Leverage Azure Multi-Factor Authentication with Azure AD

Overview Technical Article

Microsoft France

Published: December 2013 (Updated: June 2015)

Version: 1.0b

Author: Philippe Beraud (Microsoft France)

Contributors/Reviewers: Arnaud Jumelet, Jean-Yves Grasset (Microsoft France)

For the latest information on Azure Multi-Factor Authentication, please see

azure.microsoft.com/en-us/services/multi-factor-authentication

Copyright © 2015 [Microsoft Corporation](http://www.microsoft.com). All rights reserved.

Abstract: With escalating IT security threats and a growing number of users, Software-as-a-Service (SaaS) applications, and devices, multi-factor authentication is becoming the new standard for securing access and how businesses ensure trust in a multi-device, mobile, cloud world.  Passwords not enough strong can be easily compromised, and the consumerization of IT along with the Bring-Your-Own-Device (BYOD) trend have only increased the scope of vulnerability. Regulatory agencies agree and have mandated its use across a broad range of industries.

Azure Multi-Factor Authentication (Azure MFA) helps reduce organizational risk and enable regulatory compliance by providing an extra layer of authentication in addition to a user’s account credentials. For that purpose, it leverages for additional authentication a convenient form factor that the users already have (and care about): their phone. During sign in, users must also authenticate using the mobile app or by responding to an automated phone call or text message before access is granted. An attacker would need to know the user’s password and have in their possession of the user’s phone to sign in. As a solution for both cloud-based and on-premises applications, Azure MFA can notably be used as part of the Azure Active Directory (Azure AD) authentication.

Table of Contents

[Introduction 3](#_Toc403575126)

[Objectives of this paper 5](#_Toc403575127)

[Non-objectives of this paper 7](#_Toc403575128)

[Organization of this paper 9](#_Toc403575129)

[About the audience 9](#_Toc403575130)

[Strengthening the authentication with Azure Multi-Factor Authentication 10](#_Toc403575131)

[What is multi-factor authentication? 10](#_Toc403575132)

[What is Azure Multi-Factor Authentication? 10](#_Toc403575133)

[How it works? 11](#_Toc403575134)

[Configuring Azure AD for Multi-Factor Authentication 14](#_Toc403575135)

[Adding Multi-Factor Authentication to Azure AD 15](#_Toc403575136)

[Enabling users for Multi-Factor Authentication 18](#_Toc403575137)

[Using Multi-Factor Authentication with Azure AD 22](#_Toc403575138)

[Configuring the Multi-Factor Authentication mobile application 25](#_Toc403575139)

[Managing the user settings 29](#_Toc403575140)

[Configuring advanced settings and reports 33](#_Toc403575141)

[Creating and administering a fraud report 33](#_Toc403575142)

[Viewing Multi-Factor Authentication settings and reports 36](#_Toc403575143)

# Introduction

Today many organizations use on-premises multi-factor authentication systems to protect mission critical data in their file servers and their critical Line of Business (LOB) applications. As these workloads (or parts of them) move to the cloud (at least in a hybrid manner, see whitepaper [Enabling Hybrid Cloud today with Microsoft Technologies](http://www.microsoft.com/en-us/download/details.aspx?id=39052)[[1]](#footnote-1)), they need an effective and easy-to-use solution in the Cloud for protecting:

* That data in the Microsoft services, such Office 365, Intune, and Dynamics CRM Online, or other Software-as-a-Service (SaaS) they’ve subscribed to,
* The custom cloud-based LOB applications – on Azure or in other clouds -,
* And the [modern business applications](http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx)[[2]](#footnote-2) they’ve created.

Passwords in use that are often not enough strong and the consumerization of IT has only even increased the scope of vulnerability.

Multi-factor authentication is becoming the new standard for securing access and how businesses ensure trust in a multi-device, mobile, cloud world.

Note Not only do the above organizations need multi-factor authentication for their employees, but many of them are also increasingly building cloud-based applications for consumers and citizens that require multi-factor authentication to ensure a high level of security.  These B2C scenarios are growing rapidly and require easy end-user technology.

Furthermore, multi-factor authentication is no longer optional for many of the above organizations; many are required by various governing or regulatory agencies to strongly authenticate access to sensitive data and applications across a broad range of industries.

In such a landscape, phone-based authentication constitutes a very compelling technical approach for multi-factor authentication as it provides enhanced security for businesses and consumers in a convenient form factor that the user already has: their phone.

[Azure Multi-Factor Authentication (Azure MFA)](http://azure.microsoft.com/en-us/services/multi-factor-authentication/)[[3]](#footnote-3) addresses user demand for a simple sign-in process while also helping address the organization's security and compliance standards. The service offers enhanced protection from malware threats, and real-time alerts notify your IT department of potentially compromised account credentials.

Azure MFA helps to deliver strong security via a range of easy authentication options. Thus, in addition to entering a username and password during sign in, enabled users are also required to authenticate with a mobile app on their mobile device or via an automated phone call or a text message, allowing these users to choose the method that works best for them. Consequently, in order for an attacker to gain access to a user’s account, they would need to know the user’s login credentials AND be in possession of the user’s phone. Furthermore, support for the above multiple methods enables to support more scenarios such as offline (no carrier) scenarios.

Azure MFA exists in different flavors:

* Azure MFA stand-alone.
* Included in Azure AD Premium (see below).
* A subset of Azure MFA functionality included in Office 365 for both administrators and users.
* Free for Azure administrators.

Whilst Azure MFA is powered by a cloud service, the stand-alone version and well as the one included in Azure AD Premium support on-premises, cloud, and hybrid scenarios. The following solutions are indeed available for use with Azure MFA:

* **Adding Multi-Factor Authentication to Azure AD**. Azure MFA works with any applications that use the Azure AD directory tenants. As such, Azure MFA can be rapidly enabled for Azure AD identities to help secure access:
* The Azure management portal,
* Microsoft Online Services like Office 365, Intune, and Dynamics CRM Online, etc.
* Any custom LOB, third-party multitenant cloud-based, or modern business applications that integrate with Azure AD for authentication,
* As well as thousands of cloud SaaS applications like Box, GoToMeeting, Salesforce.com and others, thanks to the application gallery of the [Application Access Enhancements for Azure AD](http://technet.microsoft.com/en-us/library/dn308588.aspx)[[4]](#footnote-4) feature.

Users will be prompted to set up additional verification the next time they sign in.

Note For more information, see the Microsoft TechNet article [Adding Multi-Factor Authentication to Azure Active Directory](http://technet.microsoft.com/en-us/library/dn249466.aspx)[[5]](#footnote-5).

* **Enabling Multi-Factor Authentication for on-premises applications and Windows Server**. The Multi-Factor Authentication Server works out-of-the-box with a wide range of on-premises applications, such as remote access VPNs, web applications, virtual desktops, single sign-on systems and much more. This includes:
* Microsoft products and technologies like Microsoft VPN/RRAS, Remote Desktop Services and Remote Desktop Gateway, Universal Access Gateway, SharePoint, Outlook Web Access, etc.
* As well as third party VPNs and virtual desktop system.

Multi-Factor Authentication Server allows the administrator integrate with IIS authentication to secure Microsoft IIS web applications, RADIUS authentication, LDAP authentication, and Windows authentication.

Multi-Factor Authentication Server can be run on-premises on your existing hardware - as a virtual machine (VM) or not -, or in the cloud for instance as an Azure Virtual Machine. Multiple, redundant servers can be configured for high availability and fail-over.

Note For more information, see Microsoft TechNet article [Enabling Multi-Factor Authentication for On-Premises Applications and Windows Server](http://technet.microsoft.com/en-us/library/dn249467.aspx)[[6]](#footnote-6).

* **Building Multi-Factor Authentication into custom applications**. A Software Development Kit (SDK) is available for use for direct integration with custom cloud-based and on-premises applications. It enables to build Multi-Factor Authentication phone call and text message verification into the application’s sign-in or transaction processes and leverage the application’s existing user database.

Note For more information, see Microsoft TechNet article [Building Multi-Factor Authentication into Custom Apps (SDK)](http://technet.microsoft.com/en-us/library/dn249464.aspx)[[7]](#footnote-7).

## Objectives of this paper

As an addition to the white-paper [Active Directory from on-premises to the Cloud](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[8]](#footnote-8), this paper focusses on the first above solution and, as such, aims at describing how to enable, configure and use Azure MFA for Azure AD, so that Azure AD users will be prompted to set up additional verification the next time they sign in.

To enable Azure MFA, organizations start by signing up for Azure, if they have not done so already. From the Azure management portal, they create a MFA provider, linking it to an Azure AD directory tenant in our context. Organizations can then enable users in that directory tenant for multi-factor authentication. Organizations can then select the Manage option to access additional Multi-Factor Authentication configuration options and reporting.

**Built on existing Microsoft documentation and knowledge base articles, this document covers all of the above steps and provide additional guidance if any.**

Note For additional information, see Microsoft TechNet article [Using Multi-Factor Authentication with Azure AD](http://technet.microsoft.com/en-us/library/jj713614.aspx)[[9]](#footnote-9).

**The aforementioned steps not only apply for cloud users in Azure AD but also for federated users for the following two specific scenarios**:

1. The first factor of authentication is performed on-premises and the second factor is a phone-based method carried out by the synchronized identity in the cloud.

Note This corresponds to **the directory synchronization with single sign-on (SSO) scenario**to provide users with the most seamless authentication experience as they access Microsoft cloud services and/or other cloud-based applications while logged on to the corporate network. For additional information, see Microsoft TechNet article [Directory Sync with Single Sign-On Scenario](http://technet.microsoft.com/en-us/library/dn441213.aspx)[[10]](#footnote-10).

Important note This applies only to browser-based applications. Multi-Factor Authentication is not supported by non-browser applications, excepted with Office 365 ProPlus/Office 2013 applications with modern authentication enabled. Modern authentication is available to any customer running the March 2015 or later update for Office 2013 but is disabled by default. For additional information on these update, see the blog post [Office 2013 updated authentication enabling Multi-Factor Authentication and SAML identity providers](http://blogs.office.com/2014/11/12/office-2013-updated-authentication-enabling-multi-factor-authentication-saml-identity-providers/)[[11]](#footnote-11).

For the other browser-based applications, an app password must be created. An app password is a password that allows to by-pass the Multi-Factor Authentication (more information on this later in this document). Eventually, app passwords are only available to users that do not have administrative privileges.

-or-

1. The two factors of authentication are performed on-premises, with a second factor of your choice (such as a smartcard).

As a result of the on-premises authentication, Active Directory Federation Services (AD FS)[[12]](#footnote-12) or other supported third-party security token services (STS)[[13]](#footnote-13) [[14]](#footnote-14) must send a claim of type “*http://schemas.microsoft.com/claims/authnmethodsreferences*” with the value “*http://schemas.microsoft.com/claims/multipleauthn*”. Thus, the organizational id will not trigger Azure MFA for the user because it has already received the above so-called MFA claim from on-premises identity infrastructure.

Note For additional information, see Microsoft TechNet article [Azure Multi-Factor Authentication options for Federated Users](http://technet.microsoft.com/en-us/library/dn394284.aspx)[[15]](#footnote-15).

## Non-objectives of this paper

This document doesn’t discuss how to configure Azure MFA for federated identities along with the Multi-Factor Authentication Server on-premises to secure both cloud and on-premises resources.

This integration scenario implies to configure the Multi-Factor Authentication Server - available for download on the Multi-Factor Authentication management portal - to work with Active Directory Federation Services (AD FS) or other supported on-premises third-party security token services (STS) so that Multi-Factor Authentication is triggered on-premises (or in a Infrastructure-as-a-Service (IaaS) cloud environment such as Azure as per [Office 365 Adapter: Deploying Office 365 Single Sign-On using Azure](http://www.microsoft.com/en-us/download/details.aspx?id=38845)[[16]](#footnote-16) whitepaper.

Note Such an integration is natively supported by AD FS but differs in terms of integration path depending on the version of AD FS. More specifically, for additional information on using the Multi-Factor Authentication Server with AD FS 2.x, see Microsoft TechNet article [Using Multi-Factor Authentication with Active Directory Federation Services](http://technet.microsoft.com/en-us/library/dn394281.aspx)[[17]](#footnote-17). For information on using Multi-Factor Authentication Server with AD FS for Windows Server 2012 R2, see Microsoft TechNet article [Walkthrough Guide: Manage Risk with Additional Multi-Factor Authentication for Sensitive Applications](http://technet.microsoft.com/en-us/library/dn280946.aspx)[[18]](#footnote-18).

For the other supported on-premises third-party security token services (STS), the aforementioned Software Development Kit (SDK) is available for use with custom applications and directories.

Beyond this integration, this scenario additionally implies directory synchronization between the on-premises identity infrastructure (based on Windows Server Active Directory (AD) or on other (LDAP-based) directories) and the Multi-Factor Authentication Server to streamline user management and automated provisioning.

This also supposes to deploy:

* The on-premises Multi-Factor Authentication Users portal, which allows users to enroll in Multi-Factor Authentication and maintain their accounts.

