Azure AD/Office 365 seamless sign-in

**Part 1 – Choose the best option to fulfill your requirements**

Microsoft France

Published: January 2017

Version: 1.0

Authors: Philippe Beraud, Jean-Yves Grasset (Microsoft France),

Contributors/Reviewers: Daniel Pasquier (Microsoft France), Philippe Maurent (Microsoft Corporation)

For the latest information on Azure Active Directory, please see

http://azure.microsoft.com/en-us/services/active-directory/

Copyright © 2017 [Microsoft Corporation](http://www.microsoft.com). All rights reserved.

Abstract: Azure AD/Office 365 offer three main identity models (Cloud identity, Synchronized identity and Federated identity) to set up and manage accounts. In addition, the two latter provide different seamless sign-in deployment options. So it’s important to carefully consider which identity model and in turn which sign-in option are best suited for your environment, and what they imply in terms of infrastructure and operations.

Built on existing documentation, this document is intended to provide a better understanding of the above identity models with Azure AD/Office 365 and the different seamless sign-in options available in this context if any.

This document is intended for system architects and IT professionals who are interested in understanding the basics of the seamless sign-in features of Azure AD/Office 365 along with planning and deploying such a deployment in their environment.

Table of Contents

[Introduction 3](#_Toc473538001)

[Objectives of this paper 4](#_Toc473538002)

[Non-objectives of this paper 5](#_Toc473538003)

[Organization of this paper 5](#_Toc473538004)

[About the audience 5](#_Toc473538005)

[Understanding Azure AD/Office 365 identity models 6](#_Toc473538006)

[Choosing the simplest model for your needs 7](#_Toc473538007)

[Choosing the cloud identity model 8](#_Toc473538008)

[Choosing the synchronized identity model 10](#_Toc473538009)

[Choosing the synchronized identity model with password hash synchronization (PHS) 12](#_Toc473538010)

[Choosing the synchronized identity model with the pass-through authentication (PTA) 13](#_Toc473538011)

[Choosing the federated identity model 15](#_Toc473538012)

[Suggesting a decision matrix for the identity models 22](#_Toc473538013)

[Deploying the chosen identity model 23](#_Toc473538014)

[Going beyond 24](#_Toc473538015)

# Introduction

[Microsoft Office 365](http://office.microsoft.com/en-us/business/)[[1]](#footnote-2) provides secure anywhere access to professional email, shared calendars, instant messaging (IM), video conferencing, and document collaboration.

It represents the cloud version of the Microsoft communication and collaboration products with the latest version of the Microsoft desktop suite for businesses of all sizes. Office 365 indeed notably includes:

* **Microsoft Office 365 ProPlus**. [Microsoft Office 365 ProPlus](http://technet.microsoft.com/en-us/library/gg702619%28v%3Doffice.15%29.aspx)**[[2]](#footnote-3)** is the Office software that can be installed locally on a device (computer, phone, or tablet) as a subscription. Depending on the device type and related operating system, it includes the following programs: Access, Excel, InfoPath, Skype for Business (formerly Lync), OneNote, Outlook, PowerPoint, Publisher, Word, etc. The programs have the same features and functionality as other versions of Office. For example, Word in Office 365 ProPlus works the same way it does in Office Professional 2013 and Office Professional 2016. This version of Office is included in [E3, E4, E5, A3, Business Essentials and Business Premium plans](http://technet.microsoft.com/en-US/library/office-365-plan-options.aspx)[[3]](#footnote-4) and is therefore the logical companion of Office 365 services.

The programs of the Office suite can be deployed easily in a click-to-run mode on a Windows computer, either directly from the Office 365 portal or from the local network with your own management tool.

**Note**For more information, see the Microsoft TechNet article [Getting started guide for deploying Office 365 ProPlus](http://technet.microsoft.com/en-us/library/jj839718%28v%3Doffice.15%29)[[4]](#footnote-5).

* **Microsoft Exchange Online**. Exchange Online offers cloud-based email, calendar, and contacts with the most current antivirus and anti-spam solutions. It enables access to email on virtually any mobile device and takes advantage of options for voice mail, unified messaging, and archiving.
* **Microsoft SharePoint Online/One Drive for Business**. SharePoint Online is a cloud-based service for creating sites that connect colleagues, partners, and customers using enterprise social networking and collaboration.
* **Microsoft Skype for Business Online**. Skype for Business Online offers cloud-based IM, presence, and online meeting experiences with screen sharing, voice and video conferencing.

**Note** For additional information on Office 365 in addition to the content of this paper, please refer to the [Office 365 Community web site (blogs, forums, wikis, etc.)](http://community.office365.com/en-us/default.aspx)[[5]](#footnote-6).

With the exception of Internet sites for anonymous access created with SharePoint Online, users must be authenticated when accessing above services in Office 365.

**Azure Active Directory (Azure AD) is the directory behind Office 365 used to store user identities and other tenant properties by Office 365**. Just like the on-premises Active Directory stores the information for Exchange, SharePoint, Skype for Business and your custom LOB Apps, Azure AD stores the information for Exchange Online, SharePoint Online, Skype for Business Online and any custom applications build in the Microsoft’s cloud.

## Objectives of this paper

Through the availability of multiple seamless sign-in options that come with the supported identity models, Azure AD provides organizations with an open choice and eventually the ability to authenticate in accordance their own requirements, allowing their users - regardless of the subsequent implementation choice driven by the chosen identity model - to benefit from a seamless sign-experience to access Azure AD/Office 365 and the services that they have been provisioned for.

Thus, users that are on the internal corporate network or connected through a VPN will have seamless access to Azure AD/Office 365. If users are accessing Azure AD/Office 365 from home or from any computer not connected to the corporate network, they will also still have access to Azure AD/Office 365 using their corporate credentials. Such a user sign-in experience is awaited by many organizations:

* **Work computer on a corporate network**. When users are at work and signed in to the corporate network, single sign-on enables them to access Azure AD/Office 365 without signing in again;
* **Roaming with a work computer**. For users who are logged on to domain-joined computers with their corporate credentials, but who are not connected to the corporate network (for example, a work computer at home or at a hotel), single sign-on enables them to access Azure AD/Office 365 without signing in again as well;
* **Home or public computer**. When the user is using a computer that is not joined to the corporate domain, the user must sign in with corporate credentials to access Azure AD/Office 365. This is still an advantage since they will only have to remember one set of credentials for their corporate and Azure AD/Office 365 accesses.
* **Mobile device**. On a mobile device (phone or tablet), in order notably to access Microsoft Exchange Online using Microsoft Exchange ActiveSync (EAS), the users must sign in with their corporate credentials. This is still an advantage since they will only have to remember one set of credentials for their corporate and Office 365 accesses.

