An overview of Azure Active Directory

Overview Technical Article

Microsoft France

Published: December 2013 (updated: June 2016)

Version: 2.0c

Author: Philippe Beraud (Microsoft France)

Reviewers: Arnaud Jumelet (Microsoft France), Christophe Leroux, Philippe Maurent (Microsoft Corporation)

For the latest information on Azure Active Directory, please see

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

Copyright © 2016 [Microsoft Corporation](http://www.microsoft.com). All rights reserved.

Abstract: Identity management, provisioning, role management, and authentication are key services both on-premises and through the (hybrid) cloud. With the Bring Your Own Apps (BYOA) for the cloud and Software as a Service (SaaS) applications, the desire to better collaborate a la Facebook with the “social” enterprise, the need to support and integrate with social networks, which leads to a Bring Your Own Identity (BYOI) trend, identity becomes a service where identity “bridges” in the cloud talk to on-premises directories or the directories themselves move and/or are located in the cloud.

Active Directory (AD) is a Microsoft brand for identity related capabilities. In the on-premises world, AD provides a set of identity capabilities and services and is hugely popular (88% of Fortune 1000 and 95% of enterprises use AD). Azure Active Directory (Azure AD) is AD reimagined for the cloud, designed to solve for you the new identity and access challenges that come with the shift to a cloud-centric, multi-tenant world.

Azure AD can be truly seen as an Identity Management as a Service (IdMaaS) cloud multi-tenant service. This document is intended for IT professionals, system architects, and developers who are interested in understanding the various options for managing and using identities in their (hybrid) cloud environment based on the Azure AD offerings and how to leverage their related capabilities.

Table of Contents

[Introduction 4](#_Toc454202917)

[Objectives of this paper 5](#_Toc454202918)

[Non-objectives of this paper 6](#_Toc454202919)

[Organization of this paper 6](#_Toc454202920)

[About the audience 6](#_Toc454202921)

[What is Azure AD? 7](#_Toc454202922)

[Editions of Azure AD 10](#_Toc454202923)

[Anatomy of Azure AD 16](#_Toc454202924)

[Creating multiple directories in Azure AD 26](#_Toc454202925)

[Deleting a specific directory in Azure AD 29](#_Toc454202926)

[Managing directory configuration 31](#_Toc454202927)

[Extending your on-premises identity infrastructure with Azure 31](#_Toc454202928)

[Managing the Internet domains for your directory 36](#_Toc454202929)

[Synchronizing your directory with the on-premises directories 39](#_Toc454202930)

[Federating your directory with the on-premises directories 54](#_Toc454202931)

[Many applications, one identity repository 63](#_Toc454202932)

[Discovering all cloud applications in use within your organization 63](#_Toc454202933)

[Leveraging pre-integrated popular SaaS applications 67](#_Toc454202934)

["Bringing Your Own Application" (BYOA) 75](#_Toc454202935)

[Accessing your on-premises web applications on the Internet 87](#_Toc454202936)

[Providing identity and access management to (your) modern business applications 95](#_Toc454202937)

[Managing access to applications 98](#_Toc454202938)

[Assigning/Removing users 98](#_Toc454202939)

[Using groups to control access 101](#_Toc454202940)

[Leveraging dynamic groups 102](#_Toc454202941)

[Registering the devices 103](#_Toc454202942)

[Using Conditional Access Control 107](#_Toc454202943)

[Monitoring and protecting access to applications and beyond 111](#_Toc454202944)

[Monitoring security reports and blocking users 111](#_Toc454202945)

[Using Azure Multi-Factor Authentication 115](#_Toc454202946)

[Leveraging the Privileged Identity Management service 116](#_Toc454202947)

[Empowering users 122](#_Toc454202948)

[Using the Azure AD Access Panel 122](#_Toc454202949)

[Editing the profile settings for the users 123](#_Toc454202950)

[Self-service password reset for cloud users 125](#_Toc454202951)

[Self-service group management for users 129](#_Toc454202952)

[Accessing applications from the Azure AD Access Panel 131](#_Toc454202953)

[Self-service for application access 134](#_Toc454202954)

[Customizing the Azure AD Access Panel (and the Sign-in page) 137](#_Toc454202955)

[Using the “My Apps” mobile applications 140](#_Toc454202956)

# Introduction

The cloud is changing the way in which applications are written. Accelerated market cycles, multi-tenancy, pure cloud solutions and hybrid deployments, web programmability, and the rise of devices (smartphones, tablets, etc.) as well as rich clients as consumption models offer without any doubt new opportunities.

[Modern business applications](http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx)[[1]](#footnote-1) also present at the same time new challenges for the key services both on-premises and through the (hybrid) cloud that represent the identity management, the provisioning, the role management, and the authentication.

With:

* The "Bring Your Own Apps" (BYOA) for cloud and Software-as-a-Service (SaaS) applications,
* The desire to better collaborate a la Facebook with the “social” enterprise,
* The need to support and integrate with social networks, which lead to a "Bring Your Own Identity" "(BYOI) trend,
* Etc.

Identity becomes a service where identity “bridges” in the cloud “talk” to on-premises directories or the directories themselves move and/or are located in the cloud (see Gartner report [2013 Planning Guide: Identity and Privacy](http://www.gartner.com/id=2221415)[[2]](#footnote-2)).

Identity, like compute, storage and networking, is an essential platform service. In the same way that identity played a critical role in the adoption of workgroup computing, identity services will play a critical role as organizations adopt the cloud. Organizations will use cloud services and applications created by ISVs, Platform-as-a-Service (PaaS) cloud platforms for (Line of Business (LOB)) custom development, as well as Infrastructure-as-a-Service (IaaS) cloud environment for specific workloads, or part of them, to onboard the cloud for IT optimization reasons.

Kim Cameron, Microsoft Chief Identity Architect, is convinced[[3]](#footnote-3) that “organizations will find they need new identity management capabilities to take full advantage of the cloud. They will also find that the most reliable and cost-effect way to obtain these capabilities is through Identity Management as a Service – i.e. using the cloud to master the cloud.

We can therefore predict with certainty that almost all organizations will subscribe to identity services that are cheaper, broader in scope and more capable than the systems of today.

Enterprises will use these services to manage authentication and authorization of internal employees, the supply chain, and customers (including individuals), leads and prospects. Governments will use them when interacting with other government agencies, enterprises and citizens.

Identity Management as a Service will require that we move beyond the models of identity management that have guided our thinking to date. A new service-based model will emerge combining more advanced capabilities with externalization of operations to achieve reduction in risk, effort and cost."

## Objectives of this paper

**Azure Active Directory (Azure AD) is Microsoft’s vehicle for providing Identity Management as a Service (IdMaaS) capabilities in a public cloud.**

As a complement of the white paper Active Directory from the on-premises to the Cloud, which is part of the same series of documents available on the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[4]](#footnote-4), this paper provides you with a "guided tour" of Azure AD to:

* Learn about its various editions and the related capabilities.
* Learn about its interfaces such as the various endpoints published to sustain standard-based protocols for modern business applications.
* Discover its compelling capabilities such as the ones provided by the Application Access Enhancements for Azure AD that simplifies managing access to thousands of pre-integrated SaaS applications[[5]](#footnote-5). You can expect to even see additional identity and access management capabilities in the future.
* Understand how it can work in concert with on-premises Windows Server Active Directory (AD) (or non-AD sources), as well as the possible options to perform federated provisioning and synchronization of identity information from these sources to Azure AD.
* Etc.

This paper can be seen a starting point for anyone challenged with identity, provisioning, federation or cloud based authentication, interested in leveraging efficiencies of the cloud and automation to get efficiencies in identity and access management, and consequently in leveraging an IdMaaS solution. They will directly tackle these areas.

Note For additional information, see the Microsoft MSDN article [Getting started with Azure AD](http://msdn.microsoft.com/en-us/library/dn655157.aspx)[[6]](#footnote-6).

This document is an attempt to present the most important features and capabilities of Azure AD as available – in general availability (GA) or in public preview – at the time of this writing.

Even more Azure AD functionalities will be integrated over the next year(s) for your identities in the cloud. Since its general availability in April 2013, Azure AD indeed keeps continuing to receive enhancements that make Azure AD even more useful for IT professionals and developers.

Note Please make sure you periodically check the [Azure AD community forum](http://social.msdn.microsoft.com/Forums/en-US/WindowsAzureAD/threads)[[7]](#footnote-7) as well as the MSDN [Azure blog](http://blogs.msdn.com/b/windowsazure/)[[8]](#footnote-8) for notification of upcoming enhancement and changes that relate to Azure AD.

**This document will thus evolve over the time on a regular basis to reflect such additions and enhancements. This document constitutes the third revision.**

## Non-objectives of this paper

This document doesn’t discuss the deployment and configuration of Windows Server AD (WSAD) on-premises.

This document is intended as an overview document for the Azure AD offerings, and as such, it doesn’t provide neither in-depth description nor detailed step-by-step instructions on how to implement a specific covered feature or capability. Where necessary, it instead refers to more detailed documents, articles, and blog posts that describe a specific feature or capability.

## Organization of this paper

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

* What is Azure AD?
* Managing directory configuration
* Many applications, one identity repository
* Managing access to applications
* Monitoring and protecting access to applications
* Empowering users

## About the audience

This document is intended for IT professionals, system architects, and developers who are interested in understanding the various options for managing and using identities in their (hybrid) cloud environment based on the Azure AD offerings foundation and how to leverage their related capabilities.

AD, AD in Azure and Azure AD are indeed useful for slightly different scenarios. We recommend using Azure AD in addition to on-premises AD (and AD in Azure) in most cases as one doesn’t replace the other.

# What is Azure AD?

As mentioned in the introduction, Azure Active Directory (AD) is Microsoft’s vehicle for providing IdMaaS capabilities in a public cloud. Microsoft’s approach to IdMaaS is deeply grounded in – and extends – the proven concepts of on-premises Active Directory (AD).

Active Directory (AD) is a Microsoft brand for identity related capabilities. In the on-premises world, Windows Server Active Directory (WSAD or simply AD) provides a set of identity capabilities and services and is hugely popular (88% of Fortune 1000 and 95% of enterprises use AD).

