of an Azure MFA Registration Policy is only available if you have Azure Active Directory P2 licenses. When you have these licenses available and assigned to users, you may create an MFA Registration Policy via Azure Identity Protection –

1. Open the [Azure Identity Protection](https://portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview) Blade in the Azure Portal
2. Click **MFA Registration**
3. Configure MFA Registration Policy options

* **Microsoft recommends** Configure the MFA Registration Policy so that it applies to All Users, allowing access with MFA Registration required. Refer to the associated [guidance](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection#multi-factor-authentication-registration-policy)

In cases where you do not have Azure Active Directory P2 licenses and cannot create an MFA Registration Policy, you may have lingering users that have not registered for MFA. This could occur for example, if they don't use apps protected with MFA. It's important to get all users registered so that bad actors cannot guess the password of a user and register for MFA on their behalf – effectively taking control of the account.

You can work around the absence of an Azure MFA Registration Policy –

1. Create a group, add all your unregistered users to it
2. Using Azure Conditional Access, enforce MFA for this group for access to all resources. This will block access until the user registers (except from apps using legacy authentication)
3. Every night have a script re-evaluate the group membership, and remove them when they have registered. When this occurs, your other Azure Conditional Access policies will apply

You may identify registered and non-registered Azure MFA users with PowerShell commands that rely on the [MSOnline PowerShell module](https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-msonlinev1?view=azureadps-1.0) –

Registered users may be identified with

Get-MsolUser -All | where {$\_.StrongAuthenticationMethods -ne $null} | Select-Object -Property UserPrincipalName | Sort-Object userprincipalname

Non-Registered users may be identified with

Get-MsolUser -All | where {$\_.StrongAuthenticationMethods.Count -eq 0} | Select-Object -Property UserPrincipalName | Sort-Object userprincipalname

Use **Table 8** to record your use of an MFA Registration Policy

|  |  |
| --- | --- |
| Deployment Choice | Yes/No |
| Configure MFA Registration Policy |  |
| Use MFA Registration Policy Workaround |  |

**Table 8**

#### Planning Azure Conditional Access Policies (Figure 2, Ref 2.7)

Azure Conditional Access Policies should be used in conjunction with Azure MFA, but this is not their only use case. To plan the use of Azure Conditional Access Policies, refer to the [Azure Conditional Access Deployment Plan](http://aka.ms/conditionalaccessdeploymentplan)

Two examples of an Azure Conditional Access Policy that may be used with Azure MFA are shown in **Table 9**

|  |  |
| --- | --- |
| When this happens | Then do this |
| An access attempt is made:   * To all cloud apps * By Global Administrators | [Require MFA (for admin)](file:///C:\Users\markreno\Desktop\MFA%20Guide\CA%20Deployment%20Plan.docx#_MFA_for_admins) |
| An access attempt is made:   * To a specific app * By All Users and Groups | [Require MFA when not at work](file:///C:\Users\markreno\Desktop\MFA%20Guide\CA%20Deployment%20Plan.docx#_MFA_when_not) |

**Table 9**

#### Planning Azure MFA Rollout for Users (Figure 2, Ref 2.8)

Considering your communication and support capacity, determine your roll out plan for Azure MFA. The plan should include a pilot deployment followed by deployment waves that are within support capacity.

Use **Table 10** and **Table 11** to plan your rollout –

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

**Table 10**

|  |  |  |
| --- | --- | --- |
| Deployment Group | User Count | Start/Finish Date |
| Pilot Users | 100 | / |
| MFA Rollout Group 1 | 1000 | / |
| MFA Rollout Group 2 | 1000 | / |
| Etc. |  |  |

**Table 11**

Configuring users for Azure MFA directly, will result in an “always on” configuration unless they fulfil simple Azure MFA exclusion conditions configured via the Azure MFA Service Settings (see “Trusted IPs” and “Remember multi-factor authentication” above)

* **Microsoft recommends** It is preferable to use [Azure Conditional Access](http://aka.ms/conditionalaccessdeploymentplan) policies to control the requirement for an additional authentication factor