Note Not all type of mobile devices are using EAS, some are using [Exchange Web Services (EWS)](http://msdn.microsoft.com/en-us/library/office/dd877012%28v%3Dexchg.150%29.aspx)[[6]](#footnote-7) instead. For more information, see the web site [Office for Mobile Devices](http://products.office.com/en-us/mobile/Office)[[7]](#footnote-8).

* **Microsoft outlook or other e-mail clients**. The users must sign in with their corporate credentials to access their e-mail messages if they are using Outlook or an e-mail client that is not part of Office such as an IMAP or a POP client.

Built on existing Microsoft documentation and knowledge base articles, this paper further presents the supported identity models of Azure AD/Office 365 along with the associated seamless sign-in deployment options.

For that purpose, this document:

* Describes the different identity models in Azure AD/Office 365,
* Covers, for each identity model, the seamless sign-in deployment options if any,
* Shortly illustrates, in this context, the identity architecture and features in Azure AD/Office 365,

, so that Azure AD/Office 365 projects can be more easily completed, and consequently enabling customers to realize the full potential of the Microsoft offerings in the cloud.

## Non-objectives of this paper

This document provides neither guidance for setting up and configuring the discussed seamless sign-in deployment options in a production environment – beyond highlighting key scenarios - nor a complete technical reference for Azure AD Connect, AD FS, or any other technology, product or service being mentioned as part of this document.

Finally, this document doesn’t provide a complete end-to-end walkthrough to rollout a working Azure AD/Office 365 configuration to test and evaluate the seamless sign-in deployment options. This is the purpose of the remaining Part 2, Part 4, Part 4bis, Part 5, Part 6, and Part 7 of this whitepaper.

## Organization of this paper

To cover the aforementioned objectives, this document adopts an organization according to the following themes, each of them being addressed in the following sections:

* Understanding Azure AD/Office 365 identity models.
* Going beyond.

## About the audience

This document is thus intended for system architects and IT professionals who are interested in understanding this seamless sign-in capabilities of Azure AD/Office 365.

# Understanding Azure AD/Office 365 identity models

With the exception of Internet sites for anonymous access created with SharePoint Online, users must be authenticated when accessing services in Office 365.

For that purpose, Azure AD/Office 365 basically offer two types of identities:

1. **Cloud IDs (cloud identity)**. Users receive, for signing into Azure AD, cloud credentials that are separate from other desktop or corporate on-premises credentials. Cloud identities are mastered in the cloud in Azure AD/Office 365.

**Note** With the optional directory synchronization, the user IDs mastered on-premises can be synchronized to the service/cloud in the form of cloud identities.

1. **Federated IDs (federated identity)**. Organizations with an on-premises identity directory (Active Directory or another directory) can leverage the single sign-on feature (a.k.a. identity federation). Users can then sign into Azure AD/Office 365 using their own corporate credentials. The user’s IDs are mastered on-premises and synchronized to the organization’s Azure AD/Office 365 tenant in the form of federated identities. In other words, the identities in the cloud are synchronized copies (w/ a limited subset of attributes) of their associated on-premises identity references.

Considering the above, users can gain access to Azure AD/Office 365 by authenticating to their Azure AD/Office 365 user accounts, either through a prompt to provide valid credentials or through a single sign-on process. Once authenticated, users’ identities refer to the user names associated with the Azure AD/Office 365 accounts. Considering the above, we have three main identity models available plus their variants in terms of seamless sign-in options that may be offered:

1. **Cloud identity model**.
2. **Synchronized identity model** (cloud identity model + directory synchronization).
3. **Synchronized identity model** plus the password hash synchronization (PHS) configured with optional seamless single sign-on (SSO).
4. **Synchronized identity model** with pass-through authentication (PTA), and optional seamless SSO.
5. **Federated identity model** (+ directory synchronization).

The above identity models unsurprisingly affect the user experience, the administrative requirements, the deployment considerations, and the capabilities using Office 365: one should note that each identity model layers on the previous one (except the first one) and that the last two models result in hybrid identities.

Thus, one of the very first question that arises is to how to smoothly integrate/bridge the organization’s existing on-premises identity infrastructure with Azure AD/Office 365 optimally at no additional administration cost and with a user experience as seamless as possible.

## Choosing the simplest model for your needs

In order to make the best choice regarding your own environment, objectives, needs and constraints, you should have a basic understanding of the underlying mechanisms, their requirements along with the user and administrative related sign-in and management experiences.

Regarding the above identity model breakdown, the notion of an “identity bridge”[[8]](#footnote-9) between the on-premises environment and Azure AD/Office 365 can be split down in two parts:

1. **Identity synchronization**. On-premises identities can be synchronized to the Azure AD repository (i.e. the organization’s tenant), and possibly vice-versa for some hybrid scenarios notably relating to Exchange Online.

Azure AD/Office 365 comes with the [Azure Active Directory Connect (Azure AD Connect)](http://www.microsoft.com/en-us/download/details.aspx?id=47594)[[9]](#footnote-10) tool, a single and unified wizard that streamlines and automates the overall onboarding process for directory synchronization with the on-premises directories.

1. **Seamless sign-in experiences**. The above Azure AD Connect also allows – if you want to - to set up different seamless sign-in deployment options including the (cross-domain) single sign-on (SSO) feature, a.k.a. identity federation, but not only.

This single sign-on option requires to set up a standard-based identity federation trust relationship between the on-premises environment (typically with AD FS) and Azure AD/Office 365. The (perceived) complexity of identity federation as well as the additional cost implied by the related infrastructure on-premises, has refrained some organizations to implement the single sign-on feature of Azure AD/Office 365.

Consequently, the Azure AD Connect capabilities offer in turn alternative solutions a seamless sign-in experience without necessarily relying on identity federation:The password (hash of) hash synchronization (PHS) and the pass-through authentication (PTA) feature indeed offer relevant alternatives in many situations

The objective of the next sections consequently aims at discussing all the supported identity models and highlighting the sign-on options available, the technical considerations that pertains to them in order to give you all the key points for a decision, which is not always straightforward since some capabilities also depends on the Azure AD edition, for instance the password write-back in the Premium P1 and P2 editions.