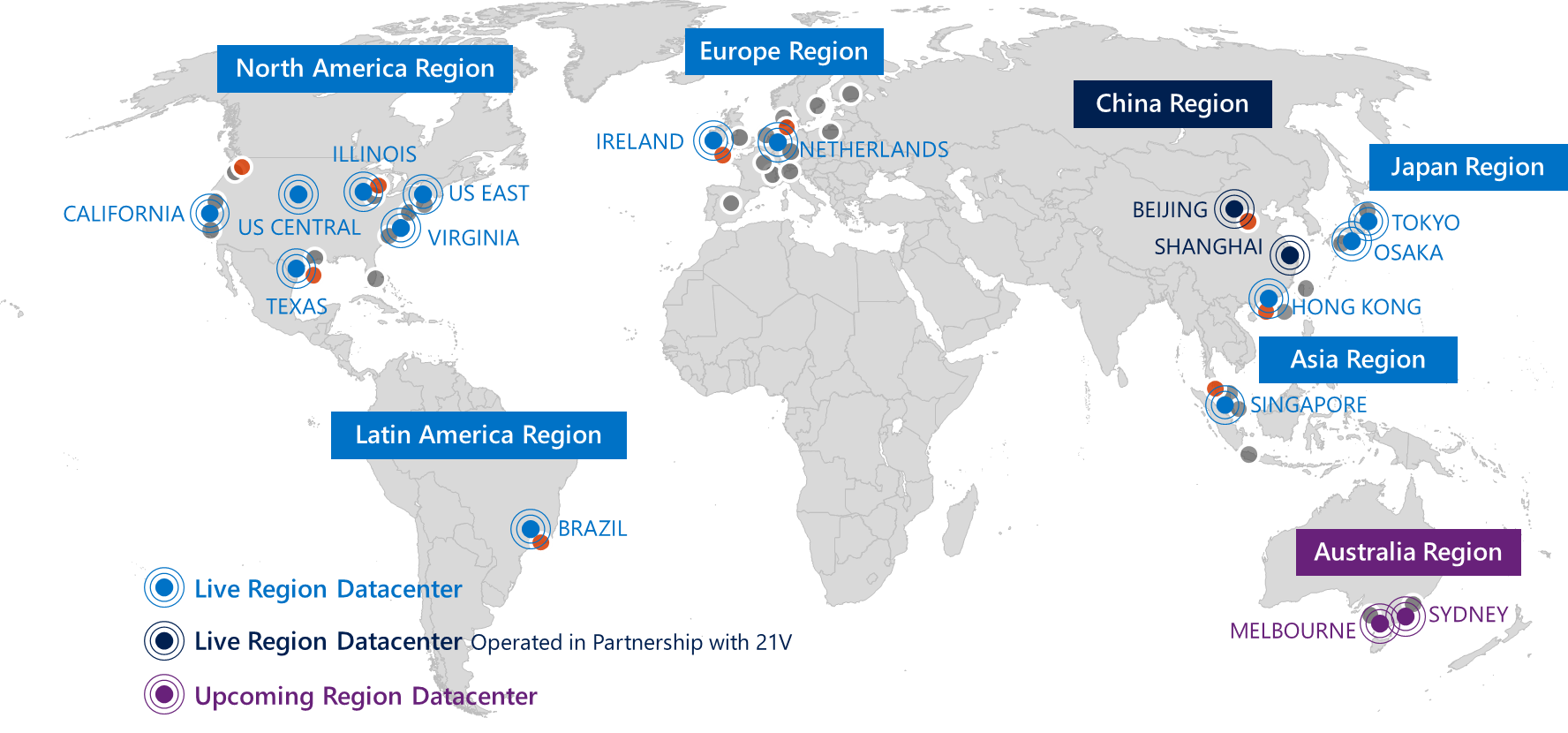
The foundational concept of on-premises AD is that the content of the directory is the property of the organization deploying it and access to and use of that content is completely under the organization’s control. This is also the fundamental concept behind Azure AD.

**Azure AD is NOT a monolithic directory of information belonging to Microsoft, but rather, at the time of writing, more than four million different directories belonging to and completely controlled by different organizations.**

**This architecture and commitment is called “multi-tenant” and great care has been provided to insulate tenants (organizations) from each other and from their service operator – Microsoft.**

We have indeed re-engineered AD[[9]](#footnote-9) [[10]](#footnote-10), to support massive scale, devices based on any operating system or architecture, [modern business applications](http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx)[[11]](#footnote-11), modern protocols, high availability, and integrated disaster recovery.

Since its introduction, Azure AD "has handled 400 billion identity authentications in Azure AD"[[12]](#footnote-12). "We have 350 million Azure Active Directory users. […] We actually process 4 billion, with a B, authentications every week with Azure Active Directory"[[13]](#footnote-13). This is a real testament to the level of scale we can handle. “At a high level, Azure AD is a high availability, geo-redundant, multi-tenanted, multi-tiered cloud service that has delivered 99.99% uptime for over a year now. We run it across 28[[14]](#footnote-14) datacenters around the world. Azure AD has stateless gateways, front end servers, application servers, and sync servers in all of those data centers. Azure AD also has a distributed data tier that is at the heart of our high availability strategy. Our data tier holds more than 500 million objects and is running across 13 data centers.” [[15]](#footnote-15)

****

Since we first talked about it in November 2011, and with such above numbers in mind, Azure AD has shown itself to be a robust identity and access management service for Microsoft cloud services. **No other cloud directory offers this level of enterprise reliability or proven scale.** Quoting from the report [KuppingerCole Leadership Compass Cloud User and Access Management](http://news.microsoft.com/itanalyst/docs/06-20-14CompassCloudUser.pdf)[[16]](#footnote-16): "Looking at the Market Leadership chart, we see Microsoft being the clear leader. This is based on the fact that their Azure Active Directory on one hand shows good direct acceptance and on the other builds the foundation for widely used Microsoft Office 365. Furthermore, Microsoft has an exceptionally strong partner ecosystem."

Furthermore, last year, Gartner in their Magic Quadrant (MQ) for Identity Management as a Service (IDaaS) [Gartner, June 2015] has placed Azure AD after its only first year of availability in the “Visionaries” MQ.

As of this writing, **Gartner has just released their MQ for IDaaS for 2016 [Gartner June 2016] and Azure AD Premium has been placed in the “Leaders” quadrant**, and positioned very strongly for our completeness of vision.



Important note The above graphic was published by Gartner, Inc. as part of the larger research document - a complimentary access is provided [here](https://info.microsoft.com/EMS-IDaaS-MQ-2016.html)[[17]](#footnote-17)- and should be evaluated in the context of the entire document. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

As Alex Simons, Director of Program Management, Microsoft Identity and Security Services Division, says, “we’re thrilled with the result. It really validates our vision of providing a complete solution for hybrid identity and access for supporting employees, partners and customers all backed by world class security based on Microsoft’s intelligent security graph. This result says a lot about our commitment in the identity and access management space but more importantly about our customers, implementation partners and ISV partners who have worked together with us. They have been awesome about sharing their time and energy every day, to make sure that the products and services we build meet their needs and are helping them position their companies to thrive in the emerging world of cloud and devices.

You might be surprised to know that Microsoft also is the only vendor in the Leader quadrant across Gartner’s Magic Quadrants for IDaaS, Cloud Infrastructure as a Service (IaaS), Server Virtualization, Application Platform as a Service, Cloud Storage Services, and as a leader across the data platform and productivity services. This really shows you why customers are choosing Microsoft across the full spectrum of cloud computing – our services are well integrated and also among the best available in their individual categories.”[[18]](#footnote-18)

Alex Simons adds: “our effort doesn’t stop here. We have a lot of hard work ahead of us and we are planning to deliver more innovative capabilities to further improve our position in the “leaders” quadrant.”[[19]](#footnote-19).

This said, a number of people are (still) surprised to find out that every Office 365 customer already has an Azure AD directory.  **Azure AD is the directory behind Microsoft Online Services subscriptions like Office 365, Dynamics CRM Online, Intune, etc. and is used to store user identities and other tenant properties**. Just like the on-premises AD stores the information for Exchange, SharePoint, Lync and your custom LOB applications, Azure AD for instance stores the information for Exchange Online, SharePoint Online, Lync Online and any custom applications build in the Microsoft’s cloud (or in another cloud).

It is possible to extend the usage of these directory tenants to other LOB based applications you’re developing and/or to [thousands](http://azure.microsoft.com/en-us/marketplace/active-directory/)[[20]](#footnote-20) of cloud pre-integrated SaaS applications like ADP, Concur, Google Apps, Salesforce.com and others, regardless of the public cloud they are hosted on. The pre-integrated SaaS applications are preconfigured via an application gallery with all the parameters needed to at least provide a seamless sign-in experience with them, thanks to the [Application Access Enhancements for Azure AD](http://technet.microsoft.com/en-us/library/dn308588.aspx)[[21]](#footnote-21) (see later in this document).

## Editions of Azure AD

Azure AD is available in three different editions to choose from:

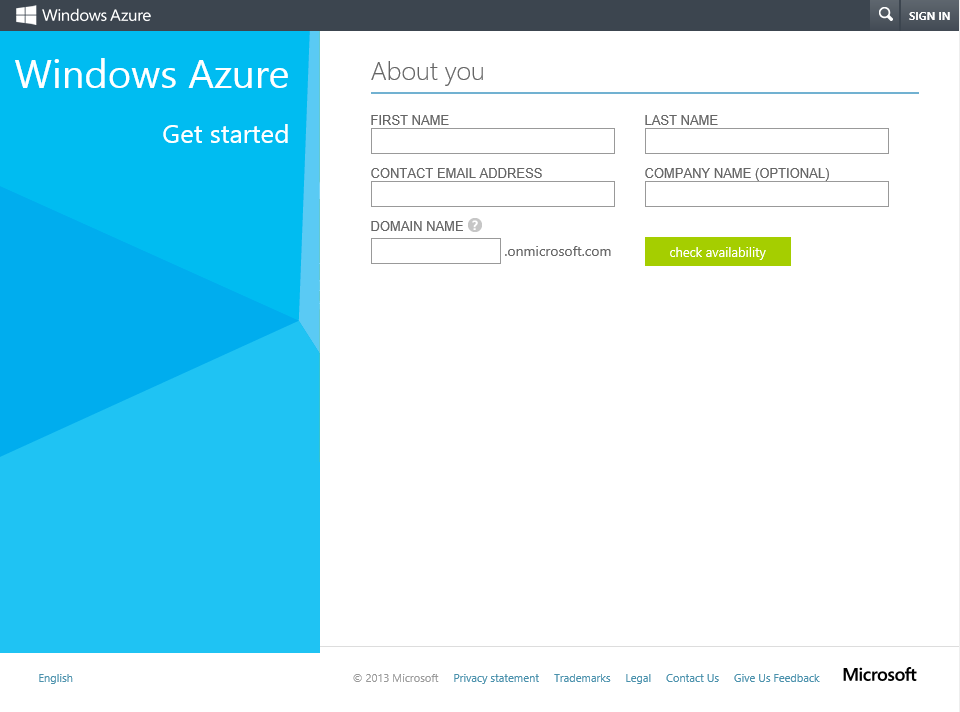
1. **Azure Active Directory (Free)**. With the Free edition of Azure AD, you can manage user accounts, synchronize with on-premises directories, and get single sign-on across Azure, Office 365, and thousands of popular SaaS applications.