Note For additional information, see Microsoft TechNet article [Installing the Azure Multi-Factor Authentication Users Portal](http://technet.microsoft.com/en-us/library/dn394290.aspx)[[19]](#footnote-19).

* And optionally the Multi-Factor Authentication Server mobile app web service, which is used in the Multi-Factor Authentication mobile app activation process. The Multi-Factor Authentication App offers an additional out-of-band authentication option (see later in this document).

Note For additional information, see Microsoft TechNet article  [Deploying the Azure Multi-Factor Authentication Server Mobile App Web Service](http://technet.microsoft.com/en-us/library/dn394277.aspx)[[20]](#footnote-20).

With all of the above, the enrolled users can use their on-premises corporate credentials (user name and password) and their existing phone for additional authentication to access Azure AD and any cloud-based application that is integrated into Azure AD as well as their existing on-premises resources.

This scenario is no longer discussed as part of this document. It is rather covered in detail in the whitepaper [Leverage Azure Multi-Factor Authentication Server for Azure AD single sign-on with AD FS](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[21]](#footnote-21).

As already mentioned, the Multi-Factor Authentication Server also works out-of-the-box with a wide range of on-premises applications, such as remote access VPNs, web applications, virtual desktops, single sign-on systems and much more. Those scenarios are not discussed in this document either.

## Organization of this paper

To cover the aforementioned objectives, this document is organized by themes which are covered in the following sections:

* Strengthening the authentication with Azure Multi-Factor Authentication.
* Configuring Azure AD for Multi-Factor Authentication.
* Configuring advanced settings and reports.

## About the audience

This document is intended for system architects and IT professionals who are interested in understanding how to enable and configure Azure MFA for Azure AD users to help secure access the Azure management portal, Microsoft services like Office 365, Intune, and Dynamics CRM Online, as well as any cloud-based applications that use/integrate with Azure AD.

# Strengthening the authentication with Azure Multi-Factor Authentication

## What is multi-factor authentication?

Multi-factor authentication, also commonly referred to as two-factor authentication, is a best practice for securing user access. It works by requiring any two or more of the following authentication factor:

* **A knowledge factor**: *something only you know* (typically a password or a PIN).
* **A possession factor**: *something only you have* (a trusted device that is not easily duplicated).
* **An inherence factor**: *something only you are* (biometrics).

After presentation, each required factor must be verified and validated for authentication to occur. Multi-factor authentication is stronger when factors are verified using distinct (or out-of-band) channels.

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. On the other hand, if the user happens to lose the device, the finder of that device won’t be able to use it unless he or she also knows the user’s password.

The most common multi-factor methods include hardware tokens like RSA SecurID, certificates, smartcards, and increasingly phone-based authentication methods, which leverage the user’s telephone as the trusted device for the second factor of authentication.

## What is Azure Multi-Factor Authentication?

As already introduced, Azure MFA is, as its name indicates, an Azure service that helps safeguard access to data and applications by strengthening traditional sign-in approaches. In terms of applications, the service supports both cloud applications that use or integrate with Azure AD as well as on-premises applications using the Multi-Factor Authentication Server.

Generally available and fully backed by a [Service Level Agreement (SLA)](http://go.microsoft.com/fwlink/?linkid=313266&clcid=0x409)[[22]](#footnote-22), the service is trusted by thousands of enterprise customers, healthcare organizations, banking and financial services companies, as well as government agencies at the state, local and federal level. The service authenticates millions of logins and financial transactions around the globe each month. It is battle-tested and enterprise-ready.

Note Azure MFA is powered by the market-leading PhoneFactor service acquired by Microsoft in October 2012[[23]](#footnote-23). With some minor exceptions, all of the features and capabilities offered by PhoneFactor are included in the Multi-Factor Authentication service, including the on-premises PhoneFactor Agent, which has been renamed the Multi-Factor Authentication Server.

Traditionally, strong authentication has been time consuming to deploy and has required significant ongoing resources to support. And it was a hassle for users who had to carry extra devices or whose access was limited to computers with smartcard readers or that had certificates installed.

With Azure MFA and the user’s telephone as the trusted device for a second or an additional factor of authentication:

* There are no devices or certificates to purchase, provision, and maintain. It works with the user’s existing landline phone or mobile device.
* The authentication process is so simple. It takes just seconds and no special training is required.
* Unlike hardware tokens, users replace their own lost or broken phones.
* Users manage their own authentication methods and phone numbers, eliminating calls to your help desk for basic changes.
* Azure MFA is built into Azure AD, so user management is centralized (for cloud users as well as for federated users in some specific scenarios).
* Enrollment is fully automated. With Azure AD cloud identities, users are prompted to complete set up the next time they sign in. This allows for rapid deployment to large numbers of geographically dispersed users.
* Users get easy, anywhere access and you get a solution that’s easy to manage.

Note For additional information, see Microsoft TechNet article [Azure Multi-Factor Authentication](http://technet.microsoft.com/en-us/library/dn249471.aspx)[[24]](#footnote-24).

## How it works?

Azure MFA offers the additional security you demand using the phones your users already carry.

Multiple phone-based authentication methods are available, allowing users to choose the one that works best for them, and, support for multiple methods ensures additional authentication is always available:

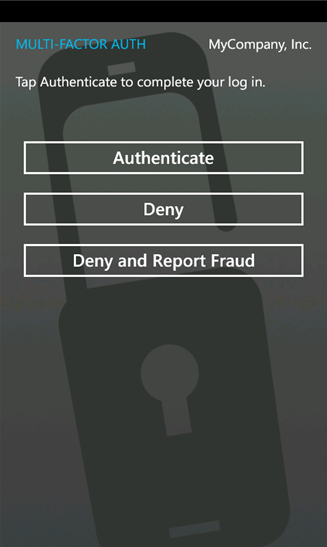
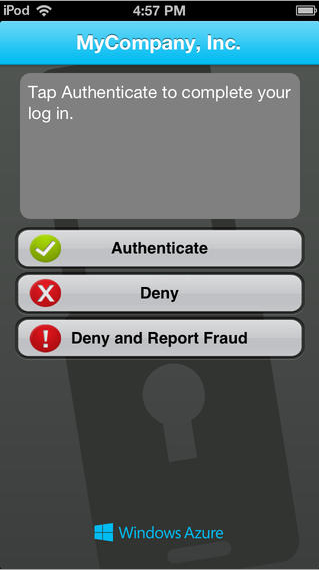
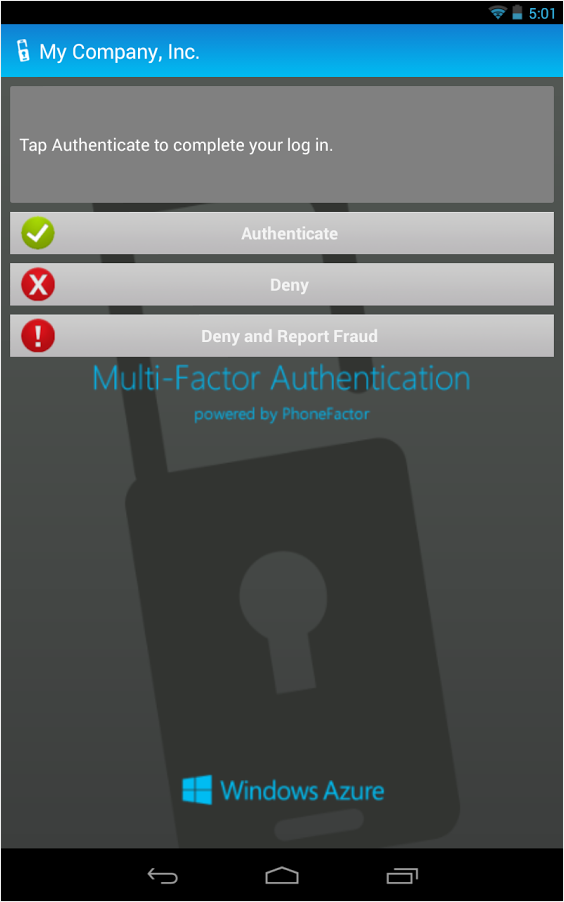
* **Multi-Factor Auth apps** are available for [Windows Phone](http://www.windowsphone.com/en-us/store/app/phonefactor/0a9691de-c0a1-44ee-ab96-6807f8322bd1)[[25]](#footnote-25), [iOS](ttps://itunes.apple.com/us/app/phonefactor/id475844606?mt=8)[[26]](#footnote-26) phones and tablets, and [Android](https://play.google.com/store/apps/details?id=com.phonefactor.phonefactor)[[27]](#footnote-27) devices.

As illustrated later in this document, users download the free app **Multi-Factor Auth** from the device store and activate it using a code provided during set up. When the user signs in, a notification is pushed to the app on their mobile device. The user taps to approve or deny the authentication request. (Cell or Wi-Fi access is required for installing and setting up the app.)

Once the app is installed, it can operate in the following two different modes:

1. **Notification**. In this mode, the app prevents unauthorized access to accounts and stops fraudulent transactions. This is done using a push notification to your phone or registered device as a second out-of-band channel.

Simply view the notification and if it is legitimate select **Authenticate**. Otherwise you may choose **Deny** or choose to **Deny and Report the Fraud**.

1. **One-Time Password (OTP)**. In this mode, the app can be used as software token to generate an Open Authentication (OATH) passcode. This passcode can then be entered along with the username and password in the same inbound channel to provide the second form of authentication. This option is great in instances of spotty phone coverage.

Note It’s comparable to software or soft tokens solutions offered by vendors like RSA and Gemalto.

Note Initiative for Open Authentication (OATH) is an industry-wide collaboration to develop an open reference architecture using open standards to promote the adoption of strong authentication across all networks. The cornerstone of the related specifications are the HMAC-based One-Time Password (HOTP) algorithm as per [RFC 4226](http://tools.ietf.org/html/rfc4226)[[28]](#footnote-28) and Time-Based One-Time Password (TOTP) algorithm as per [RFC 6238](http://tools.ietf.org/html/rfc6238)[[29]](#footnote-29). For additional information, visit the [OATH web site](http://www.openauthentication.org)[[30]](#footnote-30).

Important note OATH shouldn’t be confused with the OAuth, which is an open standard for authorization. OAuth2 as per [RFC 6749](http://tools.ietf.org/html/rfc6749)[[31]](#footnote-31) and [RFC 6750](http://tools.ietf.org/html/rfc6750)[[32]](#footnote-32) is the current version of the protocol. It focusses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, and mobile phones.

* **Automated phone calls** are placed by the Azure MFA online service to any phone, landline or mobile. The user simply answers the call and presses # on the phone keypad to complete their sign in through a distinct channel.
* **Text messages** are sent by the Multi-Factor Authentication service to any mobile phone. The text message contains a one-time passcode. The user is prompted to either reply to the text message with the passcode or enter the passcode into the sign in screen.

The users always sign in with their existing username and password. After the user’s credentials are verified, Multi-Factor Authentication is initiated using the above methods depending on the user’s enrollment.

The Multi-Factor Authentication service offers strong protection against even the most sophisticated attacks:

* Its out-of-band push, call, and text methods offer added protection against malware and man-in-the-middle attacks.
* If the user does not approve an authentication request when prompted or cannot be reached for authentication, access is denied. However, because the Azure AD user’s credentials are verified before the Multi-Factor Authentication service is triggered, this is an indication that the user’s password has been compromised. In some cases, the user will have the option to submit a fraud alert during the authentication request. This will prevent further login attempts and sends a notification to your IT department. You can then work with the user to reset the user’s password.
* A PIN option where available offers an additional layer of security by requiring users to also enter a secret PIN to authenticate. Rules regarding PIN strength and expiration can be set by the administrator of the directory tenant. If a user’s PIN has expired, for example, they will be prompted the set a new PIN the next time they are prompted for multi-factor authentication.

Azure Multi-Factor Authentication enables compliance with regulatory requirements for multi-factor authentication such as the following ones to name of few:

* NIST 800-63 Electronic Authentication Guidelines for Level 3 Assurance,
* HIPAA Requirements Relative to Electronic Protected Health Information (EPHI),
* Payment Card Industry Data Security Standards (PCI DSS),
* Criminal Justice Information System (CJIS) Security Policy,
* Authentication in an Internet Banking Environment Guidance (FFIEC).