Note For a description of the available editions of Azure AD, see article [Azure Active Directory editions](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-editions)[[10]](#footnote-11). For more information on usage model, see article [Azure Active Directory Pricing](http://www.windowsazure.com/en-us/pricing/details/active-directory/)[[11]](#footnote-12). For information on the usage constraints and other service limits for the Azure AD service per edition, see article [Azure subscription and service limits, quotas, and constraints](https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#active-directory-limits)[[12]](#footnote-13).

In order to allow you to choose the best model for your organization, the three different identity models are considered along with their variants if any in ascending order from a complexity prospective – and from set of capabilities prospective: **the simplest approach that fulfills your objectives, needs and constraints is always the best**.

At the end of the section, you should be in a position to relevantly assess **the best identity model that applies to your own specific situation.**

**Note** There is from now on a much richer bibliography on the subject coming directly from the Microsoft product groups that is available on Microsoft team blogs, MSDN or Microsoft TechNet. Relevant references are indicated throughout the reading.

## Choosing the cloud identity model

The first model is indubitably the simplest one: the user’s identity (account) is created in Azure AD with an associated password. As the model’s name indicates and as already stated above, the identity only resides in the cloud.

Users sign in with their cloud identity. Cloud identities are authenticated using traditional challenge/response, where users type in their username - for example johndoe@litware369.com for the Litware369 (fictitious) company’s Azure AD domain used later throughout this whitepaper for illustration purposes - and the related password. Authentication happens in the cloud and these credentials can be validated by Azure AD. Users are always prompted for credentials.

The cloud identity has no direct correlation with another identity repository. As mentioned above, users have two IDs:

1. One to access on-premises applications and resources.
2. And another one for Azure AD/Office 365, i.e. the Microsoft Online Services cloud ID.

If users belong to an organization using Active Directory on-premises, the on-premises username can be the same (johndoe@litware369.com) even if it qualifies in this case the on-premises identity. Remember that **the two identity repositories are distinct**. Consequently, users are prompted for credentials even when already logged into their AD domain when accessing Azure AD/Office 365. (These credentials can be cached locally to help reduce subsequent prompts.)



Figure 1 Cloud Identity model

The main benefit of this model is that, as soon as the users’ cloud identity is created in Azure AD/Office 365, users can access to all services that have been assigned to them: there is no deployment or integration footprint with an existing on-premises infrastructure to deal with.

In addition, enhanced security features such as [multi-factor authentication](http://technet.microsoft.com/en-us/library/dn383636.aspx)[[13]](#footnote-14) [[14]](#footnote-15) are natively offered by the cloud platform and thus immediately available.

However, the direct drawback is that the **cloud identities have to be separately created and managed**. While, for a small number of accounts, cloud identities can be manually managed from the [Office 365 portal](https://portal.microsoftonline.com)[[15]](#footnote-16) or the Azure management portal, there is a need to rely on some automation process like, for example, PowerShell scripts for a larger population.

Furthermore, IT professionals will have to manage the password policy both in cloud and on-premises. The cloud identities password policy is stored in the cloud in Azure AD. Password reset has to be managed for on-premises and cloud IDs and hence the users have to change the password as per the policy for both.

So, in this model, **users cannot benefit from a seamless sign-in experience** with corporate logon or on-premises applications as no password synchronization is in place. The user is responsible for managing the passwords in both directories.

Furthermore, users will probably have more difficulties to deal with another password potentially implying additional and costly help desk operations (except if you additionally subscribed to the Azure AD Basic and Premium editions that both allow self-service password reset and make you users aware of this capability).

Nevertheless, this cloud identity model could represent a suitable choice if you want to benefit very quickly from Azure AD/Office 365 and provided that:

1. You have no existing on-premises identity infrastructure or conversely the number of users that are concerned is relatively low and you are ready to manage their cloud identities manually or through scripting.

-or-

1. The on-premises identity infrastructure is fairly complex and some rationalization effort is required/welcome before transitioning to a more integrated model.

One of the interest of this very simple model resides in the fact that it enables you to later transition to a more integrated identity model without losing the investment in the cloud identities already created.

## Choosing the synchronized identity model

This second model allows to keep the on-premises directory in sync with Azure AD/Office 365. It thus provides a real integration with the on-premises directory by **synchronizing identities and groups to the Azure AD**.

**Azure AD Connect is now the one stop shop for connecting your on-premises directories to Azure AD, whether you are evaluating, piloting, or in production.**

Note For more information, see article [Integrating your on-premises identities with Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect)[[16]](#footnote-17).

**Azure AD Connect is the best way to connect your on-premises directory with Azure AD and Office 365. Azure AD Connect is replacing DirSync and Azure AD Sync and these two older sync engines are deprecated from April 13, 2016 reaching end of support April 13,2017.**

Note For more information, see article [Upgrade Windows Azure Active Directory Sync (“DirSync”) and Azure Active Directory Sync (“Azure AD Sync”)](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-dirsync-deprecated)[[17]](#footnote-18).

Important note Customers using DirSync or Azure AD Sync will continue to synchronize after April 13, 2017 but they not be able to receive support for their synchronization tool. They must upgrade to the latest version of Azure AD Connect in order to receive support.

Important note Customers running Azure AD Connect 1.0.x.0 also received the message to upgrade to the latest version of Azure AD Connect in order to receive support. Microsoft recommends customers to stay current with Azure AD Connect releases. For a full list of fixes and improvements over the time of Azure AD Connect, see article [Azure AD Connect: Version Release History](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-version-history/)[[18]](#footnote-19).

**Note** Azure AD Connect can be deployed either on-premises or in Microsoft Azure to benefit from a better site availability without any footprint on on-premises hardware.



Figure 2 Synchronized Identity model

One of the benefits is that it enables controlling and managing the corporate user accounts in the traditional way through the Active Directory Users and Computers snap-in. Typical administration tasks involving user accounts, contacts, and groups provisioning, de-provisioning, group membership modifications, account deactivation are performed on the on-premises Active Directory and seamlessly replicated to Azure AD within a 30 minutes’ delay.

**Note** For more information, see blog post [Azure AD Connect 1.1 is now GA – Faster sync times, automatic upgrades and more!](https://blogs.technet.microsoft.com/enterprisemobility/2016/02/18/azure-ad-connect-1-1-is-now-ga-faster-sync-times-automatic-upgrades-and-more/)[[19]](#footnote-20).