Note This is a free edition as being used by the above Microsoft Online Services subscriptions. If you’ve already subscribed to a Paid Office 365 subscription, you can benefit from an Azure $0 subscription that you can use to access the [Azure management portal](http://manage.windowsazure.com)[[22]](#footnote-22) with your existing Office 365 subscription in order to directly manage the related Azure AD tenant with all the access management and security feature set and thus [empower](http://blogs.technet.com/b/ad/archive/2013/09/10/empower-your-office-365-subscription-identity-management-with-application-access-enhancements-for-windows-azure-ad.aspx)[[23]](#footnote-23) your Office 365 subscription. For example, the aforementioned Application Access Enhancements for Azure AD can be only managed today by accessing the directory through the Azure management portal. You can sign-up for this $0 subscription by following the link <https://account.windowsazure.com/PremiumOffer/Index?offer=MS-AZR-0110P&whr=azure.com>.

Note Independently of any Microsoft Online Services subscriptions, 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>.

The first user you generate as part of the sign-up process based on the fields below will also be an administrator of the directory. This user will be declared in the default domain of the directory tenant *<domain name>*.onmicrosoft.com. You will sign in to Azure with this account.

Note Contrary to other Azure resources, your Azure AD directories are not child resources of an Azure subscription. So if you cancel or allow your Azure subscription to expire, you can still access your directory data using Windows PowerShell, the Azure AD Graph API (see later in this document), or other interfaces such as the Office 365 administration console.



1. **Azure Active Directory Basic**. Azure AD Basic provides the application access and self-service identity management requirements of task workers with cloud-first needs. With the Basic edition of Azure AD, you get all the capabilities that Azure AD Free has to offer, plus group-based access management, self-service password reset for cloud applications, customizable environment for launching enterprise and consumer cloud applications, and an enterprise-level SLA of 99.9 percent uptime.

An administrator with Azure AD Basic edition can activate an Azure AD Premium trial.

Note For additional information, see the blog post [Azure Active Directory Basic is now GA!](http://blogs.technet.com/b/ad/archive/2014/09/15/azure-active-directory-basic-is-now-ga.aspx)[[24]](#footnote-24).

1. **Azure Active Directory Premium**. With the Premium edition of Azure AD, you get all of the capabilities that Azure AD Free and Azure AD Basic have to offer, plus additional feature-rich enterprise-level identity management capabilities.

The edition in part of the [Enterprise Mobility Suite (EMS)](http://www.microsoft.com/en-us/server-cloud/products/enterprise-mobility-suite/)[[25]](#footnote-25) offering, a comprehensive and cost effective solution for enterprise mobility needs.

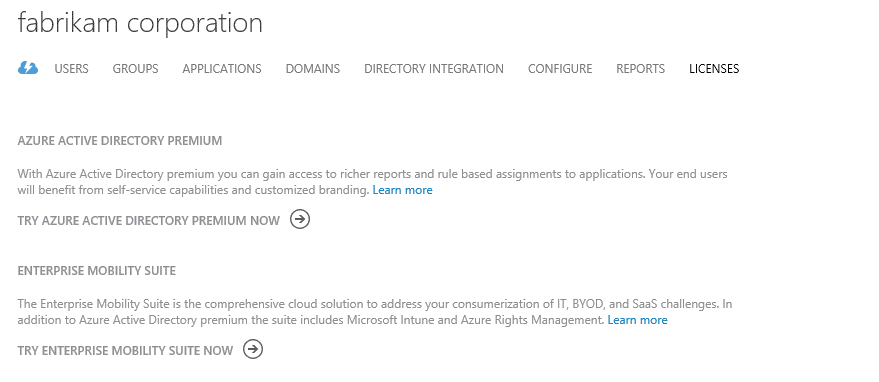
Note The EMS offering is not only available with an [Enterprise Agreement (EA)](http://www.microsoft.com/en-us/Licensing/licensing-programs/enterprise.aspx)[[26]](#footnote-26) but also through the Microsoft’s [Cloud Solution Provider (CSP)](https://mspartner.microsoft.com/en/us/pages/solutions/cloud-reseller-overview.aspx)[[27]](#footnote-27) and [Open](http://www.microsoft.com/licensing/licensing-options/open-license.aspx)[[28]](#footnote-28) programs. For additional information, see the blog post [Azure AD and Enterprise Mobility Suite now available without an Enterprise Agreement](http://blogs.technet.com/b/ad/archive/2015/03/12/azure-ad-and-enterprise-mobility-suite-now-broadly-available-outside-of-an-enterprise-agreement.aspx)[[29]](#footnote-29).

Note For a description of each edition below and a comparison table, see the Microsoft MSDN article [Azure Active Directory editions](http://msdn.microsoft.com/en-us/library/azure/dn532272.aspx)[[30]](#footnote-30). For more information on usage model, see the Microsoft MSDN article [Azure Active Directory Pricing](http://www.windowsazure.com/en-us/pricing/details/active-directory/)[[31]](#footnote-31). For information on the usage constraints and other service limits for the Azure AD service per edition, see the Microsoft MSDN article [Azure AD service limits and restrictions](http://msdn.microsoft.com/en-us/library/azure/dn764971.aspx)[[32]](#footnote-32).

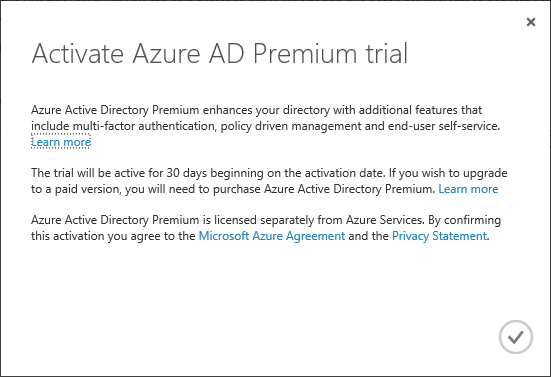
To sign-up today for Azure Active Directory Premium features, proceed with the following steps:

Note For additional information about how to sign up and start using the Premium edition, see the Microsoft MSDN article [Getting started with Azure AD Premium](http://msdn.microsoft.com/en-us/library/azure/dn499825.aspx)[[33]](#footnote-33). You can also watch the Channel 9 demo videos [Enabling Azure Active Directory Premium trial](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Enabling-Azure-Active-Directory-Premium-trial)[[34]](#footnote-34), [How to Purchase Azure Active Directory Premium - New Customers](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/How-to-Purchase-Azure-Active-Directory-Premium-New-Customers)[[35]](#footnote-35), and [How to Purchase Azure Active Directory Premium - Existing Customers](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/How-to-Purchase-Azure-Active-Directory-Premium-Existing-Customer)[[36]](#footnote-36).

1. Sign into the classic Azure management portal as the global administrator of the directory you wish to customize.
2. Click **ACTIVE DIRECTORY**, and then select the directory where you want to assign licenses.
3. Select **LICENSES**.



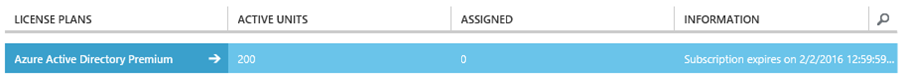
1. Click **TRY AZURE ACTIVE DIRECTORY PREMIUM NOW**.



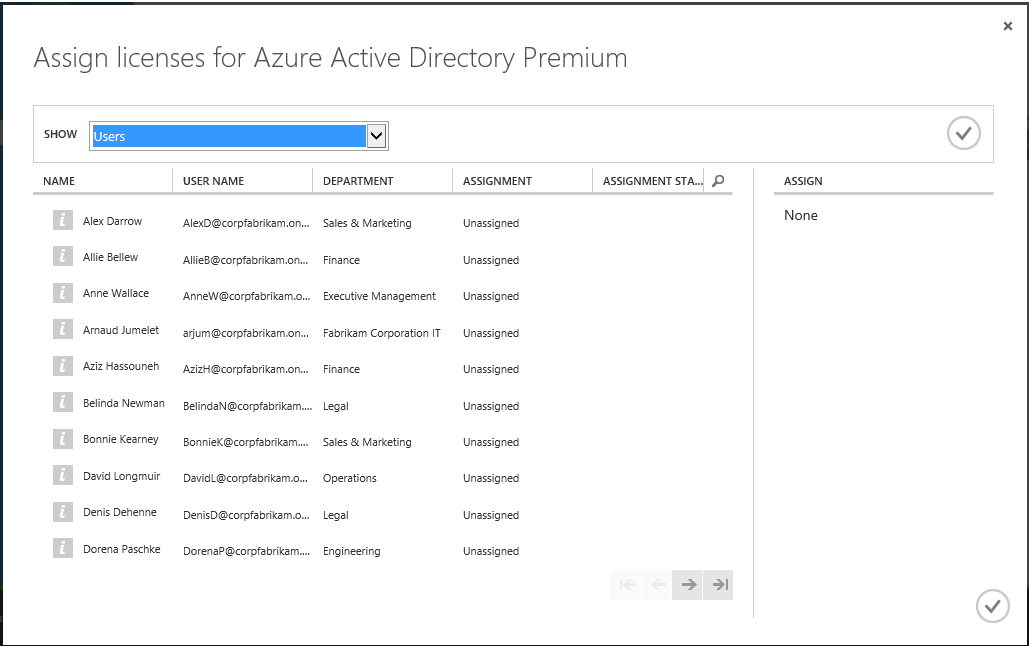
1. Click the check mark icon to activate the trial.



1. Once activated, you can start assigning premium licenses to your users.



Click **ASSIGN**.

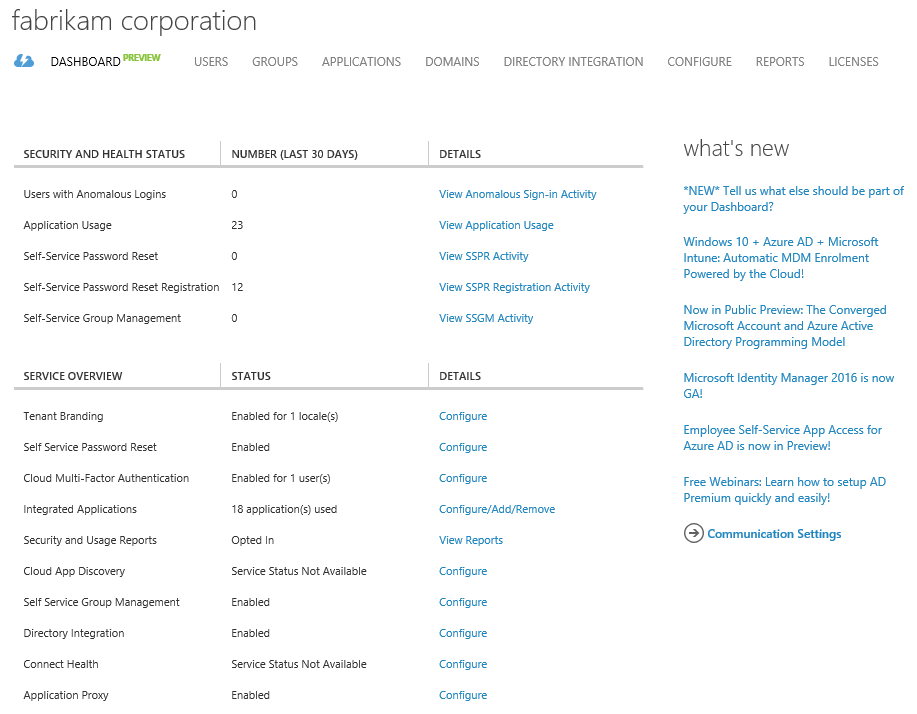


1. In the **Assign licenses for Azure Active Directory Premium** dialog box, select the users you want to assign licenses to, and then click the check mark icon to save the changes.