### Planning Deployment for On-Premises Integration with Azure Multi-Factor Authentication

The decisions and activities you will need to consider for integration of Azure Multi-Factor Authentication with on-premises resources are captured in the flow-chart shown in **Figure 3**



**Figure 3**

This flow-chart excludes scenarios where you have modern-auth aware (WS-Fed, SAML, OAuth, OpenID Connect) applications that are directly integrated with Azure Active Directory. Whether the app is hosted on-premises or in the cloud, if it is directly dependent upon Azure Active Directory for authentication (the app is a relying party of Azure Active Directory), it falls into the [Planning Deployment for the Azure Multi-Factor Authentication Service](#_Planning_Deployment_for) section above

#### Publishing Applications with Azure Application Proxy (Figure 3, Ref 3.1)

Applications residing on-premises that are published to your Azure Active Directory tenant via [Azure Active Directory Application Proxy](https://docs.microsoft.com/en-au/azure/active-directory/manage-apps/application-proxy) and that are configured to use Azure Active Directory pre-authentication, may take advantage of Azure Multi-Factor Authentication

These applications may be subject to Azure Conditional Access Policies that enforce Azure Multi-Factor Authentication, just like any other Azure Active Directory integrated app

Likewise, if Azure Multi-Factor Authentication is enforced for all user sign-ins, on-premises applications published with Azure Active Directory Application Proxy, will be protected

Use **Table 12** to plan your use of Azure MFA with Azure App Proxy

|  |
| --- |
| Use Multi-Factor Authentication with Application Proxy – Yes/No |
|  |

**Table 12**

#### Integrating Azure Multi-Factor Authentication with Active Directory Federation Services (Figure 3, Ref 3.2)

If your organization is federated with Azure AD, you can use Azure Multi-Factor Authentication to secure AD FS resources, both on-premises and in the cloud. Azure MFA enables you to eliminate passwords and provide a more secure way to authenticate. Starting with Windows Server 2016, you can now configure Azure MFA for primary authentication

Unlike with AD FS in Windows Server 2012 R2, the AD FS 2016 Azure MFA adapter integrates directly with Azure AD and does not require an on-premises Azure MFA server. The Azure MFA adapter is built in to Windows Server 2016, and there is no need for additional installation

There is an additional consideration when using Azure MFA with AD FS 2016 and that is when the target application may be subject to Azure Conditional Access Policy. **Table 13** illustrates this nuance

|  |  |
| --- | --- |
| Configuration Scenario | Azure Conditional Access is Available? |
| Application is a relying party to Azure AD. Azure AD is federated with AD FS 2016 | Yes |
| Application is a relying party to AD FS 2016. Azure AD may be managed or federated with AD FS 2016 | No |
| AD FS 2016 is configured to use Azure MFA as the primary authentication method | No |

**Table 13**

For more information refer to the [AD FS 2016 MFA Integration guidance](https://docs.microsoft.com/en-au/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa)

Use **Table 14** to plan your use of Azure MFA with AD FS 2016

|  |
| --- |
| Use Multi-Factor Authentication with AD FS 2016 – Yes/No |
|  |

**Table 14**

#### Integrating Azure Multi-Factor Authentication with Network Policy server (Figure 3, Ref 3.3)

The Network Policy Server (NPS) extension for Azure MFA adds cloud-based MFA capabilities to your authentication infrastructure using your existing servers. With the NPS extension, you can add phone call, text message, or phone app verification to your existing authentication flow without having to install, configure, and maintain new servers. This integration has the following limitations –

* With the PAP protocol all methods are supported
* With the CHAPv2 protocol, only authenticator app push notifications and voice call are supported
* Azure Conditional Access policies cannot be applied

The NPS extension acts as an adapter between RADIUS and cloud-based Azure MFA to provide a second factor of authentication to protect VPN or Remote Desktop Gateway connections for federated or synced users. Users that are registered for Azure MFA will be challenged for all authentication attempts

For more information refer to the [NPS MFA Integration guidance](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension)