There is no manual configuration that you need to be concerned with, everything can be configured via a wizard. This one piece really does provide seamless user management between the on-premises and Azure AD/Office 365 environments.

**The synchronization engine of Azure AD Connect not only provides today a simplified guided configuration experience. It also synchronization of multiple on-premises AD forests**. Beyond these key characteristics, Azure AD Connect offer a rich set of sync capabilities such as:

* Control over which attributes are synchronized based on desired cloud services to consume..
* Ability to set up the connection to Active Directory with minimal Windows Server AD privileges.
* Setup synchronization rules by mapping attributes and controlling how the values flow to the cloud.

and, with the Azure AD Premium P1 or P2 editions, also a rich set of write-back capabilities with the ability to enable:

* Provisioning from the cloud with user write back to on-premises AD.
* Write back of “Groups in Office 365” to on-premises distribution groups in a forest with Exchange.
* Device write back so that for example on-premises access control policies enforced by AD FS can recognize devices that registered with Azure AD (more on this later in this document). This includes the recently announced support for Azure AD Join in Windows 10.

Note For more information, see whitepaper [Azure AD & Windows 10: better Together for Work and School](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[20]](#footnote-21).

* Enable your users to perform self-service password reset in the cloud with write-back to on-premises AD.

Moreover, Azure AD Connect also offer the option to synchronize user passwords from an on-premises Active Directory to a cloud-based Azure AD/Office 365 tenant, which leads us with the next variant: The Password Hash Synchronization (PHS).

Note Additional capabilities are going to be available such as the support for a mixture of directories (Active Directory, LDAP directory, SQL database, and others), the ability to remap and transform existing on-premises attributes, or the support for write-back scenarios like self-service group management (Azure AD Premium (P1 and P2) editions only).

## Choosing the synchronized identity model with password hash synchronization (PHS)

Password Hash Synchronization (PHS) is a feature of Azure AD Connect to retrieve the user account password hashes from an on-premises Active Directory and replicate a digest of this hash to a cloud-based Azure AD/Office 365 tenant.



Figure 3 Synchronized Identity model with the PHS feature

**Note** From a security standpoint, the password information that is replicated in Azure AD is the result of a one-way function (SHA-256) applied to the user’s password hash stored in an encrypted form, which means that, even if this secret leaks, it cannot be used to access to any resource on your corporate internal network. For a detailed description of the password synchronization mechanism, see blog post [AAD Password Sync, Encryption and FIPS compliance](https://blogs.technet.microsoft.com/enterprisemobility/2014/06/28/aad-password-sync-encryption-and-fips-compliance/)[[21]](#footnote-22).

This feature enables end-users to sign into Azure AD services, such as Office 365, Dynamics 365, Intune, and Azure AD Domain Services, using the same password they’re using to sign in to their organization’s on-premises Active Directory.

Note For more information, see article [Implementing password synchronization with Azure AD Connect sync](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-synchronization)[[22]](#footnote-23).

**Such a feature provides a “same sign-on” experience**, where users sign in to their corporate machine and Azure AD/Office 365 with the same credentials. To provide a better experience, a password change is replicated within 2 minutes. Moreover, after a successful authentication, the users can be optionally asked for a multifactor authentication (MFA) in the cloud.

With the PHS feature, this synchronized identity model provides seamless sign-in user experience while requiring a minimal investment from an administrative perspective. With such a tradeoff, it constitutes the **preferred option for most organizations** with possibly the pass-through authentication (PTA) feature covered hereafter.

Moreover, in addition to the PHS feature, the seamless single sign-on (SSO) feature currently in public preview as the time of this writing allows end-users to only need to type their username and not their password to sign in to Azure AD/Office 365 or other cloud apps and services when they are on their corporate machines and connected on the organization’s corporate network.

The seamless SSO feature leverages the Windows Integrated Authentication (WIA) capabilities and the Kerberos protocol.

Note For more information, see article [What is Single Sign On (SSO) (preview)](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso)[[23]](#footnote-24).

## Choosing the synchronized identity model with the pass-through authentication (PTA)

A second variant of the synchronized identity model is offered via the Azure AD pass-through authentication (PTA) if you’re reluctant to sync the (hash of) hash of the passwords with your Azure AD/Office 365 tenant.

So, the PTA feature currently in public preview as the time of this writing provides a simple solution for having password validation for Azure AD/Office 365 performed against the organization’s identity infrastructure, without the need for complex network infrastructure or for the on-premises passwords to exist in the cloud in any form (hash of hash). **Such a feature provides another “same sign-on” experience.**

Note For more information, see blog post [Introducing #AzureAD Pass-Through Authentication and Seamless Single Sign-on](https://blogs.technet.microsoft.com/enterprisemobility/2016/12/07/introducing-azuread-pass-through-authentication-and-seamless-single-sign-on/)[[24]](#footnote-25) and article [What is Azure AD Pass-through Authentication](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication)[[25]](#footnote-26).

**Important note** The PTA feature does NOT support organizations using Alternate Login IDs. For more information on Alternate Login IDs, see article [Configuring Alternate Login ID](https://technet.microsoft.com/en-us/library/dn659436.aspx)[[26]](#footnote-27).

The PTA feature that can be configured via Azure AD Connect leverages for that purpose a simple on-premises agent that listens for password validation requests. Once a request comes in, the agent retrieves the username and password and validates the credential against the on-premises Active Directory infrastructure. The validation occurs over standard Windows APIs. An on-premises domain controller then evaluates the request and returns a response to the agent, which in turn returns this to Azure AD. Azure AD then evaluates the response and responds to the user as appropriate, for example by issuing a security token for the intended service or asking for a multifactor authentication (MFA) in the cloud.



Figure 4 Synchronized Identity model with the PTA feature

Furthermore, with this approach, IT professionals will have to manage the password policy only on-premises. The organization’s identity infrastructure stores and controls the password policy. Password reset occurs for on-premises IDs only.

From a technical implementation perspective, the above agent corresponds to the [lightweight connector](https://download.msappproxy.net/subscription/d3c8b69d-6bf7-42be-a529-3fe9c2e70c90/connector/download)[[27]](#footnote-28) initially introduced by the Azure AD Application Proxy capability of Azure AD Premium P1.

This connector can be easily deployed to multiple machines to provide high availability and load balancing. Since all communications are outbound only, there is no requirement for a DMZ or for the connector to be installed in a DMZ.

Moreover, in addition to the PTA feature, and in the same way it is available for the PHS feature, you can optionally set up with Azure AD Connect the seamless SSO.