You can alternatively set the view filter to group (all groups) in **SHOW**, and then select the groups that you want to assign. Confirm the selection by clicking the check mark icon to save the changes.

Note For additional information, see the blog post [Simplified License Assignment with Azure AD and EMS](http://blogs.technet.com/b/ad/archive/2014/09/18/simplified-license-assignment-with-azure-ad-and-ems.aspx)[[37]](#footnote-37). You can also watch the Channel 9 demo videos [How to assign EMS/Azure AD Premium licenses to user accounts](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/How-to-assign-Azure-AD-Premium-Licenses-to-user-accounts)[[38]](#footnote-38) and [Assign EMS/Azure AD Premium licenses with PowerShell](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Assign-EMS-Azure-AD-Premium-lics-with-PowerShell)[[39]](#footnote-39).

The premium edition of azure AD provides a dashboard for the directory, which is the one place to manage all of your services. It also makes it easy for you to keep up with new features and events.



Note For additional information, see the blog post [Azure AD Premium Dashboard is in preview!](http://blogs.technet.com/b/ad/archive/2015/09/15/azure-ad-premium-dashboard-is-in-preview.aspx)[[40]](#footnote-40).

The rest of this section describes the main characteristics of Azure AD (regardless of the "flavor", i.e. the edition) that organizations and cloud-based applications can leverage, as well as the core functionalities that Azure AD provides for the users of these applications and for the developers of these applications to be successful.

In terms of key scenarios, Azure AD can:

* Be a **centralized "organization-owned" repository** for all identities and cloud hosted applications.
* Provide a comprehensive console for the administrator to manage identities, synchronization with on-premises directory services and assign (or remove) application access.
* Monitor and protect access to many applications using built in security features such as the cloud-based Azure Multi-Factor Authentication (MFA) and security and audit reporting.
* Empower information workers with true single sign-on for their enterprise SaaS applications from a single web page, i.e. the Azure AD Access Panel.

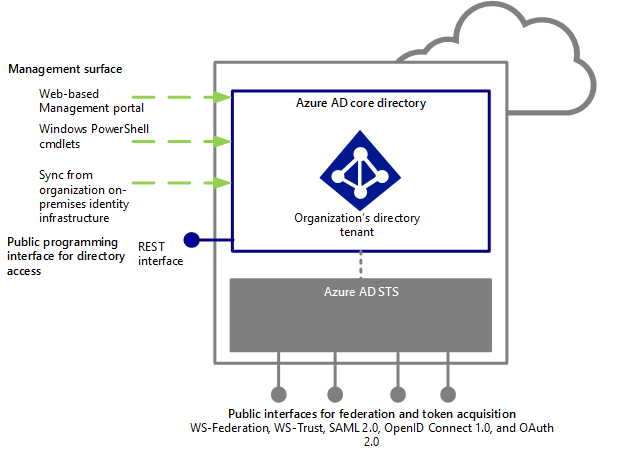
A description for all of the above is provided in a dedicated section.

Let’s consider the anatomy of Azure AD.

## Anatomy of Azure AD

At the simplest level, Azure AD is a scalable directory infrastructure that provides for storage, data access, replication and synchronization, device registration, and security token services (STS).

Below is a conceptual diagram showing the public interfaces, and the management surface area:



### Core directory service

The core directory service represents the heart of Azure AD. As a directory service in the cloud and with the objective to eliminate the need of an application-specific store for notably identity information, Azure AD aims at supporting - within organization owned tenant(s) - data of common interest across the vast majority applications whether they are cloud, SaaS, mobile, etc. applications as well as the possible relationships between those data.

#### Data model and schema

Users and groups are typically good examples where organizations want to create them once and reuse them across their applications or the ones for which they buy a subscription.

Information in the core directory service should generally have the following characteristics:

* Public in the sense of something that is useful to share across the organization, and not something private like the salary attribute of a user object,
* Mostly static over the time, and not changed often,
* Small, generally pointers to information vs. the information itself.

Unsurprisingly, Azure AD follows the WSAD data model with suitable changes for cloud use. The core data model is as follows:

* The core directory service is divided into *directory contexts*, one or multiple per tenant plus a system context. Each directory context has an immutable, globally unique, non-reusable GUID-valued identifier – a *context ID* – and contains a set of entities (or objects) and association (or links) between the entities. Each object or link belongs to exactly one context.
* Each object has an object class or type (*ObjectType*): *TenantDetail*, *User*, *Contact*, *Group*, *Device*, *Application*, *ServicePrincipal*, etc. and an immutable, globally unique, non-reusable GUID-valued identifier, i.e. an *object ID (ObjectId)*.
* An object contains a set of *properties*: *DisplayName*, *UserPrincipalName*, *JobTitle*, *Department*, *TelephoneNumber*, etc. Each property has a name and, if set, contains a value or a set of values. The object class determines which properties may appear on the object, and the property determines the type (string, binary, integer, structure, etc.) and multiplicity of the values.
* An object may contain a set of *navigation* *properties* that each corresponds to a *link* (or association). A link is a directional, typed relationship from one object to another object, all in the same context. The type of the link is its *link class*: *Manager*, *DirectReports*, *MemberOf*, *Members*, etc. Links significantly contribute to establish an enterprise social graph as discussed in the [John Shewchuk blog post](http://blogs.msdn.com/b/windowsazure/archive/2012/06/20/reimagining-active-directory-for-the-social-enterprise-part-2.aspx)[[41]](#footnote-41). Links maintain referential integrity: deleting the source or target object of the relationship implicitly deletes the link.
* Object (respectively link) instances may be group into set of

Note For additional information, see the Microsoft MSDN article [Entity Reference](http://msdn.microsoft.com/en-us/library/azure/dn151470.aspx)[[42]](#footnote-42).

The Azure AD directory schema defines the properties, object classes, and link classes; much of it is a subset of standard LDAP v3 (and WSAD) schemas.

It however differs from that of LDAP directories in the following ways:

* Unlike entries in an LDAP directory, objects do not have distinguished names and are not arranged into a distinguished multi-level hierarchy. Objects can be interpreted as having various hierarchical relationships based on links and property values.
* The directory does not support object class inheritance. In WSAD, such a capability was used in very limited ways but added significant complexity to the system.

The Azure AD directory schema is defined per specific version. It may evolve as it was the case for the WSAD directory schema over the time since its first introduction in the early 2000.

Generally speaking, applications that consume directory information – and that are thus instantiated as an *Application* object in the directory - tend to fall into the following three classes with respect to directory extensibility requirements:

Note For more information on *Application* object, see the [Leverage Azure AD for modern business applications](http://www.microsoft.com/en-gb/download/details.aspx?id=36391)[[43]](#footnote-43) white paper.

1. A first class of application that corresponds to the vast majority doesn’t need to extend the directory and has no extensibility requirements to address.
2. A second class of applications has very simple extensibility needs where they need to publish some information about a directory entity, such as a user, to other applications. As of today, a built-in extensibility mechanism addresses this kind of extensibility requirements in the specific and historical context of Microsoft services such as Office 365.
3. The final class of applications is the one without any surprise that has additional or extensive extensibility needs. They may maintain significant information about users and other objects, and also may have complex query needs based on properties and links. These queries may be in the mainline high volume path of the application.

The use of an application-specific local store for extensibility could be an option in this case. With the advent of the cloud, storage capabilities are widely available through services such as Azure storage and Azure SQL database. An application that falls into this model may usually maintain its own tables in a storage service. A typical model might be that rows in the table represent Azure AD directory entities about which the application maintains its information. One of the columns of the table would be a key that identifies the entity in the directory (i.e. the join key). The other columns represent application-specific information. The application can make use of the differential query capability supported by the directory to manage the lifecycle of the rows in its tables utilizing the “join key”.

This said, Azure AD provides custom schema extensibility capability (currently in public preview) in Azure AD Graph API that allow augmenting existing entity with additional custom attributes without requiring an external data store. A common example may consist in storing a payroll number for the user.

Note Azure AD Graph API is a RESTful API that provides a directory programming surface for querying and updating the directory, and thus to sustain the identities lifecycle management as whole. For more information, see the Microsoft MSDN article [Azure AD Graph API](http://msdn.microsoft.com/library/azure/hh974476.aspx)[[44]](#footnote-44).

As of this writing, the aforementioned *User*, *Group*, *TenantDetail*, *Device*, *Application* and *ServicePrincipal* entities can be extended with “String” type or “Binary” type single-valued attributes. Azure AD Graph API provides for that purposes REST interfaces for an application to register, unregister, enumerate, read, write, and filter by extension properties. Extension properties are registered on the *Application* object that corresponds to the application within the directory. The application must be granted write access to register an extension property. 100 extension properties (across ALL types and ALL applications) can be written to any single object.

Multi-tenant applications that register extension properties in the directory are referenced from all the tenants consenting to that application. Once a customer tenant has consented to an application (even for read) the extension properties registered on that application are available in the consenting tenant for reading/writing by any application that has the appropriate access.

Note For more information, see the blog post [Extend Azure Active Directory Schema using Graph API (preview)](http://blogs.msdn.com/b/aadgraphteam/archive/2014/03/06/extend-azure-active-directory-schema-using-graph-api-preview.aspx)[[45]](#footnote-45) and the Microsoft MSDN article [Azure AD Graph API Directory Schema Extensions](http://msdn.microsoft.com/en-us/library/azure/dn720459.aspx)[[46]](#footnote-46).

#### Directories

As most people know, the forest in WSAD represents the administrative and security boundary. Likewise, each directory in Azure AD is as a fully independent resource.

In other words, each directory is a peer, fully-featured, and logically independent of other directories that you manage. There is no parent-child relationship between directories.

This independence between directories includes:

* **Resource independence**. If you create or delete a resource in one directory, it has no impact on any resource in another directory, with the partial exception of external users. Furthermore, if you use a custom verified domain “fabrikam.com” with one directory, it cannot be used with any other directory.
* **Administrative independence**. If, for example, you add or remove an administrator role from one directory, this has no impact on any administration privileges in any other directory.
* **Synchronization independence**. You can configure each directory independently to extend your on-premises identity infrastructure with this directory and get data synchronized.

As a forest contains one or multiple domains, a directory contains one or multiple domains. (See later in this document). For that purpose, as you can declare enterprise administrator(s) for the forest, there are similarly directory wide administrators.

#### Administrative units

Administrative units (AUs) in Azure AD are like OUs in WSAD modernized for the cloud. They let you sub-divide your Azure AD directory, enabling the separation of administrative duties and policy creation across a large organization. They represent a new Azure AD container of resources that can be used for delegating administrative permissions over subsets of users and applying policies to a subset of users.