Use **Table 15** to plan your use of Azure MFA with Network Policy Server

|  |
| --- |
| Use Multi-Factor Authentication with NPS – Yes/No |
|  |

**Table 15**

### Planning Decision Summary Sheet

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Authentication |  | | | | | |  |
| **Method** | **Description** | | | | | | **Selected** |
| Call to phone | Places an automated voice call. The user answers the call and presses # in the phone keypad to authenticate. The phone number is not synchronized to on-premises Active Directory | | | | | |  |
| Text message to phone | Sends a text message that contains a verification code. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS. Two-way SMS means that the user must text back a particular code. Two-way SMS is deprecated and not supported after November 14, 2018. Users who are configured for two-way SMS are automatically switched to call to phone verification at that time | | | | | |  |
| Notification through mobile app | Sends a push notification to your phone or registered device. The user views the notification and selects **Approve** to complete verification. The Microsoft Authenticator app is available for [Windows Phone](http://go.microsoft.com/fwlink/?Linkid=825071), [Android](http://go.microsoft.com/fwlink/?Linkid=825072), and [iOS](http://go.microsoft.com/fwlink/?Linkid=825073) | | | | | |  |
| Verification code from mobile app | The Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The Microsoft Authenticator app is available for [Windows Phone](http://go.microsoft.com/fwlink/?Linkid=825071), [Android](http://go.microsoft.com/fwlink/?Linkid=825072), and [iOS](http://go.microsoft.com/fwlink/?Linkid=825073) | | | | | |  |
| **Allow App Passwords – Yes/No** | | | | | | | |
|  | | | | | | | |
| **Design Decision** | | | | | | **Yes/No** | |
| IP ranges must be defined (no AD FS) | | | | | |  | |
| Named Locations will be used (Conditional Access used) | | | | | |  | |
| Trusted IPs feature required (no Conditional Access) | | | | | |  | |
| **IP Range Name** | | | | | | **IP Range Definition** | |
| <name> | | | | | | <subnet> | |
| <name> | | | | | | <subnet> | |
| Etc. | | | | | |  | |
| **Remember Multi-Factor Authentication – Yes/No** | | | | | | | |
|  | | | | | | | |
| **Deployment Choice** | | | | **Yes/No** | | | |
| Configure MFA Registration Policy | | | |  | | | |
| Use MFA Registration Policy Workaround | | | |  | | | |
| Environment | | **Environment URL** | | **Project stage** | | **Start/Finish date** | |
| Non-production | |  | | POC-Configuration | | / | |
|  | | POC-Testing | | / | |
| Production | |  | | Configuration | | / | |
|  | | Testing | | / | |
|  | | Pilot | | / | |
|  | | General Availability | | / | |
| **Deployment Group** | | | **User Count** | | **Start/Finish Date** | | |
| Pilot Users | | | 100 | | / | | |
| MFA Rollout Group 1 | | | 1000 | | / | | |
| MFA Rollout Group 2 | | | 1000 | | / | | |
| Etc. | | |  | |  | | |
| **Use Multi-Factor Authentication with Application Proxy – Yes/No** | | | | | | | |
|  | | | | | | | |
| **Use Multi-Factor Authentication with AD FS 2016 – Yes/No** | | | | | | | |
|  | | | | | | | |
| **Use Multi-Factor Authentication with NPS – Yes/No** | | | | | | | |
|  | | | | | | | |

# Implementing Your Solution

## Implementing the Azure Multi-Factor Authentication Service

### Implementing Azure MFA Verification Options

To choose Azure MFA Verification Options –

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Users**
3. At the top of the Users blade, click **Multi-Factor Authentication**. This will open the Azure MFA management portal
4. Click **service settings**
5. Scroll to **verification options** and select the Azure MFA verification options you wish to use
6. Click **save**

* **Microsoft recommends** You should enable "Notification through mobile app", "Call to phone", and "Verification code from mobile app"
* Push notifications through the mobile app provide the best user experience
* A voice call to phone is important because it persists through a phone handset upgrade, allowing the user to register the mobile app on the new device
* Verification code from mobile app can be used when the phone has no data connection or cellular signal

### Implementing Azure MFA App Passwords

To implement Azure MFA App Passwords –

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Users**
3. At the top of the Users blade, click **Multi-Factor Authentication**. This will open the Azure MFA management portal
4. Click **service settings**
5. Scroll to **app passwords** and select the app passwords option you wish to use
6. Click **save**