## Choosing the federated identity model

Finally, the federated identity model is built on top of the synchronized identity model and adds the identity federation dimension. As already noticed, this model indeed requires to setup a standard-based federation trust relationship and thus to deploy AD FS or a supported third party identity provider solution (see later in this document).

Directory synchronization is a requirement for this model in order to keep the on-premises identity infrastructure in sync with the Azure AD/Office 365 tenant.



Figure 5 Federated Identity model

Users sign in with corporate ID for access to online and corporate services. Unlike the previous identity model, **authentication always occurs on-premises** against the organization’s identity infrastructure and users get true single sign-on (SSO). For example, in the context of this paper, AD FS queries Active Directory for authenticating users and then delivers a (signed) security token as a proof of a successful authentication to allow access to the Azure AD/Office 365 tenant.

In comparison, with the PHS feature and the so-called “same sign-on” experience with the previous synchronized identity model, users will have to re-enter at least once the same on-premises credentials when accessing Azure AD/Office 365.

Support for on-premises multi-factor authentication (MFA) can be provided if such a solution is deployed on-premises. In comparison, with both the PHS and the PTA features, only a support for multi-factor authentication (MFA) in the cloud can be provided.

Furthermore, and like with the PTA feature, IT professionals will have to manage the password policy only on-premises and hence will not need to separately worry about password reset for federated identities. The organization’s identity infrastructure stores and controls the password policy. Password reset occurs for on-premises IDs only.

Nevertheless, implementing this model requires to both deploy, operate, and maintain a highly available fault-tolerant federation infrastructure to deliver the federation service. This service is indeed critical as every access to Azure AD/Office 365 is based on security tokens that need to be issued by an AD FS – or a supported third-party identity provider - infrastructure after a successful authentication. In case the Security Token Service (STS) becomes unavailable, the possibility to fallback to password sync is offered by Azure AD.

Since the synchronized identity (with the PHS or the PTA features plus the seamless SSO feature) and the federated identity models appear to be very close in terms of both capabilities and end-user experience, and the former is easier to deploy without the requirement for a highly available fault-tolerant federation infrastructure, what could be the reasons if any to finally opt for the federated identity model in lieu of synchronized identity model?

Reasons for choosing this model generally correspond to a series of (more) advanced scenarios and relate to the following three distinct areas that are detailed in the next sections:

1. Leveraging an already existing infrastructure.
2. Complying with specific policy requirements.
3. Fulfilling technical requirements.

**Note** To give credit where credit is due, this analysis takes its inspiration from the blog post [Choosing a sign-in model for Office 365](http://blogs.office.com/2014/05/13/choosing-a-sign-in-model-for-office-365/)[[28]](#footnote-29), written by Paul Andrew, product manager on the Office 365 team.

The core recommendation is straightforward and pure common sense: **choose the synchronized identity model with the PHS or the PTA features unless you have to deal with one or more of the following scenarios**.

### Leveraging an already existing infrastructure

If your organization has already an identity federation infrastructure in place that is used to provide single sign-on for internal, partner applications, cloud-hosted SaaS, etc., the third model obviously enables to further extend this infrastructure for accessing Azure AD/Office 365 thanks to the single sign-on feature:

* If **the federation infrastructure is based on AD FS**, you will have to verify the requirements and follow the planning and configuration steps described in the next sections. This said, there is no specific obligation to implement the federated identity model simply because an AD FS service is already in place.

Note As previously mentioned, Azure AD Connect provides a single and unified wizard that streamlines the overall onboarding process for directory synchronization and single sign-on, and that automatically performs the following steps: download and setup of all the pre-requisites, download, setup and guided configuration of the synchronization, activation of the sync in the Azure AD tenant, setup, and/or configuration of AD FS, etc. (See section § Simplifying the onboarding process later in this document).

Note The [Azure Active Directory Connect Health (Azure AD Connect Health)](https://msdn.microsoft.com/en-us/library/azure/dn906722.aspx)[[29]](#footnote-30) cloud based service in the [Azure portal](https://portal.azure.com/)[[30]](#footnote-31) helps you monitor and gain insight into health, performance and login activity of your on-premises identity infrastructure. As such, it offers you the ability to view alerts, performance, usage patterns, configuration settings, enables you to maintain a reliable connection to Azure AD and much more.

The currently available release in GA not only focusses on AD FS (i.e. Azure AD Connect Health for AD FS) but also on sync to allow you to monitor and gain insights into the sync service of Azure AD Connect (i.e. Azure AD Connect Health for sync). In addition, the monitoring of the AD DS infrastructure is now available in public preview (i.e. Azure AD Connect Health for AD DS).

Azure AD Connect Health is a feature of the Azure AD Premium P1 and P2 editions and represents a key part of our effort to help you monitor and secure your cloud and on-premises identity infrastructure. For more information, see article [Monitor your on-premises identity infrastructure and synchronization services in the cloud](https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health)[[31]](#footnote-32).

* If **the organization has deployed a** **non-Microsoft identity provider**, Azure AD/Office 365 acts as a relying party/service provider with standard-based federation protocols, namely WS-Federation, WS-Trust, and SAML 2.0. The aforementioned [Works with Office 365 – Identity](http://blogs.office.com/2014/01/30/the-works-with-office-365-identity-program-now-streamlined)[[32]](#footnote-33) program provides qualification requirements, technical integration documents for the above protocols as well as information on how to conduct interoperability testing via the automated testing tool [Connectivity Analyzer](http://go.microsoft.com/?linkid=9841876)[[33]](#footnote-34), thus enabling a predictable and short qualification path. A [list of third-party identity providers’ implementation](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-federation-compatibility)[[34]](#footnote-35) has already passed the tests.

**Important note** Directory synchronization feature that can be part of the third party solution is not tested as part of the program.

**Note** The whitepaper [Azure AD/Office 365 Single Sign-on with Shibboleth 2](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[35]](#footnote-36) illustrates the configuration of the single sign-on feature with Shibboleth 2 and the SAML 2.0 protocol.

* If the enterprise is **already using Microsoft Forefront Identity Management (FIM)/Microsoft Identity Management (MIM)** to manage the on-premises identity lifecycle with multiple Active Directory and/or non-MS repositories, the [Azure AD connector](http://www.microsoft.com/en-us/download/details.aspx?id=41166)[[36]](#footnote-37) may be added, as a new connector.