Administrative units (currently in public preview as of this writing) are a feature of the Azure AD Premium edition. For the moment, you can create and manage them through dedicated Windows PowerShell cmdlets (see next section).

Note For more information, see the blog post [Wrapping up the year with a boat load of Azure AD news!](http://blogs.technet.com/b/ad/archive/2014/12/11/wrapping-up-the-year-with-a-boat-load-of-azure-ad-news.aspx)[[47]](#footnote-47) and the Microsoft MSDN article [Administrative units management in Azure AD - Public Preview](https://msdn.microsoft.com/en-us/library/azure/dn832057.aspx)[[48]](#footnote-48).

#### Management surface

Azure AD allows administrators to manage information in it through:

* The use of the graphical user interface thanks to the Azure management portal or other portals.
* A set of Windows PowerShell cmdlets, that allows for scripting frequent operations: the Azure Active Directory Module for Windows PowerShell.

Note For more information, see the Microsoft MSDN article [Manage Azure AD using Windows PowerShell](http://msdn.microsoft.com/en-us/library/jj151815.aspx)[[49]](#footnote-49).

* On-premises management tools used to manage information in an on-premises directory and then synchronized into Azure AD with the directory synchronization. (More on this later in this document.)

### Security Token Services (STS)

As previously mentioned, Azure AD provides support for (federated) authentication, single sign-on, and authorization.

There are flavors of this support for browsers and for rich clients, and for identities hosted in the cloud (cloud identities) as well as federated identity providers (federated identities). These capabilities are provided by the Security Token Service (STS) in Azure AD. The STS in Azure AD is a multi-tenant STS.

#### Core security model

The core security model consists of tenant’s realms. There is a 1:1 mapping between a STS tenant realm and a directory tenant. The notion of a realm is a well-known concept in security; and the tenant realm in the STS is the equivalent of a Kerberos realm or a WSAD domain.

Tenant realms have a single, immutable, globally unique and rename safe security identifier and one or more names verified DNS names that act as friendly aliases.

Tenant realms contain principals, representing users, services, etc. A principal is an object of the corresponding type in the directory.

Principals have one or more names (such as user principal name for a user, or multiple service principal names for an application) and a security identifier, that is globally unique, immutable, and not re-usable.

**Principals can have one or more credentials (such as password, certificate, and keys) that can be used to authenticate the principal. Alternatively, the principal can be authenticated by an identifier from an external identity provider (such as an immutable ID from a security token issued by the organization on-premises identity provider).** A principal that has this kind of mapping setup is also known as a federated principal, because the principal conceptually represents a user from a federated system (such as a corporate user from the on-premises identity infrastructure).

Principals can both request and accept security tokens, typically from the tenant realm in which they reside. Tenant realms are supported by the STS that authenticates requestors and makes authoritative statements about those requestors, usually in the context of the target for the request.

These authoritative statements are packaged in security tokens and are signed by the STS. Security tokens consist of a collection of claims, which are statements made about users, for example name, id, email, group, role, etc. used for authentication and authorization decision purposes. Security tokens typically follow a secure, standardized method of packaging claims for transport.

Note For more information, see the Microsoft MSDN article [Supported Token and Claim Types](https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/)[[50]](#footnote-50).

Tenant realms can setup federation with other realms, i.e. to an existing on-premises identity infrastructure such as a corporate Active Directory environment.

### Supported (modern) protocols

Usual on-premises authentication mechanisms such as Kerberos and NTLM no longer apply in a general manner in the cloud space since cloud applications do not have most of the time connectivity to a Windows Server Active Directory (WSAD) domain controller (DC) and/or the VMs underneath aren’t domain-joined at all.

Azure Virtual Machines and Azure Virtual Network certainly provide such capabilities with the ability to instantiate a standalone DC in the cloud or to leverage secure site-to-site connectivity back to the on-premises infrastructure.

However, this should be seen more specifically rather as IaaS “migration” paths than the general situation for the workloads in the cloud. It’s all the more so with the mobility and the “Bring-Your-Own-Device” (BYOD) trend where users will also often be themselves considered outside of the organization infrastructure perimeter. Furthermore, cloud solutions can by nature encompass multiple security realms.

Consequently, Internet identity federation protocols constitute a much more scalable and efficient way to implement authentication in such context. Moreover, Internet identity federation protocols can also relevantly respond to other concerns like single sign-on between cloud applications that reside in the same of different clouds as well as claims issuance with the processing and transforming capability of security tokens in terms of type of trust, token format, semantics and (values of) claims for “impedance adaptation”.

Azure AD opts to such protocols for integrating applications and furthermore systematically aims at being open standards based wherever possible.

Note For more information, see the Microsoft MSDN article [Azure Active Directory Authentication Protocols](http://msdn.microsoft.com/library/azure/dn151124.aspx)[[51]](#footnote-51).

Currently, this translates by the support for the following OASIS standards widely established and adopted:

* [WS-Federation (WS-Fed)](http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf)[[52]](#footnote-52),
* [WS-Trust](http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf)[[53]](#footnote-53),
* [Security Assertion Markup Language (SAML) 2.0](http://go.microsoft.com/fwlink/?LinkId=193996)[[54]](#footnote-54).

All the above protocols use SAML security tokens.

Note For more information, see the Microsoft MSDN article [Supported Token and Claim Types](https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/)[[55]](#footnote-55).

WS-Federation and WS-Trust protocols supports respectively Web (browser) based clients and rich smart clients.

SAML 2.0, as a token format and a protocol, is very popular in the public sector with government agencies as well as with enterprises and educational institutions. SAML 2.0 is a suite of specifications and, as such, comprises a set of normative and non-normative documents. As part of them, the normative document [Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)[[56]](#footnote-56) defines the use cases or the “*How-to*” in regards to the use of SAML to solve specific problems of the extended enterprise, and as an important number of profiles.

As of today, Azure AD more specifically supports (for the modern applications) the SAML 2.0 web browser single sign-in profile, the SAML 2.0 web browser single sign-out profile, as well as and the Enhanced Client or Proxy (ECP) profile.

Note The SAML 2.0 ECP profile is an adaptation of the SAML 2.0 browser single sign-in profile with the parts that were designed around the limitations of a browser removed. In other words, in the SAML 2.0 ECP profile, the user agent is assumed to be something more than a browser (or perhaps a browser with a plugin for example).

Note These profiles supports various possible deployment models. The ones implemented here are the HTTP-Redirect and HTTP-POST bindings specified in the document [Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)[[57]](#footnote-57). For more information, see the Microsoft MSDN article [SAML Protocol Reference](https://msdn.microsoft.com/en-us/library/azure/dn195591.aspx)[[58]](#footnote-58).

**As previously outlined, modern applications live in an environment that includes a broad spectrum of mobile and native clients, server to server communication, and web APIs as a result of the API economy, in addition to traditional browser and web site interactions. And thus, even WS-Federation or SAML 2.0 aren’t enough to address the scenarios introduced by modern business applications.**

To address these new requirements, Azure AD unsurprisingly also provides support for the [OAuth 2.0](http://tools.ietf.org/html/draft-ietf-oauth-v2)[[59]](#footnote-59) [[60]](#footnote-60) protocol, which is gaining popularity in the Internet as an authorization protocol for accessing information. This is the primarily protocol for authorization and delegated authentication.

Using OAuth 2.0, an application can gain access (with consent from the resource owner – which could be the end user or the administrator user) to impersonate the user, or users in his organization to access the resource.

Note For more information, see the Microsoft MSDN article [OAuth 2.0 in Azure AD](https://msdn.microsoft.com/en-us/library/azure/dn645545.aspx)[[61]](#footnote-61).

The OAuth 2.0 protocol uses JSON Web Token (JWT). JWT is a compact token format[[62]](#footnote-62) especially apt for REST-based development. JWT use is growing, and products supporting the format are increasingly common in the industry.

Note For more information, see the Microsoft MSDN article [Supported Token and Claim Types](https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/)[[63]](#footnote-63).

Along with OAuth 2.0, Azure AD provides a model for representing applications as service principals in the directory (see later in this document section). An application can then make use of its own identity, i.e. the “*app identity*”, or instead the user’s identity, i.e. the “*app + user identity*” (or delegated identity).

Finally Azure AD provides the support for the [OpenID Connect](http://openid.net/specs/openid-connect-core-1_0.html)[[64]](#footnote-64) protocol. OpenID Connect defines an identity layer on top of OAuth 2.0 and represents the state of the art in modern authentication protocols. It’s a suite of lightweight specifications that provide a framework for identity interactions via REST like APIs. It is based on OAuth 2.0, and JWT is also one of the basic components of it.

Note For more information, see the Microsoft MSDN article [OpenID Connect 1.0](https://msdn.microsoft.com/en-us/library/azure/dn645541.aspx)[[65]](#footnote-65).

**Microsoft has been deeply involved in the standards work for both OAuth 2.0 and OpenID Connect. Microsoft takes the participation in the standards community seriously and have worked hard to ensure interoperability** **with other implementations.**

Note The OpenID Foundation has recently launched a certification program for OpenID Connect implementations. For more information, see the article [The OpenID Foundation Launches OpenID Connect Certification Program](http://openid.net/2015/04/17/openid-connect-certification-program/)[[66]](#footnote-66). Azure AD has successfully passed the certification and is [certified](http://openid.net/certification/)[[67]](#footnote-67) as an OpenID Connect identity provider.

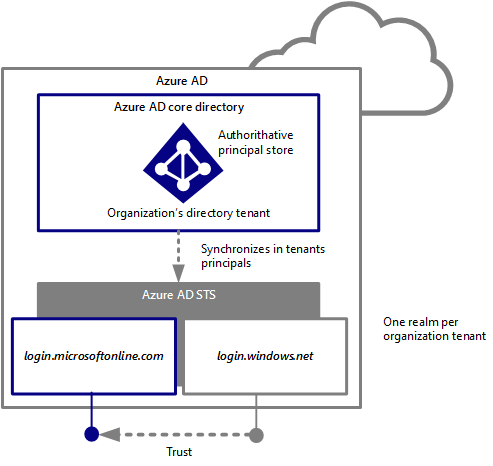
Having an OpenID Connect certification program provides confidence that certified implementations will "just work" together. This represents another important step on the road to widely-available secure interoperable digital identity for all the devices and applications that people use. Microsoft is proud to be a key contributor to the development of OpenID Connect and now of its certification program.

### A closer look at the structure of the Azure AD STS

As previously introduced, Azure AD supports several of the most widely used authentication and authorization protocols via a STS.

**In a recent past, this STS was implemented by a combination of two STS**:

1. The *login.microsoftonline.com* sign in service.
2. And login.windows.net, which was the de-facto facade for modern business applications.