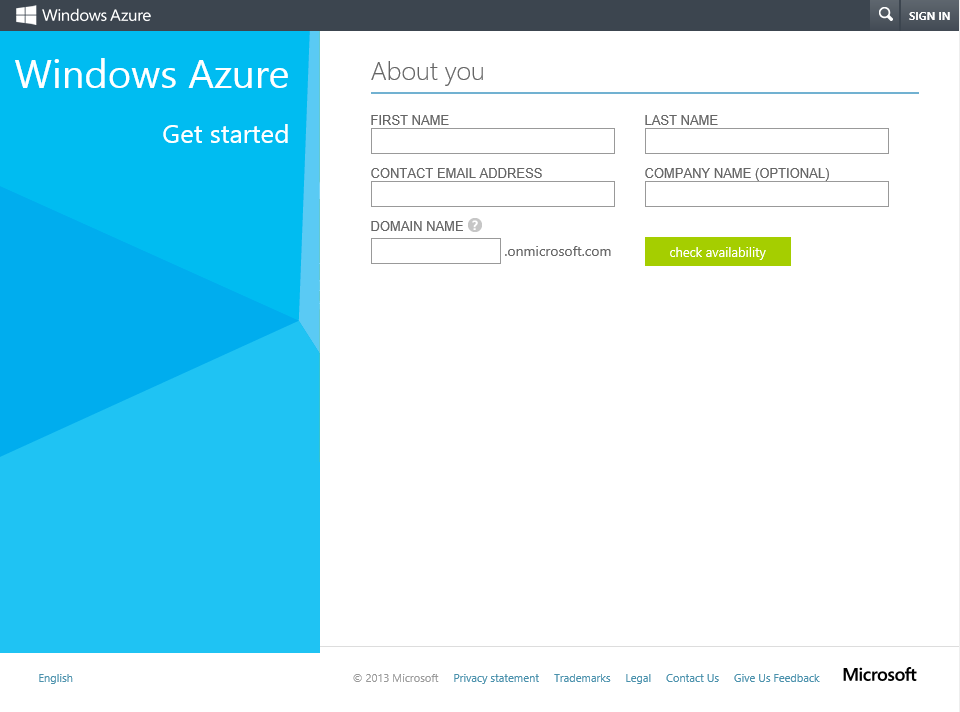
On-demand and scheduled reports are available for auditing of authentication requests.

# Configuring Azure AD for Multi-Factor Authentication

This section illustrates how to enable the Multi-Factor Authentication for Azure AD. The steps below assumes you already have an Azure subscription with your Active AD directory tenants.

If you do not have an Azure subscription or are using Office 365 and have not signed up for an Azure subscription, you will need to do so prior to enabling multi-factor authentication for your user accounts.

You can sign-up for your free Azure AD tenant and trial Azure account by following the link <https://account.windowsazure.com/signup?offer=MS-AZR-0044P>.



If you are already a paid Microsoft Office 365 customer, one simple way to add an Azure subscription to your Office 365 account consists in signing up for the $0 subscription by following the link <https://account.windowsazure.com/PremiumOffer/Index?offer=MS-AZR-0110P&whr=azure.com>/.

If you have a trialMicrosoft Office 365 subscription, you can instead navigate to the Azure Signup page at <https://account.windowsazure.com/SignUp> with your Office 365 global administrator account.

Note You can log into the Office 365 administrator portal and go to the Azure Signup page or go directly to the signup page, select sign in with an organizational account and log in with your Office 365 global administrator credentials.

Once you have completed your trial tenant signup, you will be redirected to the [Azure subscription management page](https://account.windowsazure.com/Subscriptions)[[33]](#footnote-33) and can proceed to the Azure management portal by clicking **Portal** at the top right corner of your screen.

## Adding Multi-Factor Authentication to Azure AD

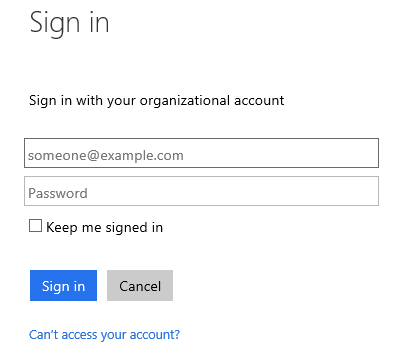
Before (cloud-based) multi-factor authentication can be enabled for users in the Azure AD directory tenant, a Multi-Factor Authentication provider must be created and linked to the directory tenant.

Important note Use of Multi-Factor Authentication is free for Azure AD global administrators when the corresponding Azure AD directory tenant has not been provisioned with Multi-Factor Authentication for directory users. When using for free to secure administrator access, advanced configuration options and reporting are not available. However, if you wish to extend multi-factor authentication to all of your users and/or want to your global administrators to leverage the advanced configuration options and reporting via the management portal, then you must purchase and configure a Multi-Factor Authentication provider. Finally, you can only have one Multi-Factor Authentication provider per tenant.

Note For additional information, see Microsoft TechNet article [Administering Azure Multi-Factor Authentication Providers](http://technet.microsoft.com/en-us/library/dn376346.aspx)[[34]](#footnote-34).

To add a Multi-Factor Authentication provider to an Azure AD (Premium) directory tenant, proceed with the following steps:

1. Open an InPrivate browsing session and navigate to the Azure management portal at <https://manage.windowsazure.com>.
2. Sign in with your administrative credentials to your Azure subscription. To sign in with your organizational account, select **Sign in with your organizational account** and enter your credentials (username and password).

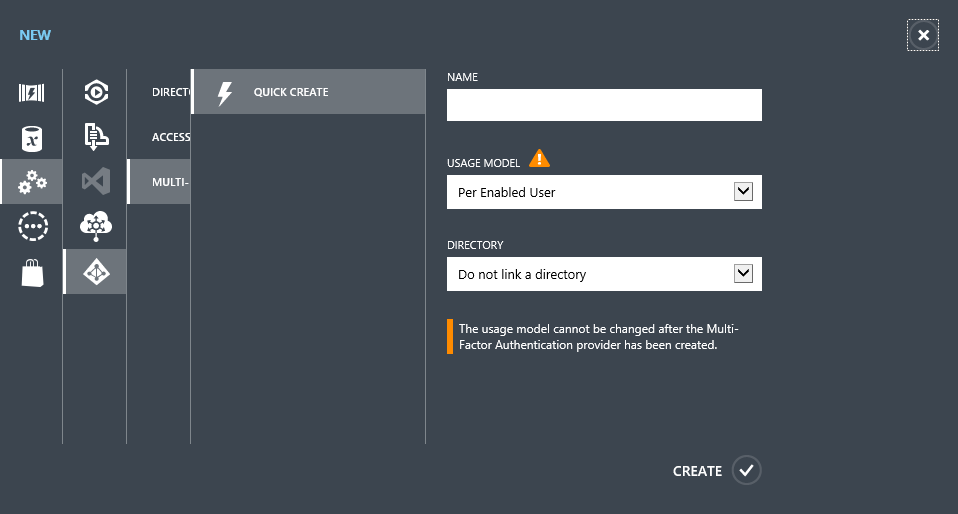


Important note You need to sign in with an organizational account to manage Multi-Factor Authentication. You cannot manage Multi-Factor Authentication with a Microsoft account.

1. On the left pane of the Azure management portal, click **ACTIVE DIRECTORY**.
2. At the top, click **MULTI-FACTOR AUTH PROVIDERS**



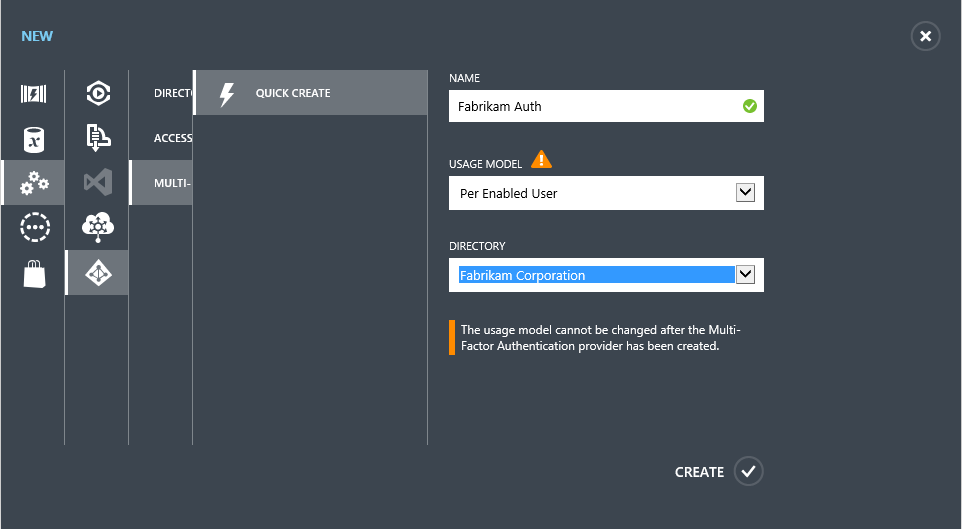
1. Click **CREATE A NEW MULTI-FACTOR AUTHENTICATION PROVIDER** or click **NEW** in the tray at the bottom, and then select **APP SERVICES**, **ACTIVE DIRECTORY**, **MULTI-FACTOR AUTH PROVIDER**, and then **QUICK CREATE**.



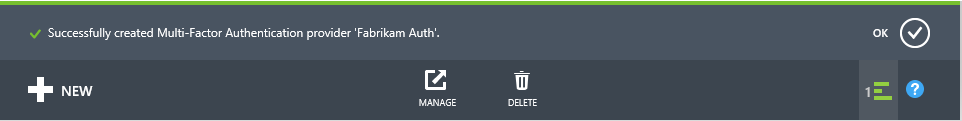
1. In **NAME**, type the name of the provider, for example “*Fabrikam Auth*”.
2. From the **USAGE MODEL** drop down, select the billing options that accommodate your need. Two billing options are available:
3. **Per Enabled User**. Generally used by enterprises to enable multi-factor for a fixed number of employees who authenticate regularly. This option is typically used for scenarios such as Office 365.
4. **Per Authentication**. Generally used by enterprises to enable multi-factor authentication for a large group of external users who authenticate infrequently.

Note For additional information on usage model, see [Multi-Factor Authentication Pricing Details](http://www.windowsazure.com/en-us/pricing/details/multi-factor-authentication/)[[35]](#footnote-35).

1. From the **DIRECTORY** drop down, select the directory name that the Multi-Factor Authentication Provider is associated with, for example **Fabrikam Corporation** as illustrated here.



1. Click **CREATE**. Please notice the notification at the bottom, and wait until the notification displays “Successfully created” before continuing: “*Successfully created Multi-Factor Authentication provider ‘Fabrikam Auth’*”.



1. Click **OK**.

## Enabling users for Multi-Factor Authentication

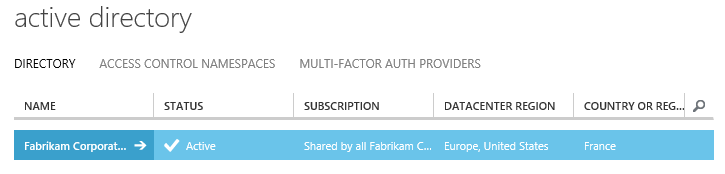
Once the Multi-Factor Authentication provider has been created, you need to enable multi-factor authentication on your users. If the Multi-Factor Authentication provider is later **deleted,** users will default back to single-factor authentication, i.e. passwords.

Note For additional information, see Microsoft TechNet article [Enable a Multi-Factor Authentication for a user account](http://technet.microsoft.com/en-us/library/dn394289.aspx)[[36]](#footnote-36).

### Creating new MFA-enabled user

To create new MFA enabled users, proceed with the following steps:

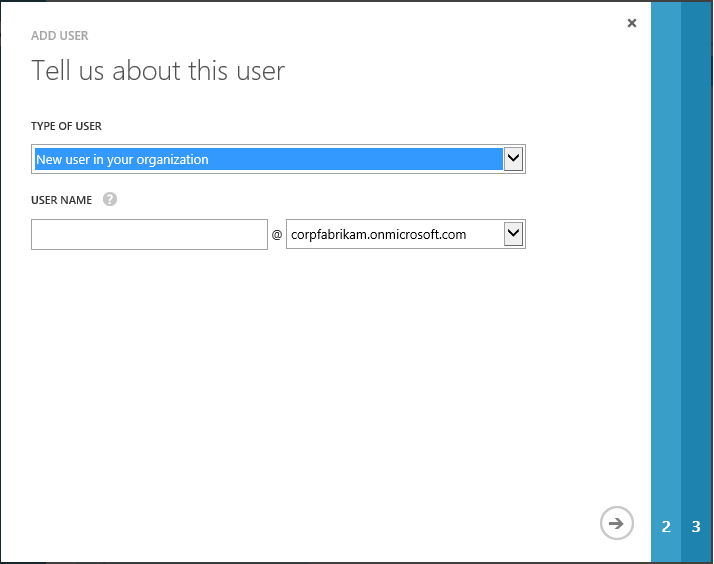
1. From the Azure management portal, click **ACTIVE DIRECTORY** on the left pane.