* **Microsoft recommends** It is strongly recommended that you **do not** use Azure MFA App Passwords and that you only work with applications that use modern protocols supporting MFA

### Implementing User Communication

To implement user communication for Azure MFA –

1. Identify a standard user communication method used by your organization. Examples may be
   1. Email
   2. Face-to-face training
   3. Recorded web session
   4. Etc.
2. Inform users about the authentication changes that are coming and what they will mean for the user – the actions they will need to take

Microsoft provides some documentation that you can use to notify and inform users about Azure MFA requirements and how they should respond. This documentation may be found [here](https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/multi-factor-authentication-end-user).

You may also direct users to the [Azure MFA Proof-up](https://aka.ms/proofup) page to sign up directly

### Implementing Named Locations or Trusted IPs

* **Microsoft recommends** It is strongly recommended that you use Azure Conditional Access which includes the “Named Locations” feature. “Named Locations” provides the same (plus more) functionality compared with “Trusted IPs”.

To implement Named Locations –

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Conditional Access**
3. Click **Named Locations**
4. Click **+New Location**
5. In the **Name** field, provide a meaningful name
6. Select whether you are defining the location using **IP ranges** or **Countries/Regions**
7. If using **IP Ranges**
   1. Decide whether to mark the location as **Trusted**. Signing in from a trusted location lowers a user's sign-in risk. Only mark this location as trusted if you know the IP ranges entered are established and credible in your organization
   2. Specify the **IP Ranges**
8. If using **Countries/Regions**
   1. Expand the drop-down menu and select the countries or regions you wish to define for this named location
   2. Decide whether to **Include unknown areas**. Unknown areas are IP addresses that can't be mapped to a country/region
9. Click **Create**

The use of “Named Locations” within Conditional Access Policies is covered under the [Azure Conditional Access Deployment Plan](http://aka.ms/conditionalaccessdeploymentplan)

To implement Azure MFA Trusted IPs –

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Users**
3. At the top of the Users blade, click **Multi-Factor Authentication**. This will open the Azure MFA management portal
4. Click **service settings**
5. Scroll to **trusted ips**
6. If your Azure Active Directory tenant is federated with AD FS, decide whether to select **Skip multi-factor authentication for requests from federated users on my intranet**
7. Define trusted ip ranges under **Skip multi-factor authentication for requests from following range of IP subnets**
8. Click **save**

### Implementing Remember MFA

To implement Remember MFA

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Users**
3. At the top of the Users blade, click **Multi-Factor Authentication**. This will open the Azure MFA management portal
4. Click **service settings**
5. Scroll to **remember multi-factor authentication**
6. Click **Allow users to remember multi-factor authentication on devices they trust**
7. Configure **Days before a device must re-authenticate (1-60)** to the number of days you wish to set

* **Microsoft recommends** Do not use “remember Multi-Factor Authentication”. Instead use [Azure Conditional Access](http://aka.ms/conditionalaccessdeploymentplan) policies to control the requirement for an additional authentication factor

### Implementing Azure MFA Registration Policy

To enable an Azure MFA Registration Policy, you must have Azure Active Directory Premium P2 licenses for users of the service.

To configure an Azure MFA Registration Policy –

1. Open the [Azure Identity Protection](https://portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview) Blade in the Azure Portal
2. Click **MFA Registration**
3. Configure MFA Registration Policy options

* **Microsoft recommends** Configure the MFA Registration Policy so that it applies to All Users, allowing access with MFA Registration required. Refer to the associated [guidance](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection#multi-factor-authentication-registration-policy)

If you do not have Azure Active Directory Premium P2 licenses for your users and cannot create an Azure MFA Registration Policy –

1. Create a group, add all your unregistered users to it
2. Using Azure Conditional Access, enforce MFA for this group for access to all resources. This will block access until the user registers (except from apps using legacy authentication)
3. Every night have a script re-evaluate the group membership, and remove them when they have registered. When this occurs, your other Azure Conditional Access policies will apply