In this past service configuration, the *login.microsoftonline.com* sign-in service was (and still is today) in charge of handling the user authentication step, i.e. username/password - with an optional second-form of authentication (e.g. a mobile phone app, an automated phone call, or text message challenge) through the native support of [Azure Multi-Factor Authentication](http://azure.microsoft.com/en-us/services/multi-factor-authentication/)[[68]](#footnote-68) in Azure AD -, and login.windows.net the policy and claims generation steps for modern application. Application authentication was thus handled directly by login.windows.net. login.windows.net acted as a federation provider, which trusted a single authority: the *login.microsoftonline.com* sign-in service.

**As of today, all authentication requests can now be served directly by the *login.microsoftonline.com* STS end-to-end.**

While being most of the time completely to an existing application - if the app makes certain assumptions about our underlying implementation it may require changes – this evolution provides several benefits:

* Users enjoy a faster sign-in experience free of extra hops.
* The sign-in user experience includes several new features, for example the ability to maintain multiple actively signed-in users, and a more responsive UI that behaves appropriately across more devices and screens.
* From an engineering perspective, this also leads to an even more reliable service thanks to a number of features this allows in the underlying implementation of the STS.

Important note Applications that send requests to *login.windows.net* continue to be supported. The redirect to *login.microsoftonline.com* occurs earlier in the authentication flow than before, and maintains protocol consistency. This said, we do recommend to reflect the evolution in such applications as soon as possible, thus allowing users to get an improved sign in experience, and authentication flows to be free of extra complexity.

Note For more information, see the blog post [Simplifying our Azure AD Authentication Flows](http://blogs.technet.com/b/ad/archive/2015/03/06/simplifying-our-azure-ad-authentication-flows.aspx)[[69]](#footnote-69).

*login.microsoftonline.com* is authoritative for organizations and security principals. Group membership information can be included in security tokens reducing friction when an application/service is performing authorization.

## Creating multiple directories in Azure AD

As an IdMaaS service, Azure AD enables you to create multiple directories that you can use for testing or other non-production usage, or for managing data synced from various on-premises identity directories, etc. The classic Azure management portal enables you to add directories and manage existing ones. You can then manage all your directories from the portal.

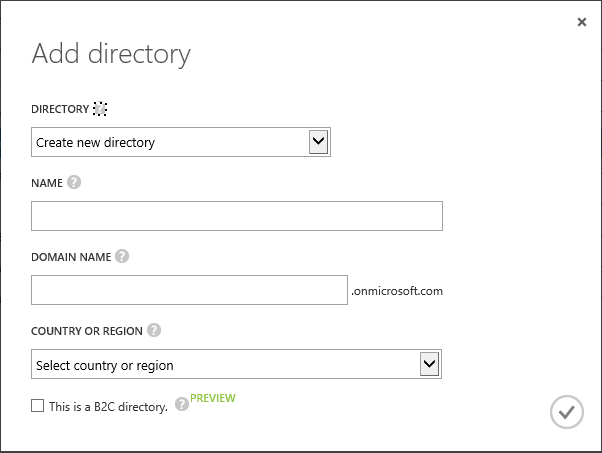
These directories are fully independent resources. In other words, as noticed before, each directory is a peer, fully-featured, and logically independent of other directories that you manage. There is no parent-child relationship between directories.

Note For more information, see the blog post [Creating and Managing Multiple Azure Active Directories](http://blogs.technet.com/b/ad/archive/2013/11/08/creating-and-managing-multiple-windows-azure-active-directories.aspx)[[70]](#footnote-70).

### Adding a new directory

To add a directory, proceed with the following steps:

1. Open a browsing session and navigate to the classic Azure management portal at <https://manage.windowsazure.com>.
2. Sign in to the Azure management portal with the credentials of your Microsoft account.
3. In the management portal, click **NEW** in the tray of the bottom, and then select **APP SERVICES**, **ACTIVE DIRECTORY**, **DIRECTORY**, and then **CUSTOM CREATE**. An **Add Directory** dialog pops up.



1. In the **Add directory** dialog, configure the basic properties for your new directory, i.e. its name, default domain name, and the country or region as follows:
   1. In **Name**, choose a name for the directory that will help distinguish it from your other directories in your Azure subscription, for example “*Fabrikam Corporation*”.

Note If the directory you're creating is to be used in production, choose a name for the directory which your users will recognize as the name of your organization. You can change the name later if you want.

* 1. In **Domain name**, choose a default domain name which you can use to bootstrap usage of this directory, for example “*corpfabrikam.onmicrosoft.com*”.

Note While the default domain cannot be changed, later you can add a custom verified domain owned by your organization (e.g., “fabrikam.com”) to enable better user experiences for sign on to that directory, or for synchronizing with the on-premises identity infrastructure.

* 1. In **Country or region**, choose a country or region for your directory. This setting is used by Azure AD to determine the datacenter region(s) for your directory. It cannot be changed later.
  2. Leave uncheck **This is a B2C directory**.

1. Then, click the check mark icon in the lower right of the dialog, and in a few seconds you'll see that your new directory has been created and is available for use.

Your user account is included in that new directory, and you're assigned to the global administrator role. This enables you to manage the directory you created without signing in as a different user of that directory. As an administrator of a directory, you can also add users from another directory of which you're a member. This is useful, for example, where there are users in your production directory who will need to collaborate on an application that is under development or testing in a non-production environment. A user can be a member of up to 20 directories.

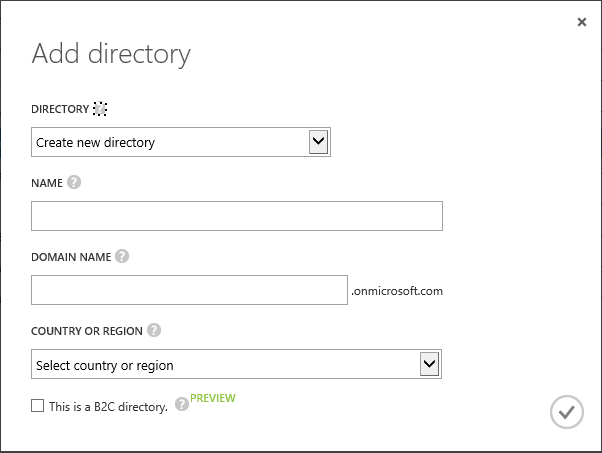
Note For additional information, see the MSDN article [Azure AD service limits and restrictions](http://msdn.microsoft.com/en-us/library/azure/dn764971.aspx)[[71]](#footnote-71).

### Using an existing directory

If you access the Azure management portal with a Microsoft account, you can configure your Microsoft account to manage an existing Azure AD that's used for Office 365 or another service, even if your Microsoft account already manages an Azure AD directory tenant.

To configure a Microsoft account to manage an existing directory, proceed with the following steps:

1. Open a browsing session, navigate to the classic Azure management portal, and sign in with the credentials of your Microsoft account.
2. In the management portal, click **NEW** in the tray of the bottom, and then select **APP SERVICES**, **ACTIVE DIRECTORY**, **DIRECTORY**, and then **CUSTOM CREATE**. An **Add Directory** dialog pops up.



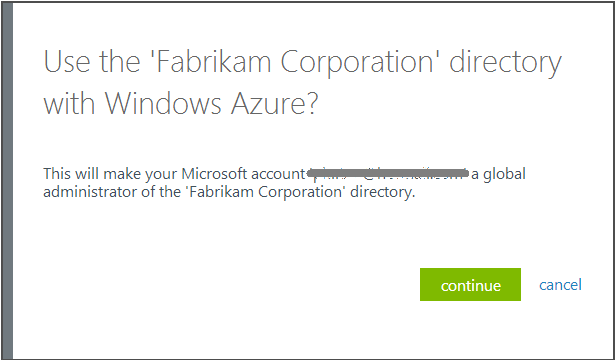
1. In the **Add Directory** dialog, change the **DIRECTORY** dropdown from the default **Create new directory** to **Use existing directory**.
2. Click **I am ready to be signed out now**.



1. Click the check mark icon in the lower right of the dialog to continue.
2. Upon signing out, you'll see the sign in screen for Azure AD. Enter your user name and password for the global administrator account in the Azure AD directory tenant that you want to manage using your Microsoft account.

Note You can authenticate either with a Microsoft account or an organizational account.

1. Once signed in, you'll see the dialog hereafter.



Click **continue** to add your Microsoft account as a global administrator of the existing directory.

1. Once that's completed, click the link to sign out of your organizational account. Then, you can sign in to the Azure management portal as your Microsoft account user, and can manage the directory to which you added the Microsoft account.

You can manage this directory tenant like other directories for which you’re a global administrator.

## Deleting a specific directory in Azure AD

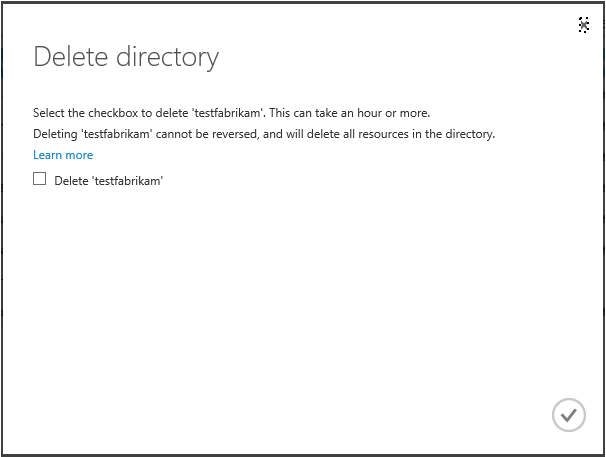
Any directory that is no longer used can be deleted with the assurance that you won’t accidentally delete a directory that controls access to important resources or is relied on by subscriptions.

To delete an existing directory, proceed with the following steps:

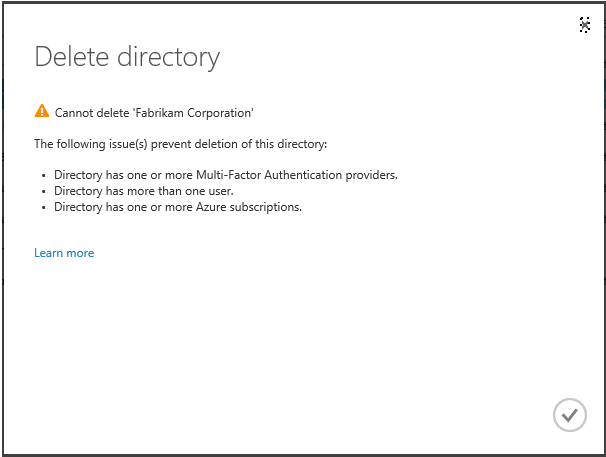
1. Open a browsing session, navigate to the Azure management portal, and sign in with the credentials of your Microsoft account.

Note You can authenticate either with a Microsoft account or an organizational account. However, you have to be a global administrator of the directory you want to delete. Also, if you sign in with an organizational account, you cannot delete the home directory of your user account. For example, if you sign in as [johndoe@corpfabrikam.onmicrosoft.com](mailto:johndoe@corpfabrikam.onmicrosoft.com), you cannot delete the directory with the initial domain *corpfabrikam.onmicrosoft.com*.