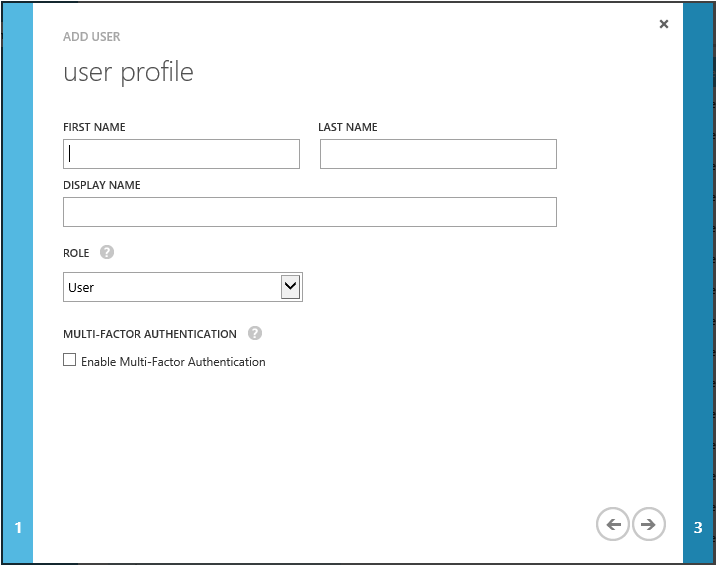
1. Under **DIRECTORY**, click the directory tenant for the user you want to create, for example **Fabrikam Corporation** as illustrated here.
2. At the top, click **USERS**



1. At the tray at the bottom, click **ADD USER**. An **ADD USER** wizard brings up.



1. In **USER NAME**, type in the username, for example ‘”*johndoe*”, and then click the next arrow.



1. In the **user profile** page, complete the following information:
2. **FIRST NAME**: specify the first name, for example “*John*”.
3. **LAST NAME**: specify, for example “Doe”.
4. **DISPLAY NAME**: specify the display name “*John Doe*”.
5. **ROLE**: keep **User** selected in the drop-down.
6. **MULTI-FACTOR AUTHENTICATION**: check the box **Enable Multi-Factor Authentication**.

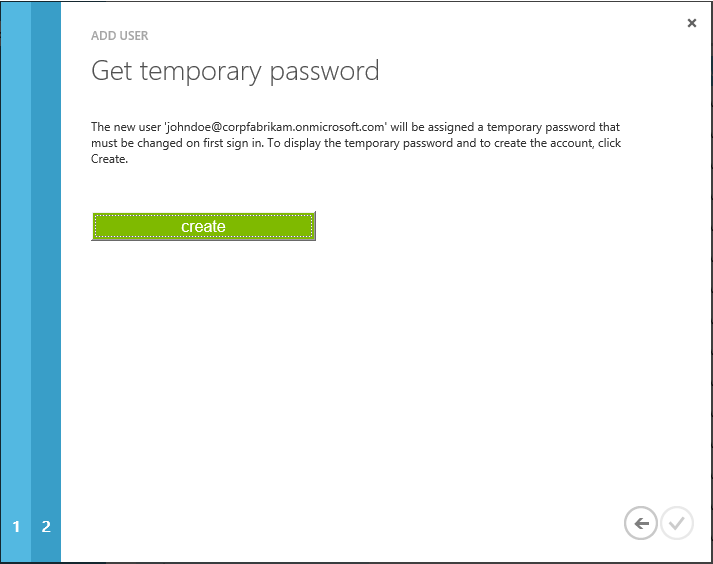
A notification pops ups.



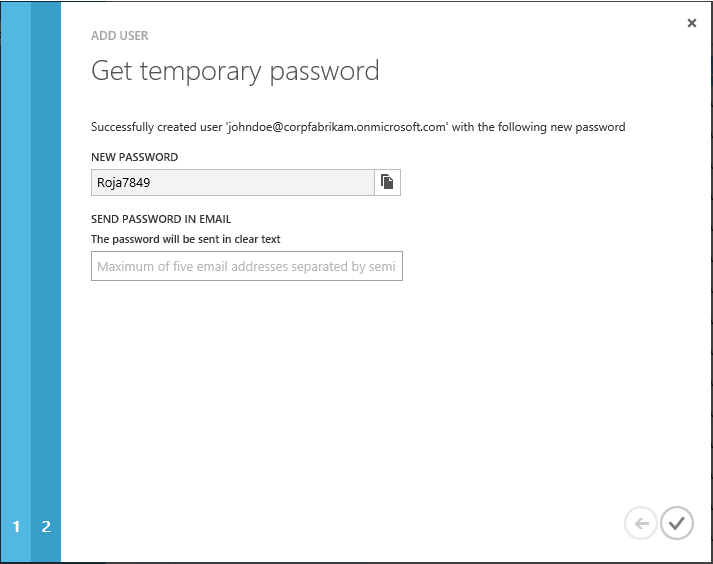
Important note As previously noticed, non-browser apps do not have built-in support for interactive prompts that are required by Multi-Factor Authentication. More specifically, in the context of Office 365, this applies to clients such as Outlook, Lync, Word, Excel, PowerPoint, PowerShell, SkyDrive Pro, Exchange ActiveSync (EAS), POP, and IMAP clients, etc.

When you enable Multi-Factor Authentication for such an Office 365 user account, they will be able to use non-browser apps, such as Outlook, Lync, etc., until they have completed multi-factor enrollment or their account status is set to Enforced. In order to continue to use non-browser apps, they must create app passwords for these apps. An app password, is a password that allows them to by-pass the Multi-Factor Authentication and continue to use their non-browser apps. It is advised that you send them an email that informs them how they can use their non-browser apps and consequently not be locked out.

1. Click next arrow.



1. In the **Get temporary password** page, click **create** to generate a temporary password.



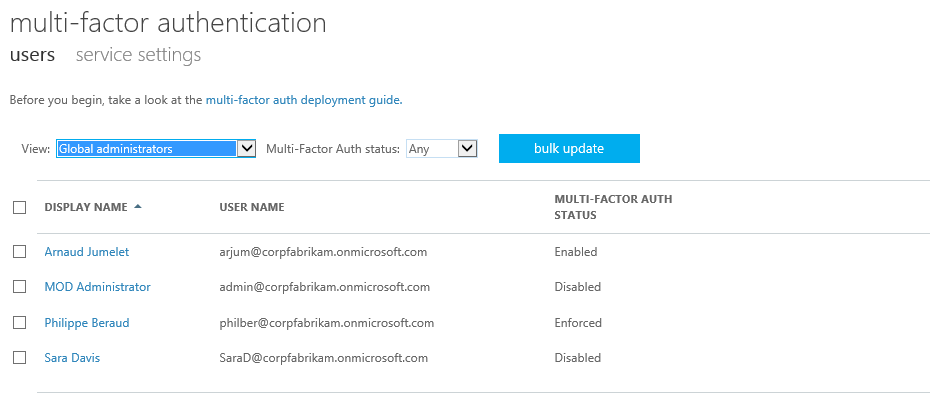
1. Copy the password and click on the check box to close the wizard.

### Enabling existing users for MFA

If you had users created prior to enabling Multi-Factor Authentication, you will need to enable Multi-Factor Authentication for these users manually.

To enable existing users for Multi-Factor Authentication, proceed with the following steps:

1. From the Azure management portal, click **ACTIVE DIRECTORY** on the left pane.
2. Under **DIRECTORY**, click the directory tenant for the user you want to create, for example **Fabrikam Corporation** as illustrated here.
3. At the top, click **USERS**.
4. In the tray at the bottom, click **MANAGE MULTI-FACTOR AUTH**. A new tab opens up with the **multi-factor authentication** page.

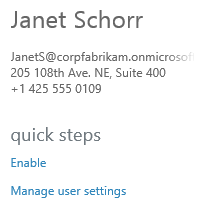


This page allows you to enable and disable Multi-Factor Authentication for users in your directory tenant. This also allows you to force users to provide their contact methods again, and reset application password.

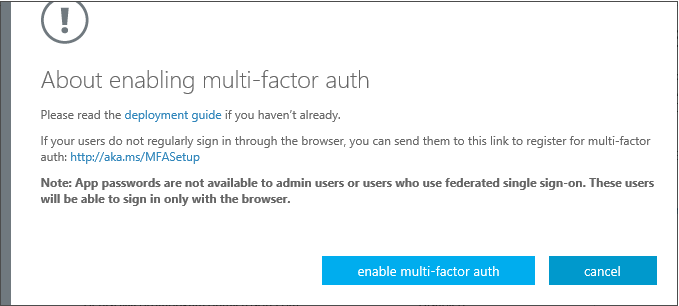
1. Change the view at the top to find the user(s) that you wish to enable for multi-factor authentication. From the **View** drop down select **Sign-in allowed users**.



1. Check the box next to the users to enable for MFA, for example “*Janet Schorr* *JanetS@corpfabrikam.onmicrosoft.com*” as illustrated here.



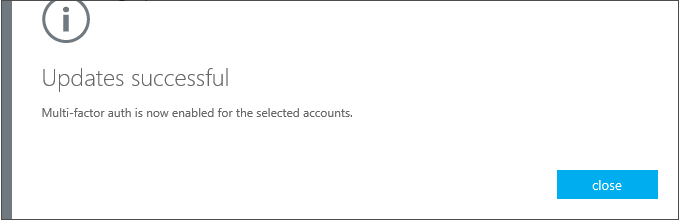
1. Click **Enable** on the right. This opens up a pop-up that specifies the next steps you need to take with your users.



1. Review the content, and then click **enable multi-factor auth**.

Important note As previously noticed, non-browser apps do not have built-in support for interactive prompts that are required by Multi-Factor Authentication. More specifically, in the context of Office 365, this applies to clients such as Outlook, Lync, Word, Excel, PowerPoint, PowerShell, SkyDrive Pro, Exchange ActiveSync (EAS), POP, and IMAP clients, etc.

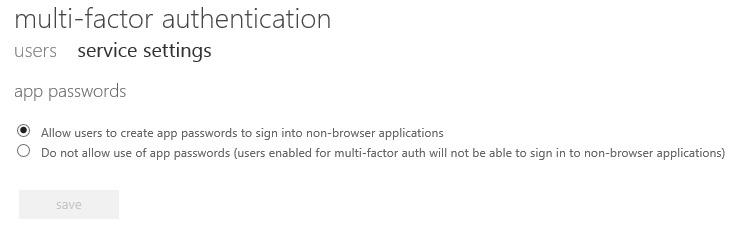
When you enable Multi-Factor Authentication for such an Office 365 user account, they will be able to use non-browser apps, such as Outlook, Lync, etc., until they have completed multi-factor enrollment or their account status is set to Enforced. In order to continue to use non-browser apps, they must create app passwords for these apps. An app password, is a password that allows them to by-pass the Multi-Factor Authentication and continue to use their non-browser apps. It is advised that you send them an email that informs them how they can use their non-browser apps and consequently not be locked out.



1. Click **close**.

To allow Office 365 users the ability to create app passwords to enable non-browser apps access, proceed with the following steps:

1. At the top of the **multi-factor authentication** page, click **service settings**.



1. Ensure that the radio button next to **Allow users to create app passwords to sign into non-browser applications** is selected.
2. Close the **multi-factor authentication** page.

Conversely, if you do not wish to enable non-browser apps access with app passwords for Multi-Factor Authentication-enabled users, this functionality can be disabled by selecting **Do not allow use of app passwords (users enabled for multi-factor auth will not be able to sign in to non-browser applications)** in the above step 2.

## Using Multi-Factor Authentication with Azure AD

Once you have enabled the user account(s) for multi-factor authentication, the user(s) can sign-in and complete the enrollment process. This section walks you through the initial logon process, illustrating how to complete the enrollment process of Multi-Factor Authentication for a user.

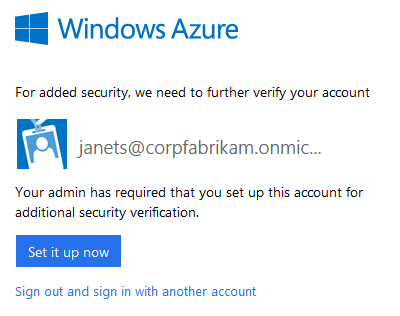
Note For additional information, see Microsoft TechNet article [Signing in for the first time using Azure Multi-Factor Authentication](http://technet.microsoft.com/en-us/library/dn394276.aspx)[[37]](#footnote-37).

To complete the enrollment process of the Multi-Factor Authentication, proceed with the following steps:

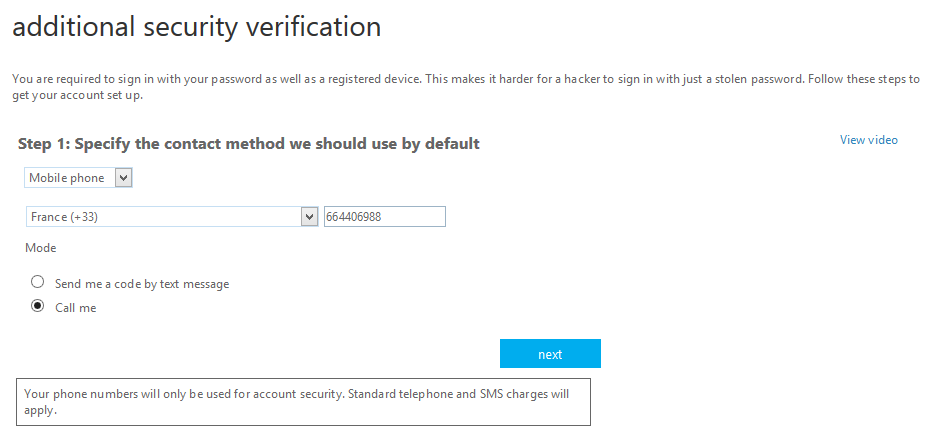
1. Open an InPrivate browsing session and navigate to <http://aka.ms/MFASetup>. You will now be redirected to the login page.