You may identify registered and non-registered Azure MFA users with PowerShell commands that rely on the [MSOnline PowerShell module](https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-msonlinev1?view=azureadps-1.0) –

Registered users may be identified with

Get-MsolUser -All | where {$\_.StrongAuthenticationMethods -ne $null} | Select-Object -Property UserPrincipalName | Sort-Object userprincipalname

Non-Registered users may be identified with

Get-MsolUser -All | where {$\_.StrongAuthenticationMethods.Count -eq 0} | Select-Object -Property UserPrincipalName | Sort-Object userprincipalname

### Implementing Conditional Access

To implement Azure Active Directory Conditional Access, refer to the separate document entitled [Azure Active Directory Conditional Access Deployment Plan](http://aka.ms/conditionalaccessdeploymentplan)

## Implementing On-Premises Integration with Azure Multi-Factor Authentication

### Implementing Azure MFA With Legacy Apps

Applications residing on-premises that are published to your Azure Active Directory tenant via [Azure Active Directory Application Proxy](https://docs.microsoft.com/en-au/azure/active-directory/manage-apps/application-proxy) and that are configured to use Azure Active Directory pre-authentication, may take advantage of Azure Multi-Factor Authentication

These applications may be subject to Azure Conditional Access Policies that enforce Azure Multi-Factor Authentication, just like any other Azure Active Directory integrated app

Likewise, if Azure Multi-Factor Authentication is enforced for all user sign-ins, on-premises applications published with Azure Active Directory Application Proxy, will be protected

### Implementing Azure MFA With On-Premises AD FS Apps

#### Integrate Azure MFA with AD FS 2016

To complete configuration for Azure MFA for AD FS 2016, you need to configure ***each*** AD FS server using the steps described

1. Open an elevated **PowerShell** prompt
2. Ensure you have the **MSOnline** PowerShell module installed. If you do not, execute

Install-Module MSOnline

1. Execute

$certbase64 = New-AdfsAzureMfaTenantCertificate -TenantID <tenantID>

where <tenantID> is the .onmicrosoft.com name of your Azure Active Directory tenant

1. Execute

Connect-MsolService

Provide global admin credentials for your Azure Active Directory tenant

1. Execute

New-MsolServicePrincipalCredential -AppPrincipalId 981f26a1-7f43-403b-a875-f8b09b8cd720 -Type asymmetric -Usage verify -Value $certBase64

The next step is only executed on one AD FS server in the farm. If the AD FS farm uses SQL server as the configuration store, you may choose any AD FS server. If the AD FS farm uses WID as the configuration store, you must choose the primary AD FS server in the farm

1. Execute

Set-AdfsAzureMfaTenant -TenantId <tenant ID> -ClientId 981f26a1-7f43-403b-a875-f8b09b8cd720

where <tenantID> is the .onmicrosoft.com name of your Azure Active Directory tenant

The final step is to restart the AD FS service on all AD FS servers in the farm. This may be done using PowerShell –

1. Execute

Restart-Service adfssrv

#### Implementing Azure MFA as the Second Factor in AD FS 2016

To implement Azure MFA as the Second Factor in AD FS 2016 –

1. Open the **AD FS management console** (on the primary AD FS server if your farm uses WID as the configuration store)
2. In the left-hand pane, expand **Service**
3. Under Service, select **Authentication Methods**
4. In the center-pane, under Multi-factor Authentication Methods, click **Edit**
5. Enable **Azure MFA**
6. Click **OK**

#### Implementing Azure MFA as the Primary Factor in AD FS 2016

To implement Azure MFA as the Primary Factor in AD FS 2016 –

1. Open the **AD FS management console** (on the primary AD FS server if your farm uses WID as the configuration store)
2. In the left-hand pane, expand **Service**
3. Under Service, select **Authentication Methods**
4. In the center-pane, under Primary Authentication Methods, click **Edit**
5. Enable **Azure MFA**
6. Click **OK**

For more information, refer to the [Microsoft Docs](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa) page

### Implementing Azure MFA With On-Premises RADIUS Apps

#### Prepare for Deployment of the Azure MFA Extension

Everyone using the NPS extension must be synced to Azure Active Directory using Azure AD Connect and must be registered for MFA. For the purposes of this document, it is assumed that you have done this.