**Note** For more information, see article [Windows Azure Active Directory Connector for FIM 2010 R2 Quick Start Guide](http://technet.microsoft.com/en-us/library/dn511002.aspx)[[37]](#footnote-38).

However, **Microsoft recommends that you do NOT implement a new deployment using this connector. This solution is superseded by Azure AD Connect.**

**Note** Among the missing capabilities, this connector does not provide password hash sync support. So a federation infrastructure or the PTA feature will still be required for a seamless sign-in experience. And to enable the latter, you will need Azure AD Connect to loop the loop...

### Complying with policy requirements

Following are some illustrations of the policy requirements that could make a good case for the federated identity model:

* **A true single sign-on is required** instead of the so-called “same sign-on” achieved through the PHS and the PTA features. For example, AD FS can be configured in such a way that users who are already signed in to a domain joined and connected machine do not require to re-enter any password to sign in at Windows Azure AD/Office 365. This allows to achieve such an objective. This said, with the new seamless SSO feature in public preview that can be configured with the PHS or the PTA features, users do not have to re-enter their password when they are on the corporate network thanks to the WIA support.
* **The credential synchronization to public cloud is not permitted as per security policies**. If a seamless user experience is expected and the policies in place prevents any credential to be synced to public cloud, the identity federated will be one of the solution to consider as authentication always occurs on-premises. This also banishes the password (hash of hash) synchronization as a back-up solution. However, the PTA feature should also be considered in respect to these policies.

**Note** The password hash stored in the on-premises Active Directory database is not replicated as it is in Azure AD. The synchronization engine rather re-hashes it to a SHA256 hash before transmitting it securely to Azure AD where in turn it is encrypted before being stored in the cloud database. As a result, even if the SHA256 hash of the initial hash is stolen, it could not be used as an attempt to connect to the on-premises network. For detailed information about password hash replication and protection, see blog post [AAD Password Sync, Encryption and FIPS compliance](https://blogs.technet.microsoft.com/enterprisemobility/2014/06/28/aad-password-sync-encryption-and-fips-compliance/)[[38]](#footnote-39).

* **On-premises conditional access control is a security policy requirement**. The client access policies initially introduced in the previous AD FS version 2.0 allow to control extranet access to applications. For example, with Office 365, such policies allow to restrict access to Exchange Online based on information like the user’s source IP address (for example, forbid email via Outlook from outside the corporate network) or group membership. For that purpose, AD FS allows to create, as an access control mechanism, issuance authorization claim rules that check for the existence of certain claims or inspect claim values to allow or deny access to the Azure AD/Office 365.

**Note** For more information, see article [Configuring Client Access Policies](http://technet.microsoft.com/en-us/library/dn592182.aspx)[[39]](#footnote-40).

AD FS in Windows Server 2012 R2 (and in Windows Server 2016) further enhances this access control mechanism based on multiple factors, including user, network location, device (AD Workplace Join), and authentication data. This is made possible by a greater variety of claim types available for the issuance authorization claim rules. Thus AD FS allows to enforce conditional access control based on user identity or group membership, network location, device (whether it is workplace joined), and the authentication state (whether multifactor authentication was performed), etc.

**Note** The AD Workplace Join capability allows users to join their devices with the organization’s workplace to access company resources and services. When a device is joined by Workplace Join, it becomes a known device and attributes of the device can be retrieved from AD to drive conditional access for the purpose of authorizing issuance of security tokens for applications. Windows 8.1, Windows RT 8.1, Android (Samsung), and iOS 6+ devices can be joined by using Workplace Join.

Workplace Join is made possible by Device Registration Service (DRS) that is included with AD FS. When a device is joined by Workplace Join, DRS provisions a device object in AD and sets a certificate on the consumer device that is used to represent the device identity. DRS is meant to face both internal and external resources. Organizations that deploy both DRS along with WAP can join devices that use Workplace Join from any Internet-connected location.

For more information, see article [Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications](http://technet.microsoft.com/en-us/library/dn280945.aspx)[[40]](#footnote-41).

**Note** The Azure Device Registration Service (Azure DRS) enables Workplace Join and register devices in Azure AD in lieu of on-premises with DRS. The registered devices can then be used in the conditional access policies that are available in AD FS similarly to what can be achieved through the deployment of DRS. For more information, see article [Setting up on-premises conditional access using Azure Active Directory Device Registration](https://azure.microsoft.com/en-us/documentation/articles/active-directory-conditional-access-on-premises-setup/?rnd=1)[[41]](#footnote-42).

**Note** For additional information on conditional access control, see article [Manage Risk with Conditional Access Control](http://technet.microsoft.com/en-us/library/dn280937.aspx)[[42]](#footnote-43).

* **The audit of authentication attempts to Azure AD/Office 365 is required**. An STS solution such AD FS logs inside the Windows event log all attempts and granted access to applications that are under its control. This said, auditing users sign-in and even more like conditional access risk policies are available with Azure AD Identity Protection with the Azure AD Premium P2 edition.

**Note** For more information, see article [Azure Active Directory Identity Protection](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection)[[43]](#footnote-44).

* **Login time restrictions are imposed** for any on-premises access. Such restrictions must also be applied to any Azure AD/Office 365 access. A STS solution like AD FS will automatically take in account these restrictions for new authentication requests thanks to its reliance on Active Directory. This said, if the user has been successfully authenticated and has consequently obtained a security token to gain access to Azure AD/Office 365, the security token can be used for a duration of 8 to 12 hours. This said, the PTA feature offers the same reliance on Active Directory and does not have the caveat of the security token lifetime.
* **Disabling a user account must be immediate**. A STS solution like AD FS will block users’ authentication requests as soon as their accounts are disabled thanks to its reliance on Active Directory. In the synchronized identity model, the replication of user accounts – including attributes like status disabled – occurs by default every 30 minutes, meaning that the user could at most be able to logon to Azure AD during this delay with the PHS feature.

**Note** Things are unfortunately not so simple in the federated identity model in so far as, for example with AD FS, IT professionals must take into account i) a potential replication delay between the Active Directory domain controllers, i.e. the DC where the administrative action is performed and the DC that is query by the AD FS STS, and ii) the lifetime of security tokens. Conversely, the PHS feature offers the ability to prohibit for a user the access to Azure AD/Office 365 almost immediately by resetting their password on-premises as password reset is synchronized to Azure AD within 2 minutes.

However, the PTA feature in the synchronized identity model offers the same reliance on Active Directory for the same benefit and even more without the lifetime of security tokens.