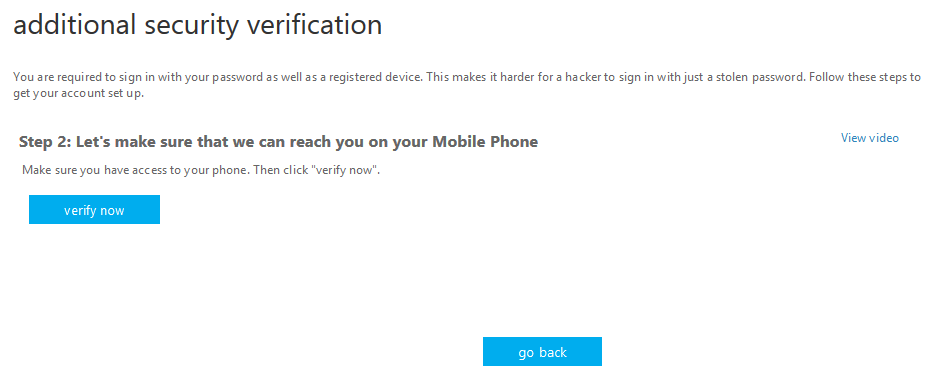
1. Click **Use another account** and sign-in with your user’s organizational account, for example as *JanetS@corpfabrikam.onmicrosoft.com* in our illustration. Because Multi-Factor Authentication has been enabled for this user, you are asked to configure it. This step is required the first time after Multi-Factor Authentication has been enabled for a user.



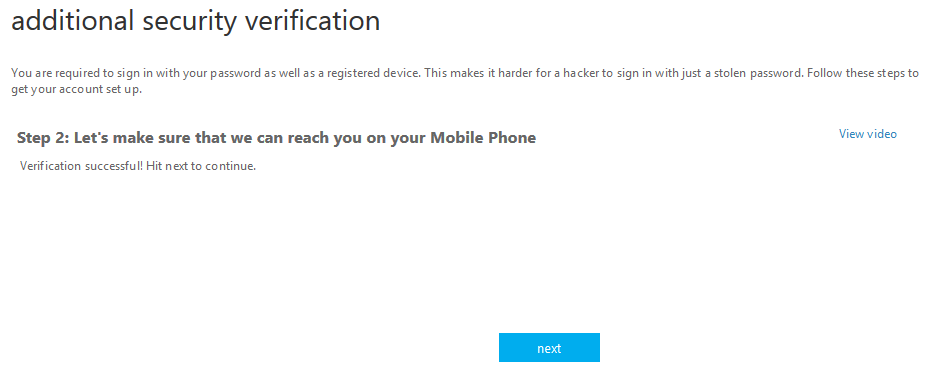
1. Click **Set it up now**.



1. From the **Step 1: Specify the contact method we should use by default** page, ensure **Mobile phone** is selected in the first drop-down.
2. In the second drop down for the country or the region, select your country.
3. Enter your mobile phone number in the textbox next to the country drop down.
4. Under **Mode**, select **Call me**. Alternatively you can select **Send me a code by text message**. The steps will be slightly different.
5. Click **next.**



1. From the **Step 2: Let’s make sure that we can reach you on your Mobile Phone** page, click **verify now**.
2. When you receive the call, answer, press # and hang-up. When Multi-Factor Authentication is provided through a phone call, the user will always press # to proceed with the authentication.



1. Click **next**.



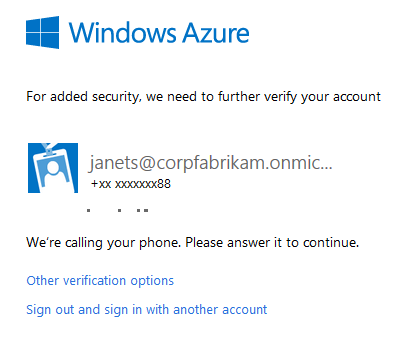
1. From the **Step 3: Apps like Microsoft Office will need new passwords for this account** page, click **I don’t use this account with these apps.**

Note After the enrollment process has been completed, users can setup app passwords for non-browser apps (such as Outlook, Lync, etc.). We illustrate this capability later in this document.

At this stage,you have now been verified into Azure AD.

To login with a configured account, proceed with the following steps:

1. At the login screen, your organizational account is already entered, for example **JanetS@corpfabrikam.onmicrosoft.com** as illustrated here.
2. Enter the **password**, click **Sign In**.



1. When your phone rings, answer, press # and hang up.

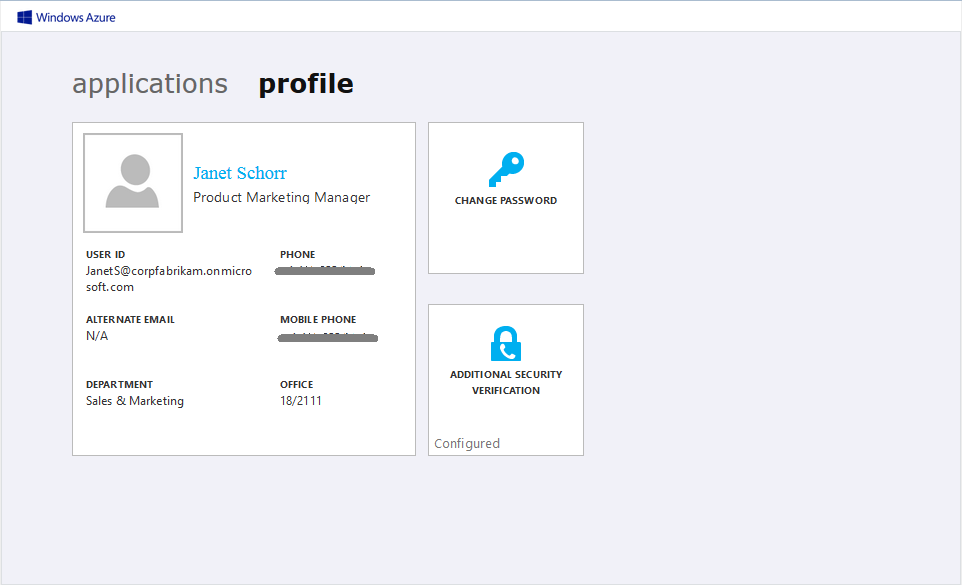
Note While your preferred authentication method is the default, you can also choose to authenticate using any of the other authentication methods you have configured by selecting the Other authentication methods link.

## Configuring the Multi-Factor Authentication mobile application

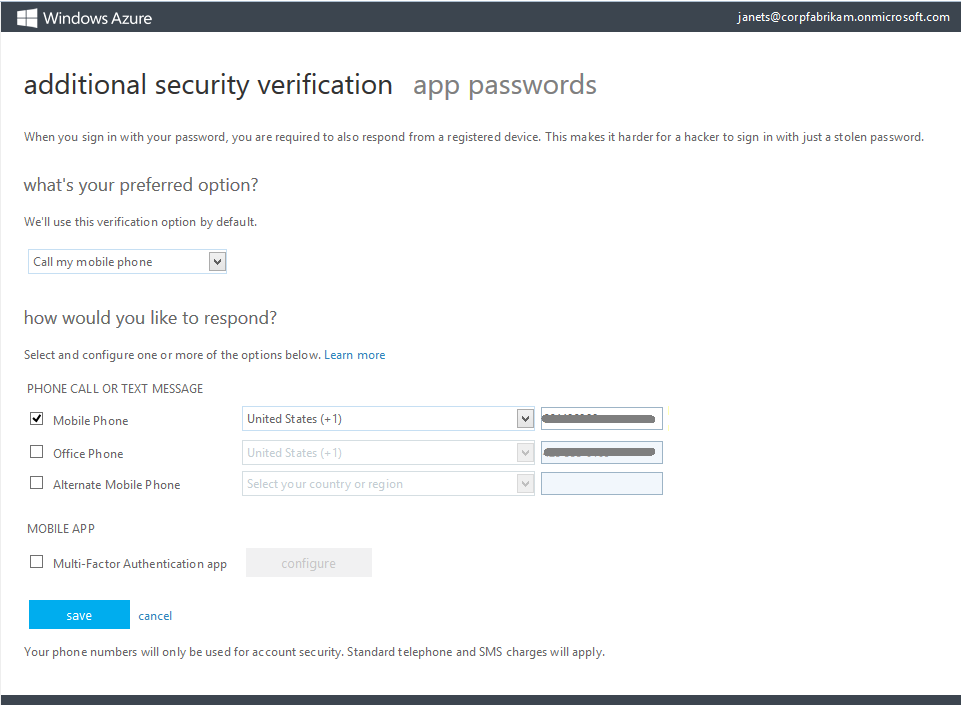
This section illustrates how to add the Multi-Factor Authentication mobile app to authenticate against Azure AD with the previously configured Multi-Factor Authentication provider.

To configure the Multi-Factor Authentication mobile application, proceed with the following steps:

1. From the application store on your phone, find and install the app **Multi-Factor Authentication**. As previously mentioned, this app is available for [Windows Phone](http://www.windowsphone.com/en-us/store/app/phonefactor/0a9691de-c0a1-44ee-ab96-6807f8322bd1)[[38]](#footnote-38), [iOS](ttps://itunes.apple.com/us/app/phonefactor/id475844606?mt=8)[[39]](#footnote-39), and [Android](https://play.google.com/store/apps/details?id=com.phonefactor.phonefactor)[[40]](#footnote-40).
2. Once the Multi-Factor Authentication mobile app has been downloaded and is installed, you can activate it for multiple accounts.
3. Open an InPrivate browsing session and navigate to the Access Panel at <https://account.activedirectory.windowsazure.com/profile>.
4. Sign-in with your organizational account, for example “*JanetS@corpfabrikam.onmicrosoft.com*” as illustrated here.



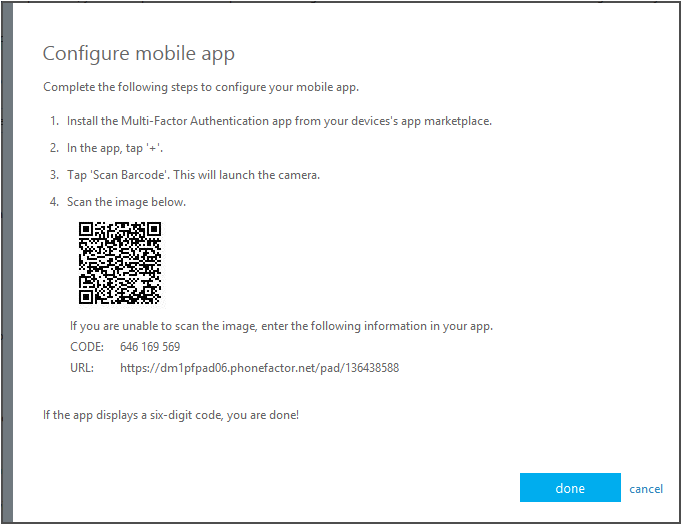
1. Click **ADDITIONAL SECURITY VERIFICATION.**



1. Check the box to enable **Multi-Factor Authentication app**.



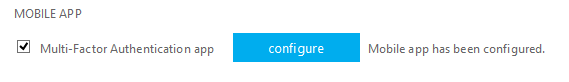
1. Click **configure**.



1. Switch to your mobile device
2. Openthe **Multi-Factor Authentication** application.
3. In the mobile app, click **New (+).**

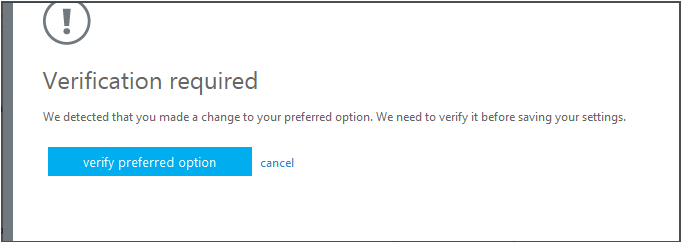
Note The interface will differ slightly between mobile OS apps.

1. Either scan the barcode, or enter the information manually. Upon scanning the barcode or entering the information, you should then see a 6 digit authentication code for the directory.
2. Switch back to the Access Panel.
3. Click **done.**
4. Notice the **checking activation status** message. Wait for this to read “**Mobile app has been configured**” before continuing.



Note You have now activated your mobile application for Multi-Factor Authentication.

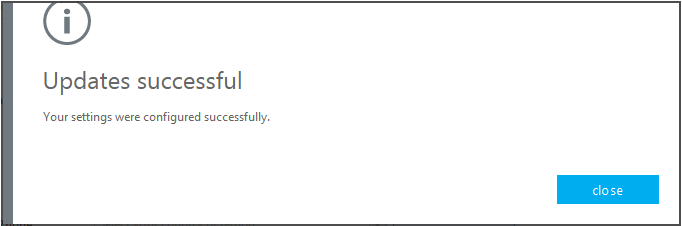
1. Under **what’s your preferred option?**, from the drop down, select **Notify me through app**.
2. Click **save.**



Note In order to use a new Multi-Factor Authentication process, you must first verify the process is working.