When you install the Azure MFA extension for NPS, you need the directory ID and admin credentials for your Azure AD tenant. You can find your directory ID. To collect this ID –

1. Open the [Azure Active Directory](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) blade in the Azure Portal
2. Click **Properties**
3. Click the copy icon next to **Directory ID** to copy the value to the clipboard
4. Save the Directory ID for later

#### Implement Your NPS Server

For the purposes of this document, it is assumed that you have an NPS instance deployed and in use already. If you are setting the NPS instance up from scratch, refer to the [Microsoft Docs](https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top) page and the [Azure MFA Extension for NPS](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension) page. At a high level, these steps are –

1. Deploy NPS
2. Configure your RADIUS apps to use NPS for authentication (for example, VPN or Remote Desktop Gateway)
3. Sync your users to the cloud
4. Determine which Azure MFA Authentication Methods you can use. This is dependent upon two factors
   1. The password encryption algorithm used between the RADIUS client (VPN, Netscaler server, or other) and the NPS servers.
      * PAP supports all the authentication methods of Azure MFA in the cloud: phone call, one-way text message, mobile app notification, and mobile app verification code.
      * CHAPV2 and EAP support phone call and mobile app notification.
   2. The input methods that the client application (VPN, Netscaler server, or other) can handle. For example, does the VPN client have some means to allow the user to type in a verification code from a text or mobile app?
5. Register your users for Azure MFA

#### Implement the Azure MFA NPS Extension

To implement the Azure MFA NPS Extension –

1. [Download the NPS Extension](https://aka.ms/npsmfa) from the Microsoft Download Center
2. Copy the binary to the Network Policy Server you want to configure
3. Run setup.exe and follow the installation instructions

If you encounter errors, double-check that the following two libraries are installed –

[Visual C++ Redistributable Packages for Visual Studio 2013 (X64)](https://www.microsoft.com/download/details.aspx?id=40784)

[Microsoft Azure Active Directory Module for Windows PowerShell version 1.1.166.0](https://www.powershellgallery.com/packages/MSOnline/1.1.166.0)

The installer creates a PowerShell script in this location: C:\Program Files\Microsoft\AzureMfa\Config (where C:\ is your installation drive)

1. Open an elevated **PowerShell** prompt
2. Execute

cd "C:\Program Files\Microsoft\AzureMfa\Config"

1. Execute

.\AzureMfaNpsExtnConfigSetup.ps1

1. When prompted, sign in as your Azure Active Directory tenant, global administrator
2. When prompted, provide the tenant ID (Directory ID) recorded earlier
3. When prompted, restart the NPS server
4. If you have a load-balanced NPS farm, repeat these steps on all NPS farm instances

# Manage Your Solution

## Monitoring and Logging

### Reports for Azure MFA

Azure Multi-Factor Authentication provides several reports that can be used by you and your organization accessible through the Azure portal. The following table lists the available reports –

|  |  |  |
| --- | --- | --- |
| Report | Location | Description |
| Blocked User History | Azure AD > MFA Server > Block/unblock users | Shows the history of requests to block or unblock users. |
| Usage and fraud alerts | Azure AD > Sign-ins | Provides information on overall usage, user summary, and user details; as well as a history of fraud alerts submitted during the date range specified. |
| Usage for on-premises components | Azure AD > MFA Server > Activity Report | Provides information on overall usage for MFA through the NPS extension, and AD FS. |
| Bypassed User History | Azure AD > MFA Server > One-time bypass | Provides a history of requests to bypass Multi-Factor Authentication for a user. |

**Table 16**

### Information Logged in AD FS when Azure MFA is Used

Standard AD FS 2016 logging in both the Windows Security Log and the AD FS Admin log, contains information about authentication requests and their success or failure. Event log data within these events will indicate whether Azure MFA was used. For example, an AD FS Auditing Event ID 1200 may contain –

<MfaPerformed>true</MfaPerformed>

<MfaMethod>MFA</MfaMethod>

## Maintenance Tasks

### Renew and Manage AD FS Azure MFA Certificates

The following guidance takes you through how to manage the Azure MFA certificates on your AD FS servers. By default, when you configure AD FS with Azure MFA, the certificates generated via the New-AdfsAzureMfaTenantCertificate PowerShell cmdlet are valid for 2 years. To determine how close to expiration your certificates are, and then to renew and install new certificates, use the following procedure.