1. In the management portal, click **ACTIVE DIRECTORY**, select the directory to delete, and then click **DELETE** in the tray of the bottom. A **Delete directory** dialog pops up.



Note To protect and prevent you from accidentally deleting an important directory, Azure AD requires that there is only one user in the directory, no applications in the directory, no subscriptions to Azure, Office 365, or other Microsoft Online services for organizations that rely on this directory, etc.



For additional information, see the MSDN article [What is an Azure AD directory?](http://msdn.microsoft.com/library/azure/jj573650.aspx#BKMK_DeleteDirectory)[[72]](#footnote-72).

1. Check the checkbox to confirm that you want to delete that directory, and then click the check mark icon in the lower right of the dialog.

# Managing directory configuration

**Azure AD enables a customer to start using its IdMaaS features with no on-premises footprint.** Accordingly, Azure AD provides for hosted (cloud) identities where customers can create users, groups and other principals for their organization. The **cloud identities** are directly mastered in an Azure AD directory tenant.

With cloud identities, users receive, for signing into Azure AD and any cloud-based application that is integrated into Azure AD, cloud credentials (that are separate from other desktop or corporate on-premises credentials if any).

This outlined, many enterprise customers will want to extend their on-premises identity infrastructure to seamlessly synchronize existing on-premises identities to the cloud and thus establish a hybrid corporate identity platform. Such an approach (also supported by Azure AD) is more sophisticated.

## Extending your on-premises identity infrastructure with Azure

If your organization uses an on-premises identity infrastructure (based on AD or on other (LDAP-based) directories), Azure AD enables you to extend it to simplify your cloud-based administrative tasks and even provide your users with a more streamlined sign-in experience.

Azure AD supports the following three directory integration scenarios:

1. **Directory synchronization**. This scenario enables to synchronize on-premises directory objects (users, groups, contacts, etc.) to the cloud to help reduce administrative overhead. Once directory synchronization has been set up, administrators can manage directory objects from the organization on-premises identity infrastructure and those changes will be synchronized to the related directory tenant.
2. **Directory synchronization with password synchronization.** This scenario is used when you want to enable your users to sign in to Azure AD and other cloud-based applications using the same user name and password as they use to log onto your corporate on-premises network. This scenario is available for an on-premises Active Directory mono-forest or multi-forest environment.

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 additional information on the password (hash of hash) synchronization capability, see the following Microsoft TechNet articles [Implement Password Synchronization](http://technet.microsoft.com/en-us/library/dn246918.aspx)[[73]](#footnote-73) and [DirSync: Password Sync Frequently Asked Questions](http://social.technet.microsoft.com/wiki/contents/articles/18096.dirsync-password-sync-frequently-asked-questions.aspx)[[74]](#footnote-74).

**Such a capability provides a “same sign-on” experience**, where users sign in to their corporate machine and Azure AD/Office 365 with the same credentials.

With the password sync capability, this integration scenario 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 that expect a seamless sign-in experience**.

1. **Directory synchronization with single sign-on. This scenario enables** to provide users with the most seamless authentication experience as they access Microsoft cloud services and/or other cloud-based SaaS applications while logged on to the corporate network.

The user’s identity is mastered on-premises in the identity infrastructure and synchronized to the Azure AD in the form of a **federated identity**.

In order to set up single sign-on, organizations need to deploy on-premises Active Directory Federation Services (AD FS) or other supported third-party security token services (STS) to federate between the on-premises and cloud directories. Once a supported STS has been set up, users can use their on-premises corporate credentials (user name and password, and/or any additional authentication factor) to access the services in the cloud and their existing on-premises resources.

Note For more information, see the guide [Azure Active Directory Hybrid Identity Design Considerations](https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-overview/)[[75]](#footnote-75).

Through directory synchronization, organizations can keep their existing on-premises identity infrastructure synchronized with their Azure AD directory tenant. As covered later in this document, secure tooling is provided for synchronization to automatically propagate on-premises initiated user adds, deletes, and changes to Azure AD directory tenant(s), streamlining the process of provisioning and managing identities and securing access to resources on-premises, in the cloud, or both, as well as write-back capabilities to handle hybrid integration scenarios.

Directory synchronization along with the related options - depending on the on-premises identity infrastructure - are further discussed later in this document for organizations that want to streamline the provisioning and the synchronization of identities.

Considering the above, Azure AD enables a seamless sign-in experience for identities that rely on password (hash of hash) synchronization (“same” sign-on) or a supported STS to federate between the on-premises and cloud directories (single sign-on).

For modern applications and SaaS subscriptions, you can deliver a seamless sign-in experience as well to eliminate the need for multiple usernames and passwords. Users can then sign into Azure AD, Microsoft cloud services or any other cloud-based application that is integrated into Azure AD using their own corporate on-premises credentials.

Users can gain access to Azure AD or any other application that is integrated into Azure AD by authenticating to their Azure AD user accounts, either through a prompt to provide valid credentials or through a federated single sign-on process. Once authenticated, user’s identities refer to the user names associated with the Azure AD accounts.

The above type of identity (cloud vs. federated) affects the user experience, administrative requirements, deployment considerations, and capabilities using Azure AD.

The following is the simplified breakdown of the experience:

* **User experience with cloud identities**. Users sign in with their cloud identity. Cloud identities are authenticated using traditional challenge/response, where users type in their user name and password. Authentication happens in the cloud. Users are always prompted for credentials although they can choose to authorize the application to memorize their password.

As mentioned above, users may have two identities, i.e. a cloud identity for Azure AD and other cloud-based applications, and potentially one for accessing on-premises applications. Consequently, in absence of password (hash of hash) synchronization, users are prompted for credentials even when logged into their on-premises infrastructure (AD or non-AD sources) when accessing Azure AD and other cloud-based applications.

As previously outlined, with password (hash of hash) synchronization, which is only available for on-premises AD mono or multi-forest environment, users can sign in to Azure AD and other cloud-based applications using the same user name and password as they use to log onto their corporate network for accessing on-premises applications.

Finally, integration with cloud-based multi-factor authentication solution can be enabled for users with the native support of the easy-to-use Azure Multi-Factor Authentication solution. (See later in this document.)

* **User experience with federated identities**. Users sign in with corporate on-premises identity for access to both cloud-based and on-premises applications. In other words, they are authenticated transparently using the on-premises identity infrastructure when accessing Azure AD itself and other cloud-based applications. Authentication happens on-premises against the organization’s identity provider servers and users get true single sign-on. Furthermore, integration with on-premises multi-factor authentication solutions can be enabled.

Important note On-premises multi-factor authentication solutions support is not available for clients other than web browsers or clients that uses passive federation, with the exception for Office 365 ProPlus/Office 2013 clients with the modern authentication (a.k.a. Active Directory Application Library (ADAL) based authentication stack) enabled. Modern authentication is available to any customer running the March 2015 or later update for Office 2013 but is disabled by default. For more information, see the blog post [Office 2013 modern authentication public preview announced](http://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/)[[76]](#footnote-76).

Other clients that do not have the capability to prompt users for strong authentication credentials can therefore not be supported. Strong authentication must only be applied to the passive federation endpoints on on-premises identity provider servers; as other clients will otherwise not be able to connect.

* **Administrator experience with cloud identities**. Organization’s administrators manage the password policy both in the cloud and on-premises. The cloud identities password policy is stored in the cloud with Azure AD. Password reset has to be managed for on-premises and cloud identities and, hence, the users have to change the password as per the policy for both. The premium edition of Azure AD provides a password write-back capability with self-service password reset.

Finally, integration with cloud-based multi-factor authentication solution can be enabled for administrators with the native support of the easy-to-use Azure Multi-Factor Authentication (MFA) solution.

* **Administrator experience with federated identities**. Organization’s administrators manage the password policy on-premises only and hence do 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 premise IDs only. Eventually, several on-premises multi-factor authentication solution integration options are offered.

The above scenarios **directory synchronization with password synchronization** is different from the **directory synchronization with single sign-on** in that it does not require the customer to deploy and maintain supported STS servers on-premises.

**Password (hash of hash) synchronization** is fully integrated with the tooling tool later discussed. This better keeps the deployment simple and removes the costs associated to the deployment and maintenance of fault-tolerant STS components.

As illustrated in terms of experience, the scenario **Directory synchronization with single sign-on** allows your users to seamlessly access their resources in the cloud without being prompted for their passwords multiple times (at least once when logging into their on-premises network, once when accessing cloud resources). When using password hash synchronization, users will still have to enter their password, although this password may be locally saved on the client.

Customers who select Azure AD as an IdMaaS for their applications and SaaS subscriptions typically want to reduce the complexity of their infrastructure and to minimize their operational costs. The directory synchronization scenario (if any) solution should be aligned to these goals and ideally require no or little on-premises hardware investments and no or little deployment effort.

Considering the above discussion, recommendations for each scenario, as well as a features and benefits matrix, are provided below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirements** | **Cloud identities without directory sync** | **Directory sync (w/ password** | **Directory sync and single-sign on** |
| Identity Model | Cloud identities | Cloud identities | Federated identities |
| Reduce hardware footprint and shorten deployment times | +++  No on-premises infrastructure required | +  Single on-premises server (or VMs) required | --  Multiple on-premises servers (or VMs) required (1) |
| Users must still be able to access their resources (modern applications and SaaS subscriptions), if the on-premises corporate network is unavailable | Yes | Yes | No (2) |
| Single on-premises AD forest – Users can use the same set of credentials across premises | No | Yes | Yes |
| Multiple on-premises AD forests – Users can use the same set of credentials across premises | No | Yes | Yes |
| On-premises non-AD directories – Users can use the same set of credentials across premises | No | No. Password hash synchronization is not available in this scenario. | Yes |
| User logon protection with Azure Multi-Factor Authentication | Yes (3) | Yes (3) | Yes (3) |
| User logon protection with customer (virtual) smartcard or other multi-factor authentication solution or | No | No | Yes (3) (4) (5) |
| User logon from outside the corporate network must be prevented | No | No | Yes (4) |
| Users are subject to logon policies such as logon time restrictions | No | No | Yes (4) |
| Organization requires access to logon attempts (security logs), for auditing purposes | Yes (6) | Yes (6) | Yes (4) |
| Account lockouts in the on-premises directory must immediately prevent new sign-in to for Azure AD and the resources that rely on it | No | No (7) | Yes (8) |

(1) Deployment in a hybrid model with some roles hosted on virtual machines in Azure is supported. For additional information, see the following Microsoft TechNet and MSDN articles [Deploy AD DS or AD FS and Office 365 with single sign-on and Azure Virtual Machines](http://technet.microsoft.com/en-us/library/dn509513.aspx)[[77]](#footnote-77) and [Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines](http://msdn.microsoft.com/library/azure/jj156090.aspx)[[78]](#footnote-78).

(2) Dependency on on-premises (or Azure-based) infrastructure availability.