1. Click **verify preferred option**.
2. Switch to your mobile device. When prompted, click **verify.**

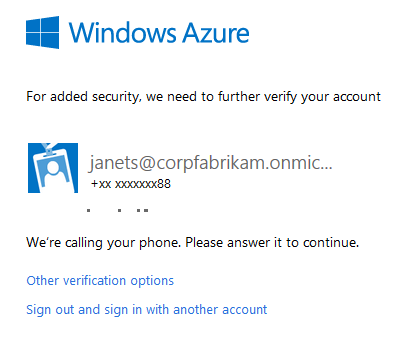
Note There are other options available here. These options will be covered later in this document.



1. Click **close.**
2. Close your browsing session.

To login with the Multi-Factor Authentication mobile app, proceed with the following steps:

1. Open an InPrivate browsing session and navigate to the Access Panel at <https://account.activedirectory.windowsazure.com/profile>.
2. Sign-in with your organizational account, for example “*JanetS@corpfabrikam.onmicrosoft.com*” as illustrated here.

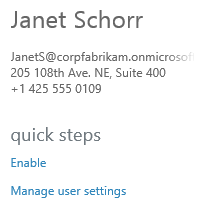


1. When the Multi-Factor Authentication mobile app notifies you of the authentication attempt, click **Verify** from the mobile app.
2. The sign in completes. Close the browsing session**.**

## Managing the user settings

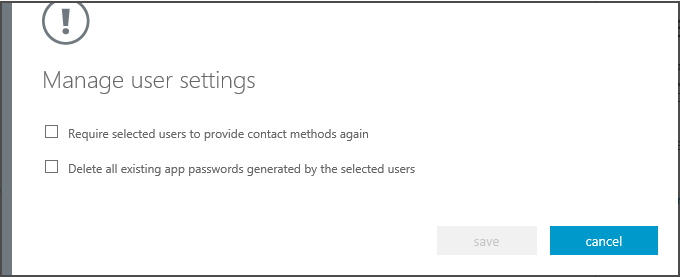
To manage the user settings, proceed with the following steps:

1. Open an InPrivate browsing session and navigate to the Azure management portal at <https://manage.windowsazure.com>.
2. Sign-in with your administrative credentials. To sign-in with your organizational account, select **Sign in with your organizational account** and logon and enter your credentials (username and password).
3. On the left pane, click **ACTIVE DIRECTORY**.
4. Under **DIRECTORY**, click the directory tenant for the user(s) you want to manage.
5. At the top, click **USERS**.
6. In the tray at the bottom, click **MANAGE MULTI-FACTOR AUTH**. A new tab opens up with the **multi-factor authentication** page.
7. Find the user that you wish to manage and place a check in the box located next to the name. As before, you may need to change the view at the top.



This will brings up two options on the right: **Enable** and **Manage user settings**.

1. Click **Manage User settings**. This brings up an eponym pop-up that allows you to select the following user settings in the event a machine or device is lost or stolen:



1. **Require selected users to provide contact methods again**. This setting forces the user to complete the enrollment process again when they sign-in. Non-browser apps (such as Outlook, Lync, etc.) will continue to work if they have app passwords associated with them unless the setting below is also selected.
2. **Delete all existing app passwords generated by the selected users**. This setting deletes all of the app passwords that were created by the selected Office 365 users. Non-browser apps (such as Outlook, Lync, etc.) that were associated with these app passwords will cease to work until a new app password is created.
3. Place a check in the desired boxes and click **save**.
4. Close the browsing session**.**

To manage the contact information and set preferred and backup contact methods from an end-user perspective, proceed with the following steps:

1. Open a browser session and navigate to <https://account.activedirectory.windowsazure.com/proofup.aspx>.
2. Sign-in with your organizational account, for example “*JanetS@corpfabrikam.onmicrosoft.com*” as illustrated here. This will take you directly to the **additional security verification** page.

You can add or update your contact information and set preferred and backup contact methods using this page.

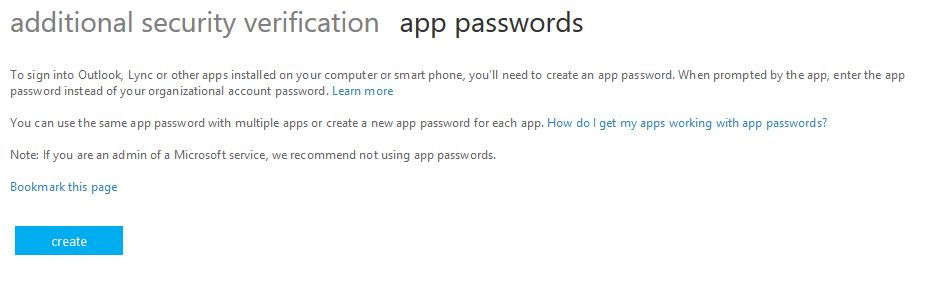
Note You will only be able to edit your office phone number using this page if you are a global or user admin and your account is not being synchronized with the Azure AD directory tenant.

App passwords can initially be created when you complete the enrollment process. This said, and as previously mentioned, users can create app passwords later on if they have already completed the enrollment process but have not setup app passwords:

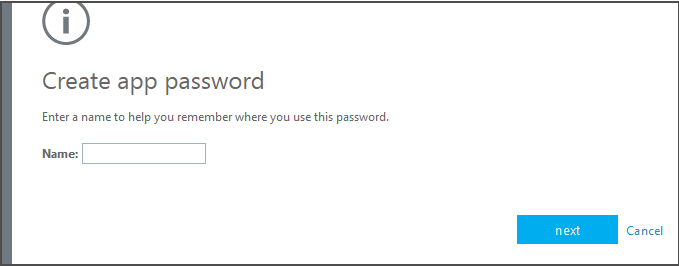
* App passwords are 16-character randomly generated passwords that, once generated, allow users who are enabled for Multi-Factor Authentication to sign-in with non-browser apps like Outlook, Lync, etc.
* App passwords are used in place of the regular user account password.
* App passwords are system-generated, and cannot be manually entered by end-users. They will only be displayed once, upon creation.
* App passwords do not automatically expire, but can be revoked anytime by end-users or an administrator.
* A user can create up to 40 app passwords and can tag them with names indicating their use.

To add app passwords after having completed the enrollment process, proceed with the following steps:

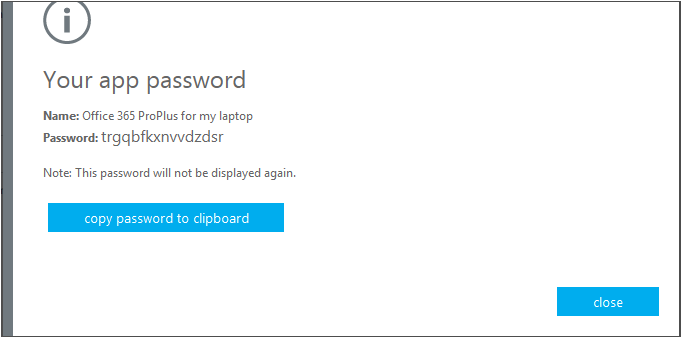
1. From the **additional security verification** page, click **app passwords** at the top.



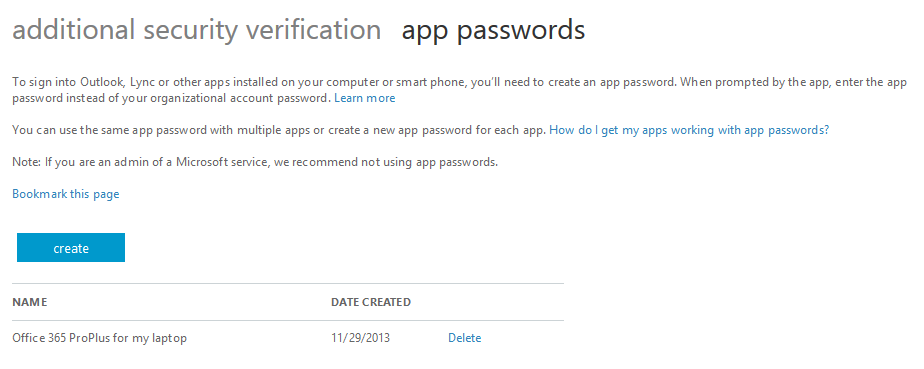
1. Click **create**. A **Create app password** dialog brings up.



1. In **Name**, enter a name for the app password, for example “*Office 365 ProPlus for my laptop*” as illustrated here, and then click **next**.



1. Click **copy password to clipboard** to copy the generated password, and then click **close**.



You should see your app password on the **app passwords** page.

1. Now, paste the app password that was copied to the clipboard into the non-browser app, such as Outlook to login.

Note For additional information, see Microsoft TechNet article [Managing your Azure Multi-Factor Authentication User Settings](http://technet.microsoft.com/en-us/library/dn270518.aspx)[[41]](#footnote-41).

# Configuring advanced settings and reports

The following section describes the advanced settings that are available for configuration and use with Azure MFA.

Note For additional information, see Microsoft TechNet article [Configuring Advanced Multi-Factor Authentication Settings](http://technet.microsoft.com/en-us/library/dn376348.aspx)[[42]](#footnote-42).

## Creating and administering a fraud report

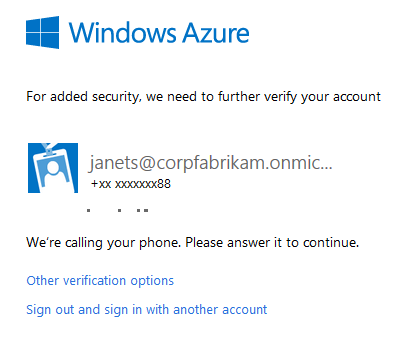
When the user gets an authentication request from Multi-Factor Authentication when they are not signing in, access is denied if the user does not approve the request when prompted or cannot be reached for authentication. However, as aforementioned, because the user’s credentials are verified before Multi-Factor Authentication is triggered, this is an indication that the user’s password has been compromised. The user has the option to submit a fraud alert during the authentication request.

The Fraud Alert feature prevents further login attempts and allows a user to notify their IT department if someone attempts to sign in using their credentials. The IT department should in turn work with the user to reset the user’s password.

The Fraud Alert feature is available with the phone call, text message, and Multi-Factor Authentication mobile app push authentication options.

To send a fraudulent report, proceed with the following steps:

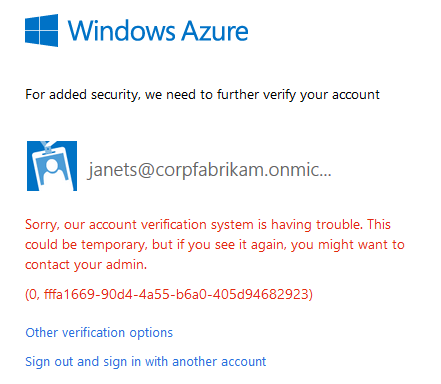
1. Open an InPrivate browsing session and navigate to the Access Panel at <https://account.activedirectory.windowsazure.com/profile>.
2. Sign in with your organizational account, for example “*JanetS@corpfabrikam.onmicrosoft.com*” as illustrated here.



1. When you receive the authentication request:

* Automated phone call: Press **0#** then **1** to submit a fraud alert
* Text message: Reply with **0#**
* Multi-Factor Authentication mobile app: Tap **Cancel and Report Fraud**, **report fraud**,and **Close**.

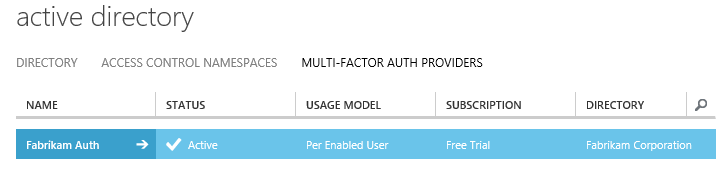
Note When a user receives a notification for logon that they did not initiate, they have the opportunity to block the login attempt by pressing 0 then #. This will fail the authentication for the user that is attempting to gain access to their account. If there are multiple attempts to access the account a user can press 1 to report fraud on the account. This will lock the users account and inform the administrators there has been unwanted authentication requests for the user.



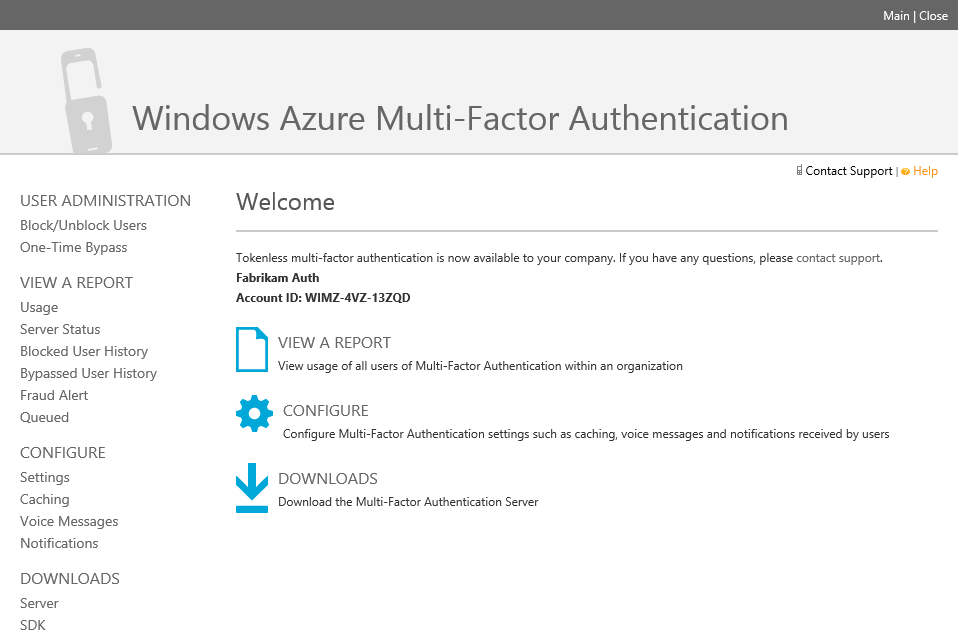
1. Close the browser session.