### Fulfilling technical requirements

Following are some illustrations of the technical requirements that also make a good case for the federated identity model:

* **SaaS applications, Line-of-Business (LOB)** **hybrid/cloud applications, etc.** already in place rely on federation and thus expect a security token as proof of authentication. The same requirement may apply to Office 365 and other applications accessed via Azure AD. However, as already outlined, there is no specific obligation to implement the federated identity model simply because a federation infrastructure with its STS is already in place.
* **A Self-service password reset functionality** or any other kind of permitted customization has been implemented in the above STS – like the ones proposed with AD FS using the guidelines [Customizing the AD FS Sign-in Pages](http://technet.microsoft.com/en-gb/library/dn280950.aspx)[[44]](#footnote-45) – the improved responsive mobile-friendly sign-in pages are consistent with Azure AD. IT professionals may want to standardize these capabilities for Azure AD/Office 365 as well.

**Note** As an alternate option, customization capabilities are available in the Azure AD Basic and Premium P1 and P2 editions that allow to **adapt the sign-in page to fit your company branding**, with your own logo, illustration and sign-in text. In addition, these two editions also offer a **user password reset portal** that allows users who have already registered their mobile phone numbers and alternate email addresses, to reset their password by themselves. Moreover, the password write back capability included with Azure AD Connect – that requires the Premium P1 or P2 editions of Azure AD – allows to synchronize passwords back to the on-premises Active Directory giving users the capability to manage their passwords from the cloud.

For more information, see articles [Add company branding to your sign-in and Access Panel pages](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-add-company-branding)[[45]](#footnote-46) and [Customizing Password Management to fit your organization's needs](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-customize)[[46]](#footnote-47).

* **A** **third-party on-premises multifactor authentication solution** is already in place. IT professionals may want to leverage this investment to also control access to Azure AD/Office 365. The federated identity model enables this path provided that the STS allows such an integration. This is the case with AD FS that can rely on this additional on-premises authentication.

## Suggesting a decision matrix for the identity models

Following Table 2 aims at suggesting a decision matrix to synthetize the above considerations regarding the discussed identity models.

Table 2 Decision matrix

|  | **Synchronized identity model** | **Federated identity model** |
| --- | --- | --- |
| **I need to…** | PHS | PTA |  |
| Sync new user, contact, and group accounts created in my on-premises AD to the cloud in a single-forest scenario | ✓ | ✓ | ✓ |
| Sync new user, contact, and group accounts created in my on-premises AD to the cloud in a multi-forest scenario | ✓ | ✓ | ✓ |
| Enable users to sign in with the same identity and password | ✓ | ✓ | ✓ |
| Immediately disable user accounts | ✓\* | ✓ | ✓ |
| Enable cloud-based multi-factor authentication solutions | ✓ | ✓ | ✓ |
| Enable self-service password reset with AD write-back option | ✓ | ✓ | ✓ |
| Customize the user sign-in page to Azure AD/Office 365 | ✓ | ✓ | ✓ |
| Enable users to sign in once using corporate credentials without password caching  | ✓\*\* | ✓\*\* | ✓ |
| Enable use of on-premises third-party multi-factor authentication solutions |  |  | ✓ |
| Do not replicate password hashes to the cloud |  | ✓ | ✓ |
| Restrict access based on location or group membership | ✓\*\*\* | ✓\*\*\* | ✓ |
| Allow authentication with non-MS identity providers |  |  | ✓ |
| Enable SSO for SaaS applications, hybrid applications, etc. |  | ✓\*\* | ✓ |
| Audit users sign-in to Azure AD/Office 365 | ✓\*\*\*\* | ✓\*\*\*\* | ✓ |

\* Using user password reset

\*\* With seamless SSO and on the corporate network

\*\*\* Using Azure AD conditional access. Requires a Premium P1 or P2 editions of Azure AD

\*\*\*\* Using Azure AD Identity Protection. Requires a Premium P2 edition of Azure AD

## Deploying the chosen identity model

The above identity models are configured with the Azure AD Connect tool.



Once configured, you can also change the sign-in option with Azure AD Connect by launching the wizard again and selecting **Configure**, and then **Change user sign-in**.



# Going beyond

As part of the same series of documents on Azure AD/Office 365 seamless sign-in, the **second part Build a base configuration for an evaluation environment** deals with an end-to-end walkthrough to rollout a working base configuration in an Azure-based test lab environment. As such, it describes as its name suggests the essential steps required to configure a base configuration to test the various above discussed identity models. By:

* Deploying the Azure Resource Manager (ARM) template that come along,
* Following the outlined steps,

you will have a common starting point to test and evaluate the identity models, and leverage for that purpose the same baseline for a typical on-premises environment. Windows Server 2012 R2 and Windows Server 2016 are both featured so that you can pick up the version that best corresponds to your environment and/or fulfils your requirements.

Through its support for standard protocols, Active Directory Federation Services (AD FS) provides claims-based (Web) single sign-on (a.k.a. identity federation) with Azure AD, and related online services such as the Microsoft Office 365 offering and its Web application and rich client applications.

The **third part Understand single sign-on (SSO) with AD FS in Windows Server 2012 R2** is intended as an overview document for further understanding the federated identity model with AD FS, how to enable single sign-on using corporate Active Directory credentials and AD FS to Azure AD/Office 365, and the different configuration elements to be aware of for such deployment.

The **fourth part Implement single sign-on (SSO) with AD FS in Windows Server 2012 R2** further illustrates how to deploy it onto the above base configuration with Azure AD Connect.

It provides a complete end-to-end walkthrough to rollout a fully operational configuration in Azure with AD FS in Windows Server 2012 R2, and leverages, for that purpose, the base configuration depicted and established in the second part for a test lab environment.

The **fifth part Implement single sign-on (SSO) with AD FS in Windows Server 2016** covers the same considerations with Windows Server 2016.

The **sixth part Understand and implement PHS and seamless SSO** covers discusses the Password hash synchronization (PHS) model. It illustrates how to enable PHS and seamless SSO using corporate Active Directory credentials to access Azure AD/Office 365, and the different configuration elements to be aware of for such deployment. This document also provides a complete end-to-end walkthrough to rollout a fully operational configuration in Azure. It also leverages for that purpose the above base configuration.

Finally, the **seventh and final part Understand and implement PTA and seamless SSO** discusses the PTA model.