#### Assess AD FS Azure MFA certificate expiration date

On each AD FS server, in the local computer My store, there will be a self-signed certificate with “OU=Microsoft AD FS Azure MFA” in the Issuer and Subject. This is the Azure MFA certificate. Check the validity period of this certificate on each AD FS server to determine the expiration date.

#### Create new AD FS Azure MFA Certificate on each AD FS server

If the validity period of your certificates is nearing its end, start the renewal process by generating a new Azure MFA certificate on each AD FS server –

1. Open an elevated **PowerShell** prompt
2. Ensure you have the **MSOnline** PowerShell module installed. If you do not, execute

Install-Module MSOnline

1. Execute

$newcert = New-AdfsAzureMfaTenantCertificate -TenantId <tenantID> -Renew $true

where <tenantID> is the .onmicrosoft.com name of your Azure Active Directory tenant

1. Execute

Connect-MsolService

Provide global admin credentials for your Azure Active Directory tenant

1. Execute

New-MsolServicePrincipalCredential -AppPrincipalId 981f26a1-7f43-403b-a875-f8b09b8cd720 -Type asymmetric -Usage verify -Value $newcert

#### Verify that the new certificate(s) will be used for Azure MFA

Once the new certificate(s) become valid, AD FS will pick them up and start using each respective certificate for Azure MFA within a few hours to a day. Once this occurs, on each server you will see an event logged in the AD FS Admin event log with the following information –

Log Name: AD FS/Admin  
Source: AD FS  
Date: 2/27/2018 7:33:31 PM  
Event ID: 547  
Task Category: None  
Level: Information  
Keywords: AD FS  
User: DOMAIN\adfssvc  
Computer: ADFS.domain.contoso.com  
Description: The tenant certificate for Azure MFA has been renewed.

TenantId: contoso.onmicrosoft.com.  
Old thumbprint: 7CC103D60967318A11D8C51C289EF85214D9FC63.  
Old expiration date: 9/15/2019 9:43:17 PM.  
New thumbprint: 8110D7415744C9D4D5A4A6309499F7B48B5F3CCF.  
New expiration date: 2/27/2020 2:16:07 AM.

### Prepare NPS for users that aren't enrolled for MFA

If you have users that aren't enrolled for MFA, you can determine what happens when they try to authenticate. Use the registry setting REQUIRE\_USER\_MATCH in the registry path HKLM\Software\Microsoft\AzureMFA to control the feature behavior. This setting has a single configuration option –

|  |  |  |
| --- | --- | --- |
| Key | Value | Default |
| REQUIRE\_USER\_MATCH | TRUE/FALSE | Not set (equivalent to TRUE) |

**Table 16**

The purpose of this setting is to determine what to do when a user is not enrolled for MFA. When the key does not exist, is not set, or is set to TRUE, and the user is not enrolled, then the extension fails the MFA challenge. When the key is set to FALSE and the user is not enrolled, authentication proceeds without performing MFA. If a user is enrolled in MFA, they must authenticate with MFA even if REQUIRE\_USER\_MATCH is set to FALSE.

You can choose to create this key and set it to FALSE while your users are onboarding and may not all be enrolled for Azure MFA yet. However, since setting the key permits users that aren't enrolled for MFA to sign in, you should remove this key before going to production.

**IMPORTANT NOTICES**

© 2018 Microsoft Corporation.  All rights reserved.  This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.   
Some examples are for illustration only and are fictitious. No real association is intended or inferred.   
   
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes

**CONFIDENTIALITY STATEMENT**

It is understood and agreed to that project plan may provide certain information that is and must be kept confidential. To ensure the protection of such information you should not disclose any part of this plan to anyone unless required to do so by law.