To view and manage fraudulent reports, proceed with the following steps:

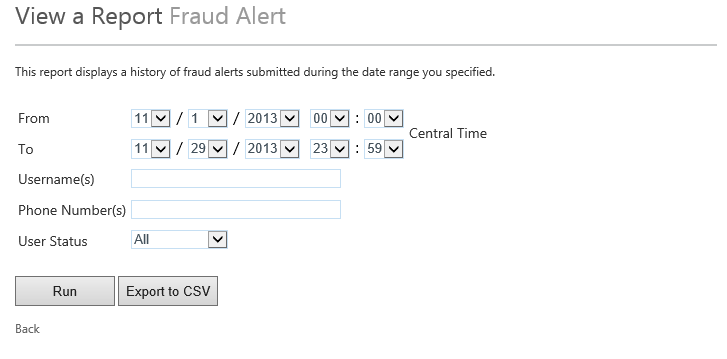
1. Open an InPrivate browsing session and navigate to the Azure management portal at <https://manage.windowsazure.com>.
2. Sign in with your administrative organizational account. To sign in with your organizational account, select **Sign in with your organizational account** and enter your credentials (username and password).
3. Sign in with your credentials to your Azure subscription.
4. On the left hand side, click **ACTIVE DIRECTORY.**
5. At the top, click **MULTI-FACTOR AUTH PROVIDERS.**



1. Select the **Fabrikam Auth** provider.
2. At the bottom, click **MANAGE**. A **Windows Azure Multi-Factor Authentication** page opens up in a new tab.

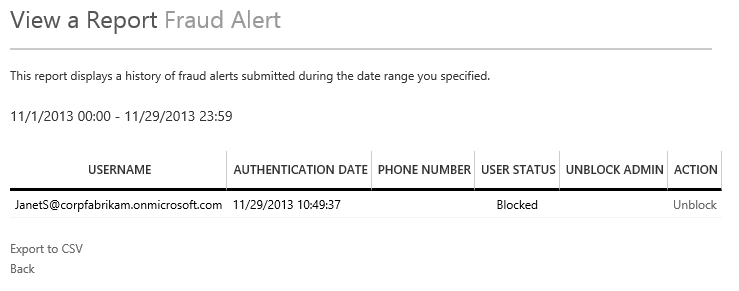


1. On the left hand side, click **Fraud Alert** under **VIEW A REPORT.**



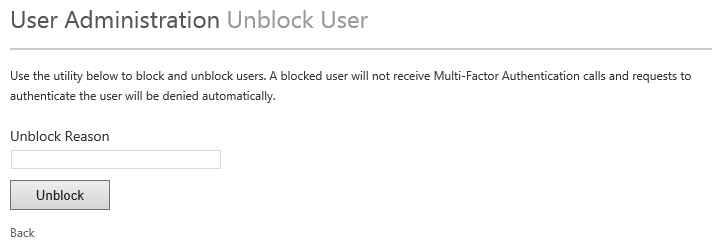
Note The fraud alert reporting section lets you view fraudulent activity from a specific period of time.

1. Click **Run** to generate a new report.

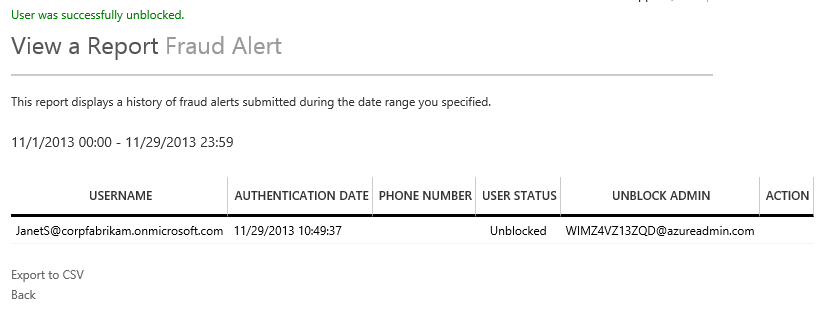


There is a new item in the report for the user. Because the user reported the fraudulent activity, their account is currently marked as **Blocked**. Once the issue has been investigated, an administrator or the IT department can unblock the user’s account so they may begin to use it again.

1. In the **Action** column, click **Unblock.**



1. In the **Unblock Reason** text box, enter a reason, for example “*Testing purpose*” in the current situation.
2. Click **Unblock.**



1. Close the browsing session.

Notice the user is now unblocked. This user can now login to their applications again.

## Viewing Multi-Factor Authentication settings and reports

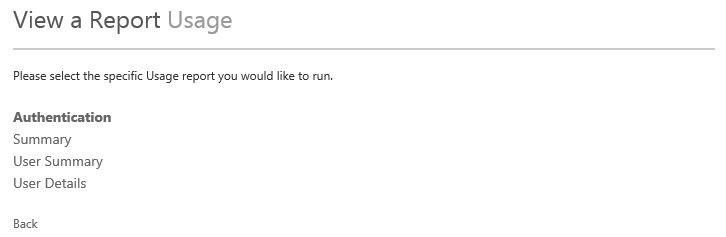
This section illustrates additional capabilities of the Azure MFA, such as:

* How to view Multi-factor authentication reports,
* How to create one-time bypass when a user doesn’t have their phone or a cell signal is not available,
* How to create custom greetings specific for an organization needs,
* And how to set authentication caching so users don’t have to use Multi-Factor Authentication for subsequent requests within specific applications and time windows.

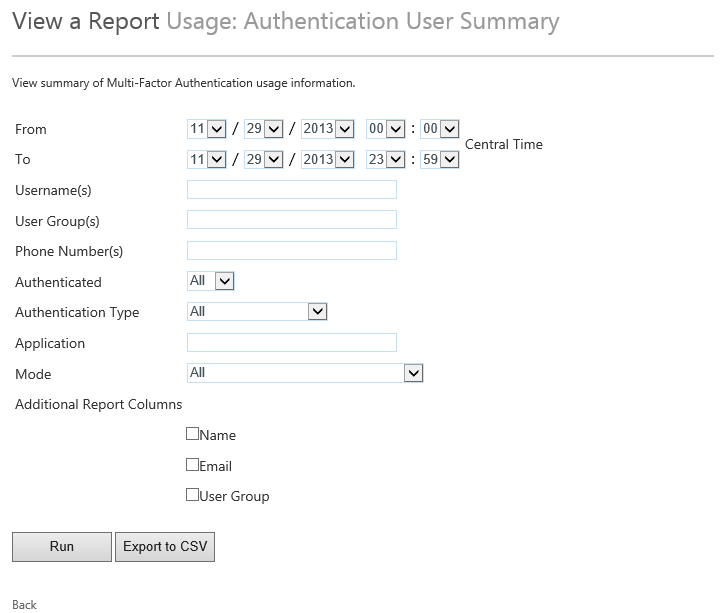
### Viewing Multi-Factor Authentication reporting

To view Multi-Factor Authentication reporting, proceed with the following steps:

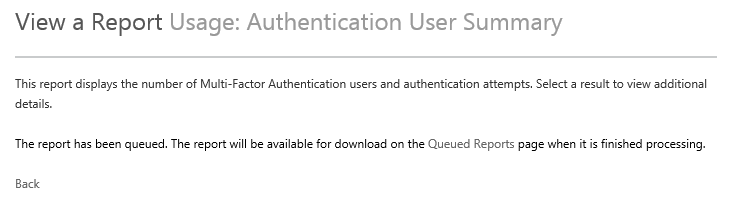
1. From the **Windows Azure Multi-Factor Authentication** page, click **Usage** on the left under **VIEW A REPORT**.



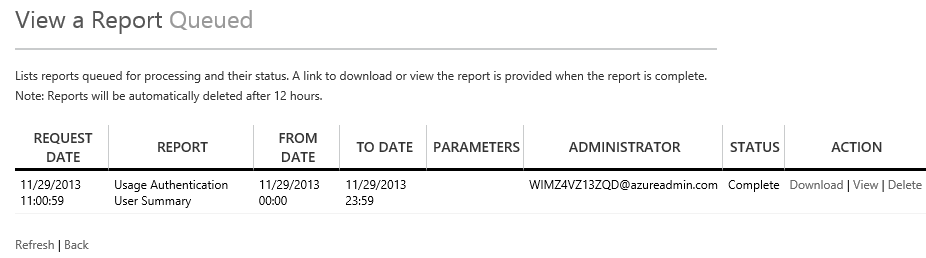
1. Click **User Summary**.



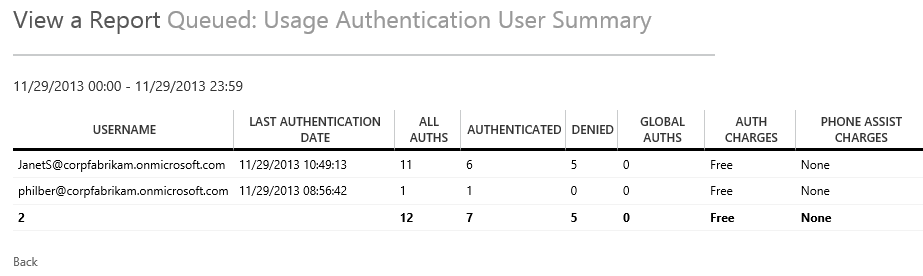
1. Click **Run**.



1. Click **Queued** on the left under **VIEW A REPORT**.



1. Click **View** to see the report.



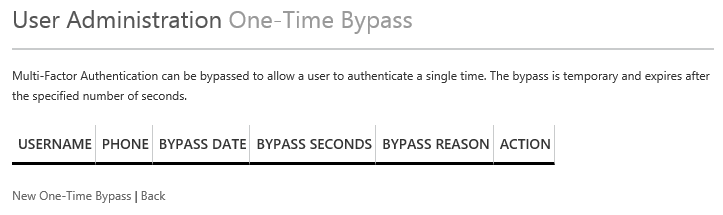
You can now see information regarding which users are logging in using the Azure MFA. You can repeat these steps above to view the other reports.

### Creating a one-time bypass

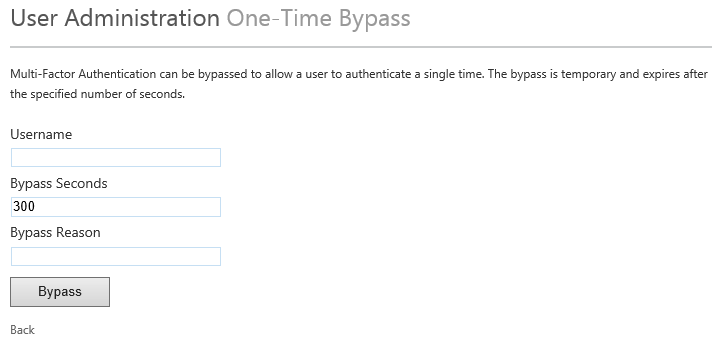
As illustrated, support for multiple methods, including Wi-Fi and offline authentication using the mobile app, and multiple phone numbers make it very rare for a user not to have a means to authenticate. However, in those instances, the user can contact their company IT help desk to request a one-time bypass of additional authentication.

To create a one-time bypass, proceed with the following steps;

1. From the **Windows Azure Multi-Factor Authentication** page, click **One-Time Bypass** on the left under **USER ADMINISTRATION**.



1. Click **New One-Time Bypass**.



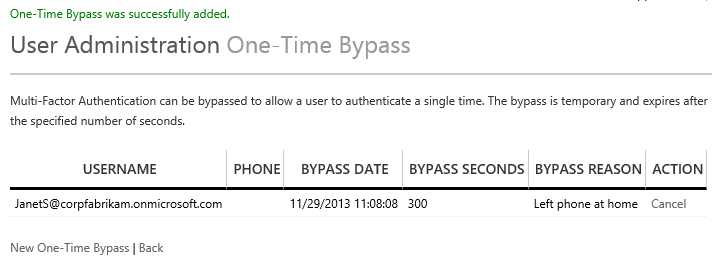
Note This option allows an administrator to grant a user a bypass of Multi-Factor Authentication for a certain amount of time. An example is if an administrator was helping a user reconfigure Multi-Factor Authentication, they may want to remove the Multi-Factor Authentication requirement for a single sign-in during a window of time to help the user.

1. Enter the following information:

* **Username**: “*JanetS@corpfabrikam.onmicrosoft.com*”
* **Bypass Seconds**: 300
* **Bypass Reason**: “Left phone at home” for example.