**This concludes the first part of this whitepaper.**

|  |
| --- |
| 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.© 2017 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. Microsoft Office 365: http://office.microsoft.com/en-us/business/ [↑](#footnote-ref-2)
2. Overview of Office 365 ProPlus: http://technet.microsoft.com/en-us/library/gg702619(v=office.15).aspx [↑](#footnote-ref-3)
3. Office 365 Plan Options: http://technet.microsoft.com/en-US/library/office-365-plan-options.aspx [↑](#footnote-ref-4)
4. Getting started guide for deploying Office 365 ProPlus: http://technet.microsoft.com/en-us/library/jj839718(v=office.15) [↑](#footnote-ref-5)
5. Office 365 Community web site: http://community.office365.com/en-us/default.aspx [↑](#footnote-ref-6)
6. EWS Managed API, EWS, and web services in Exchange: http://msdn.microsoft.com/en-us/library/office/dd877012(v=exchg.150).aspx [↑](#footnote-ref-7)
7. Office for Mobile Devices: http://products.office.com/en-us/mobile/Office [↑](#footnote-ref-8)
8. Gartner, “2013 Planning Guide: Identity and Privacy,” November 2012 [↑](#footnote-ref-9)
9. Microsoft Azure Active Directory Connect: http://www.microsoft.com/en-us/download/details.aspx?id=47594 [↑](#footnote-ref-10)
10. Azure Active Directory editions: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-editions [↑](#footnote-ref-11)
11. Azure Active Directory Pricing: http://azure.microsoft.com/en-us/pricing/details/active-directory/ [↑](#footnote-ref-12)
12. Azure subscription and service limits, quotas, and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#active-directory-limits [↑](#footnote-ref-13)
13. Set up multi-factor authentication for Office 365 users: https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6 [↑](#footnote-ref-14)
14. Manage your settings for two-step verification: https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/multi-factor-authentication-end-user-manage-settings [↑](#footnote-ref-15)
15. Office 365 portal: https://portal.office.com [↑](#footnote-ref-16)
16. Integrating your on-premises identities with Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect [↑](#footnote-ref-17)
17. Upgrade Windows Azure Active Directory Sync (“DirSync”) and Azure Active Directory Sync (“Azure AD Sync”): https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-dirsync-deprecated [↑](#footnote-ref-18)
18. Azure AD Connect: Version Release History: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-version-history/ [↑](#footnote-ref-19)
19. Azure AD Connect 1.1 is now GA – Faster sync times, automatic upgrades and more!: https://blogs.technet.microsoft.com/enterprisemobility/2016/02/18/azure-ad-connect-1-1-is-now-ga-faster-sync-times-automatic-upgrades-and-more/ [↑](#footnote-ref-20)
20. Azure AD & Windows 10: better Together for Work and School: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-21)
21. AAD Password Sync, Encryption and FIPS compliance: https://blogs.technet.microsoft.com/enterprisemobility/2014/06/28/aad-password-sync-encryption-and-fips-compliance/ [↑](#footnote-ref-22)
22. Implementing password synchronization with Azure AD Connect sync: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-synchronization [↑](#footnote-ref-23)
23. What is Single Sign On (SSO) (preview): https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso [↑](#footnote-ref-24)
24. Introducing #AzureAD Pass-Through Authentication and Seamless Single Sign-on: https://blogs.technet.microsoft.com/enterprisemobility/2016/12/07/introducing-azuread-pass-through-authentication-and-seamless-single-sign-on/ [↑](#footnote-ref-25)
25. What is Azure AD Pass-through Authentication: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication [↑](#footnote-ref-26)
26. Configuring Alternate Login ID: https://technet.microsoft.com/en-us/library/dn659436.aspx [↑](#footnote-ref-27)
27. Azure AD Application Proxy Connector: https://download.msappproxy.net/subscription/d3c8b69d-6bf7-42be-a529-3fe9c2e70c90/connector/download [↑](#footnote-ref-28)
28. Choosing a sign-in model for Office 365: http://blogs.office.com/2014/05/13/choosing-a-sign-in-model-for-office-365/ [↑](#footnote-ref-29)
29. Azure Active Directory Connect Health: https://msdn.microsoft.com/en-us/library/azure/dn906722.aspx [↑](#footnote-ref-30)
30. Azure Preview Portal: https://portal.azure.com/ [↑](#footnote-ref-31)
31. Monitor your on-premises identity infrastructure and synchronization services in the cloud: https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health [↑](#footnote-ref-32)
32. The Works with Office 365 – Identity program now streamlined: http://blogs.office.com/2014/01/30/the-works-with-office-365-identity-program-now-streamlined [↑](#footnote-ref-33)
33. Connectivity Analyzer: http://go.microsoft.com/?linkid=9841876 [↑](#footnote-ref-34)
34. Azure AD federation compatibility list: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-federation-compatibility [↑](#footnote-ref-35)
35. Azure AD/Office 365 Single Sign-On with Shibboleth 2: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-36)
36. Forefront Identity Manager Connector for Windows Azure Active Directory: http://www.microsoft.com/en-us/download/details.aspx?id=41166 [↑](#footnote-ref-37)
37. Windows Azure Active Directory Connector for FIM 2010 R2 Quick Start Guide: http://msdn.microsoft.com/en-us/library/dn511002(v=ws.10).aspx [↑](#footnote-ref-38)
38. AAD Password Sync, Encryption and FIPS compliance: https://blogs.technet.microsoft.com/enterprisemobility/2014/06/28/aad-password-sync-encryption-and-fips-compliance/ [↑](#footnote-ref-39)
39. Configuring Client Access Policies: http://technet.microsoft.com/en-us/library/dn592182.aspx [↑](#footnote-ref-40)
40. Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications: http://technet.microsoft.com/en-us/library/dn280945.aspx [↑](#footnote-ref-41)
41. Setting up on-premises conditional access using Azure Active Directory Device Registration: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-on-premises-setup [↑](#footnote-ref-42)
42. Manage Risk with Conditional Access Control: http://technet.microsoft.com/en-us/library/dn280937.aspx [↑](#footnote-ref-43)
43. Azure Active Directory Identity Protection: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection [↑](#footnote-ref-44)
44. Customizing the AD FS Sign-in Pages: http://technet.microsoft.com/en-gb/library/dn280950.aspx [↑](#footnote-ref-45)
45. Add company branding to your Sign In and Access Panel pages: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-add-company-branding [↑](#footnote-ref-46)
46. Customizing Password Management to fit your organization's needs: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-customize [↑](#footnote-ref-47)