Note If you receive a warning that the name is not in the authentication logs, ensure you have used the entire UPN name and there are no spaces or anything, this step will not work if this is incorrect. Copy from the Usage | user summary report to ensure accuracy.

1. Click **Bypass**.

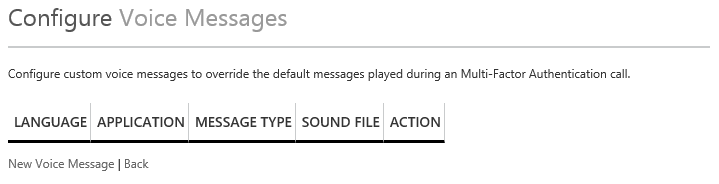


1. Open a new InPrivate browsing session and navigate to the Access Panel at <https://account.activedirectory.windowsazure.com/profile>.
2. Login with your user credentials. Notice you are not required to complete a Multi-Factor Authentication request.
3. Close your browsing session.

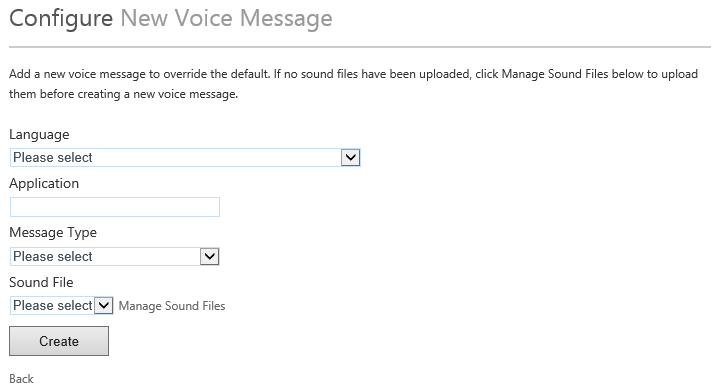
### Viewing custom greetings

To view custom greetings, proceeds with the following steps:

1. From the **Windows Azure Multi-Factor Authentication** page, click **Voice Messages** on the left hand side under **CONFIGURE**.



1. Click **New Voice Message**.



1. Expand the **Language** drop down.

Note An administrator can configure voice greeting in a variety of different languages to suit the needs of the application user base. Many companies customize the messages to include their company name, e.g. "This is Fabrikam Corporation calling to authenticate your sign in."

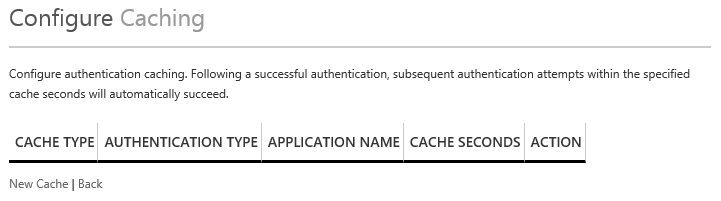
1. Expand **Message Type.** Message types are all the different messages the Azure MFA service uses. To get full coverage in an application for different languages, each one of these messages would need a custom sound file.
2. Click **Back**.

### Setting authentication caching

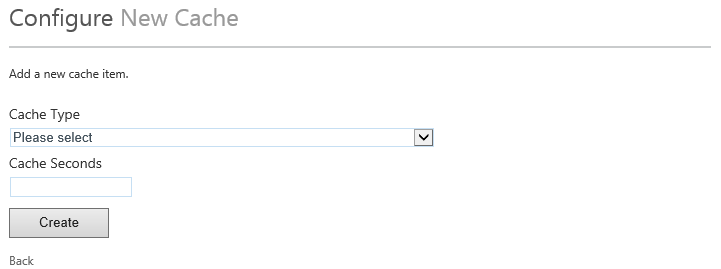
The lastadditional capability we’d like to illustrate as part of this paper is the authentication caching. As its name suggests, authentication caching allows a user to skip Multi-Factor Authentication following a successful authentication on subsequent authentication requests for a period of time**.**

To set authentication caching, proceed with the following steps:

1. From the **Windows Azure Multi-Factor Authentication** page, click **Caching** on the left hand side under **CONFIGURE**.



1. Click **New Cache**.



1. In the **Cache Type** drop down, select **User.**

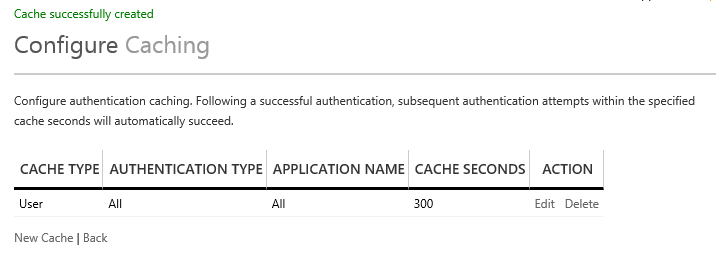
Note Cache type defines the scope or specific conditions that must be met on subsequent authentication requests:

User: Cache successful authentication for a user across all applications.

User, Authentication Type, Application Name: Cache successful authentications for user, authentication type, and application name. Subsequent request must come from the same application to utilize the cache feature.

User, Authentication Type, Application Name, IP (Server/SDK only): Cache based on previous type but also requiring initiating IP to match for the caching feature to authenticate the request.

1. In **Cache Seconds**, type “*300*”.
2. Click **Create.**



1. Close your browsing session.
2. Open an InPrivate browsing session and navigate to the Access Panel at <https://account.activedirectory.windowsazure.com/profile>.
3. Sign-in with your user’s organizational account, for example “*JanetS@corpfabrikam.onmicrosoft.com*” as illustrated here.
4. When you receive the authentication request:

* Multi-Factor Authentication mobile app: Tap **Verify**
* Automated phone call: Press **#**.
* Text message: Reply with **Verification Code**.

1. In the top right, click **JanetS@corpfabrikam.onmicrosoft.com**, and then click **Sign out.**
2. Log back in as **JanetS@corpfabrikam.onmicrosoft.com.**

Note The second time you login, you are not required to do Multi-Factor Authentication. This is because caching has allowed your authentication attempt to succeed. You can continue to login to resources for 5 minutes before you will need to complete another Multi-Factor Authentication.

1. Close your browsing session.

This concludes the guided tour of Azure MFA as well as this paper.

|  |
| --- |
| The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.  This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.  Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.  Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.  © 2015 Microsoft Corporation. All rights reserved.  The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.  Microsoft, list Microsoft trademarks used in your white paper alphabetically are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.  The names of actual companies and products mentioned herein may be the trademarks of their respective owners. |

1. Enabling Hybrid Cloud today with Microsoft Technologies: http://www.microsoft.com/en-us/download/details.aspx?id=39052 [↑](#footnote-ref-1)
2. Modern business applications: http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx [↑](#footnote-ref-2)
3. Azure Multi-Factor Authentication: http://azure.microsoft.com/en-us/services/multi-factor-authentication/ [↑](#footnote-ref-3)
4. Application access enhancements for Azure AD: http://technet.microsoft.com/en-us/library/dn308588.aspx [↑](#footnote-ref-4)
5. Adding Multi-Factor Authentication to Azure Active Directory: http://technet.microsoft.com/en-us/library/dn249466.aspx [↑](#footnote-ref-5)
6. Enabling Multi-Factor Authentication for On-Premises Applications and Windows Server: http://technet.microsoft.com/en-us/library/dn249467.aspx [↑](#footnote-ref-6)
7. Building Multi-Factor Authentication into Custom Apps (SDK): http://technet.microsoft.com/en-us/library/dn249464.aspx [↑](#footnote-ref-7)
8. Active Directory from on-premises to the Cloud: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-8)
9. Using Multi-Factor Authentication with Azure AD: http://technet.microsoft.com/en-us/library/jj713614.aspx [↑](#footnote-ref-9)
10. Directory Sync with Single Sign-On Scenario: http://technet.microsoft.com/en-us/library/dn441213.aspx [↑](#footnote-ref-10)
11. Office 2013 updated authentication enabling Multi-Factor Authentication and SAML identity providers: http://blogs.office.com/2014/11/12/office-2013-updated-authentication-enabling-multi-factor-authentication-saml-identity-providers/ [↑](#footnote-ref-11)
12. Checklist: Use AD FS to implement and manage single sign-on: http://technet.microsoft.com/en-us/library/jj205462.aspx [↑](#footnote-ref-12)
13. Use Shibboleth Identity Provider to implement single sign-on: http://technet.microsoft.com/en-us/library/jj205456.aspx [↑](#footnote-ref-13)
14. Use third-party identity providers to implement single sign-on: http://technet.microsoft.com/en-us/library/jj679342.aspx [↑](#footnote-ref-14)
15. Azure Multi-Factor Authentication options for Federated Users: http://technet.microsoft.com/en-us/library/dn394284.aspx [↑](#footnote-ref-15)
16. Office 365 Adapter: Deploying Office 365 Single Sign-On using Azure: http://www.microsoft.com/en-us/download/details.aspx?id=38845 [↑](#footnote-ref-16)
17. Using Multi-Factor Authentication with Active Directory Federation Services http://technet.microsoft.com/en-us/library/dn394281.aspx [↑](#footnote-ref-17)
18. Walkthrough Guide: Manage Risk with Additional Multi-Factor Authentication for Sensitive Applications: http://technet.microsoft.com/en-us/library/dn280946.aspx [↑](#footnote-ref-18)
19. Installing the Azure Multi-Factor Authentication Users Portal: http://technet.microsoft.com/en-us/library/dn394290.aspx [↑](#footnote-ref-19)
20. Deploying the Azure Multi-Factor Authentication Server Mobile App Web Service: http://technet.microsoft.com/en-us/library/dn394277.aspx [↑](#footnote-ref-20)
21. Leverage Azure Multi-Factor Authentication Server for Azure AD single sign-on with AD FS: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-21)
22. Microsoft Azure SLA: http://go.microsoft.com/fwlink/?linkid=313266&clcid=0x409 [↑](#footnote-ref-22)
23. Microsoft Acquires PhoneFactor: http://blogs.msdn.com/b/windowsazure/archive/2012/10/04/microsoft-acquires-phonefactor.aspx [↑](#footnote-ref-23)
24. Azure Multi-Factor Authentication: http://technet.microsoft.com/en-us/library/dn249471.aspx [↑](#footnote-ref-24)
25. Multi-Factor Authentication app on Windows Phone Store: http://www.windowsphone.com/en-us/store/app/phonefactor/0a9691de-c0a1-44ee-ab96-6807f8322bd1 [↑](#footnote-ref-25)
26. Multi-Factor Authentication app on iTunes: https://itunes.apple.com/us/app/phonefactor/id475844606?mt=8 [↑](#footnote-ref-26)
27. Multi-Factor Authentication app on Google Play: https://play.google.com/store/apps/details?id=com.phonefactor.phonefactor [↑](#footnote-ref-27)
28. RFC 4226 HOTP: HMAC-based One-Time Password: http://tools.ietf.org/html/rfc4226 [↑](#footnote-ref-28)
29. RFC 6238 TOTP: Time-Based One-Time Password Algorithm: http://tools.ietf.org/html/rfc6238 [↑](#footnote-ref-29)
30. OATH web site: http://www.openauthentication.org [↑](#footnote-ref-30)
31. RFC 6749 The OAuth 2.0 Authorization Framework: http://tools.ietf.org/html/rfc6749 [↑](#footnote-ref-31)
32. RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage: http://tools.ietf.org/html/rfc6750 [↑](#footnote-ref-32)
33. Azure subscription management page: https://account.windowsazure.com/Subscriptions [↑](#footnote-ref-33)
34. Administering Azure Multi-Factor Authentication Providers: http://technet.microsoft.com/en-us/library/dn376346.aspx [↑](#footnote-ref-34)
35. Multi-Factor Authentication Pricing Details: http://www.windowsazure.com/en-us/pricing/details/multi-factor-authentication/ [↑](#footnote-ref-35)
36. Enable a Multi-Factor Authentication for a user account: http://technet.microsoft.com/en-us/library/dn394289.aspx [↑](#footnote-ref-36)
37. Signing in for the first time using Azure Multi-Factor Authentication: http://technet.microsoft.com/en-us/library/dn394276.aspx [↑](#footnote-ref-37)
38. Multi-Factor Authentication app on Windows Phone Store: http://www.windowsphone.com/en-us/store/app/phonefactor/0a9691de-c0a1-44ee-ab96-6807f8322bd1 [↑](#footnote-ref-38)
39. Multi-Factor Authentication app on iTunes: https://itunes.apple.com/us/app/phonefactor/id475844606?mt=8 [↑](#footnote-ref-39)
40. Multi-Factor Authentication app on Google Play: https://play.google.com/store/apps/details?id=com.phonefactor.phonefactor [↑](#footnote-ref-40)
41. Managing your Azure Multi-Factor Authentication User Settings: http://technet.microsoft.com/en-us/library/dn270518.aspx [↑](#footnote-ref-41)
42. Configuring Advanced Multi-Factor Authentication Settings: http://technet.microsoft.com/en-us/library/dn376348.aspx [↑](#footnote-ref-42)