(3) For Office 365 users, this requires the [modern authentication](http://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/)[[79]](#footnote-79) (a.k.a. [Active Directory Authentication Library (ADAL)](http://msdn.microsoft.com/en-us/library/azure/dn151135.aspx)[[80]](#footnote-80) based authentication stack) for Office 365 ProPlus/Office 2013 applications. Modern authentication is available to any customer running the March 2015 or later update for Office 2013 but is disabled by default. The Office 2013 March 2015 update is fully production ready and supported. Once enabled, app passwords are then no longer needed.

(4) Dependency on the on-premises STS capabilities.

(5) VPN workaround can be implemented for other rich-clients.

(6) As per Applications Access Enhancements for Azure AD/Azure AD Basic or Premium capabilities that provide pre-defined security reports associated with the signons by the organization’s users.

(7) Disabled account status is replicated every 3 hours.

(8) Open sessions will not be terminated immediately. The access denial will only occur when the token will expire and when the application will try to get another token issued.

Important note The above table highlights many requirements that imply single sign-on to be fulfilled. In reality, today those requirements are actually required only by a small fraction of Azure AD/Microsoft services customers.

Note For more information on the benefits and features provided with each of these scenarios, see Microsoft TechNet article [Determine which directory integration scenario to use](http://technet.microsoft.com/en-us/library/jj573649.aspx)[[81]](#footnote-81).

The Azure management portal along with the other Microsoft services portals such as the Office 365 account portal help tenant administrators managing their organizations' identity and subscription data using a single instance of Azure AD. Let’s see how it works.

Note For more information, see Microsoft TechNet article [Administering your Azure AD tenant](http://technet.microsoft.com/en-us/library/hh967611.aspx)[[82]](#footnote-82).

## Managing the Internet domains for your directory

After signing up for Azure AD (or for a Microsoft service such as Office 365, Dynamics CRM Online, and others), the only domain associated with your subscription account and created with the directory tenant is the <*organization name*>.onmicrosoft.com domain chosen during registration, for example *corpfabrikam.onmicrosoft.com*.

This is the default domain. When you create a new user, the user’s sign-in name and email address are assigned to this default domain.

You can off course add one or more customs Internet domains to a directory rather than retaining the *onmicrosoft.com* domain, and then assign users to sign in with any of the validated domains.

You can register multiple Internet domain names for a directory, for example *fabrikam.com*, in addition to the initial default domain, for example *corpfabrikam.onmicrosoft.com*. A directory allows you to register an Internet domain only after you proves that your organization owns the DNS namespace in the public Internet DNS. As of this writing, you can host up to 600 registered Internet domains in your directory, each represented by a different DNS namespace.

A domain can then be either a cloud (standard) domain or a federated (single sign-on) domain, meaning that all users on a domain MUST use the same identity system: either cloud identity or federated identity as previously covered.

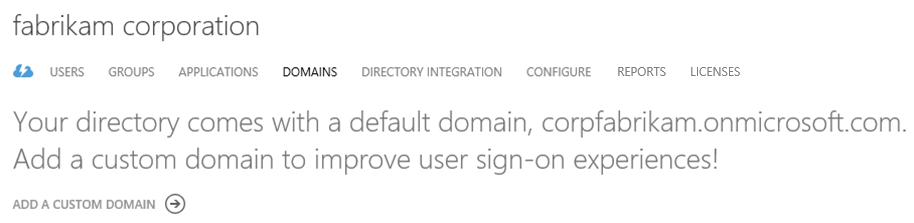
For example, you could have one group of users that only needs a cloud identity because they don’t have an on-premises account and/or access on-premises systems, and another group of users who have an on-premises account and/or use cloud applications and on-premises systems. You would use add two domains to the directory tenant, such as *contractors.fabrikam.com* and *ftes.fabrikam.com*, and only set up the federation for one of them.

A domain can be converted from cloud to federated to sustain federated identities in lieu of cloud identities, or from federated to cloud.

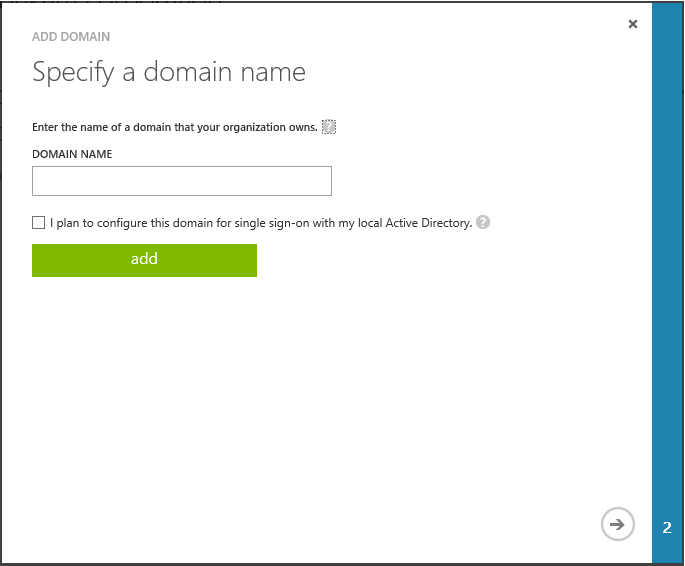
Note For more information, see the Microsoft TechNet articles [Add your domain](http://technet.microsoft.com/en-us/library/hh969247.aspx)[[83]](#footnote-83).

To register an Internet domain, proceed with the following steps:

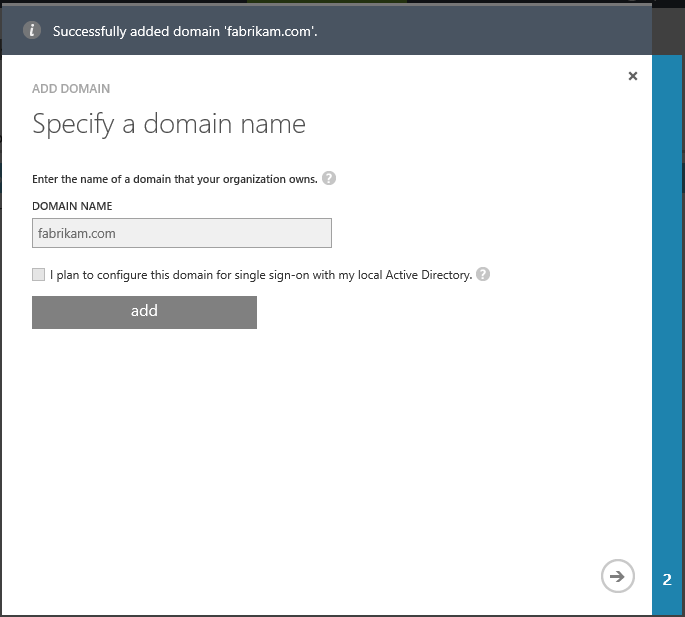
1. Open a browsing session, navigate to the Azure management portal, and sign in as the administrator of the directory to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which an Internet domain should be added.



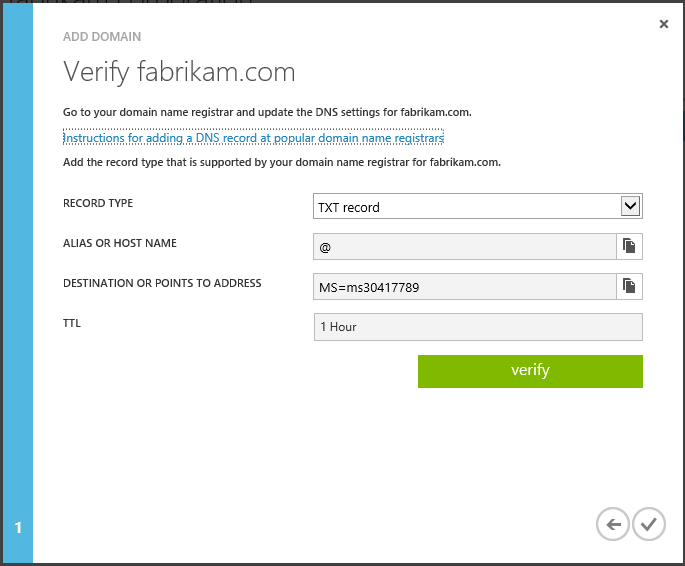
1. Click **ADD A CUSTOM DOMAIN** if no Internet domain have been added so far or **ADD** at the tray of the bottom. An **ADD DOMAIN** dialog brings up.



1. On the **Specify a domain name** page, type the domain name that you want to add. **I plan to configure this domain for single sign-on with my local Active Directory** enabled to prepare the configuration as a federated Internet domain. For the moment, do not check this option.
2. Click **add**.



1. Click the arrow icon at the bottom right.



1. Follow the steps on the page to verify the Internet domain name you have added belongs to you.

To prove that you control the domain, you then use the above information to create a CNAME record in the authoritative DNS server for the newly added DNS Internet domain. Azure AD indeed uses a DNS record that you create at your registrar to confirm that you really own the domain. In our illustration, the information to add in your DNS domain registrar consists in a TXT record with the value “*MS=ms30417789*”.

Note For more information on this process, including detailed step-by-step directions for several popular domain name registrars, see the Microsoft TechNet article [Verify a domain at any domain name registrar](http://technet.microsoft.com/en-us/library/jj151803.aspx)[[84]](#footnote-84).

1. Once the TXT record is added to your DNS domain registrar, click **verify** to complete the registration.
2. If the domain is successfully verified, click the check mark at the bottom right to close the dialog.

As an illustration of the aforementioned Azure AD module cmdlets, let’s see how to add and verify a custom Internet domain with Windows PowerShell.

Like for the above steps 4 to 6, the **New-MsolDomain** cmdlet enables to add a standard (cloud) Internet domain. After running this command, you have to prove that your organization owns the DNS namespace in the public Internet DNS.

For that purpose, and in order to verify the DNS domain name, you need to use the **Get-MsolDomainVerificationDns** cmdlet in order to get the DNS record information required to create for the new cloud domain.

Once the given TXT record is added at your DNS domain registrar, you finally prove your control of the DNS namespace by running the **Confirm-MsolDomain** cmdlet.

Likewise, you can use the **New-MsolFederatedDomain** cmdlet to create of custom federated (single sign-on) domain in your directory. Finally, the **Set-MsolDomainAuthentication** cmdlet enables to convert a standard domain into a single-sign on domain.

When a domain is federated, you will no longer have the option to add the domain suffix to the user accounts. The users will need to be created on-premises in order for them to have the federated domain name available to them. You can still create accounts directly in the cloud, but they cannot have the federated domain name assigned to them unless they are created on-premises. Remember the directory integration scenario **Directory synchronization with single sign-on earlier in this document.**

Moreover, and as expected, when the user signs-in to Azure AD with his federated account, he’s invited to authenticate on the on-premises identity infrastructure. If single sign-on is correctly set up, you will indeed notice that the user cannot even type a password in the login Web page of the sign-in service of Azure AD. Password will be indeed shaded. The user will be instead smoothly redirected to the declared on-premises identity provider.

## Synchronizing your directory with the on-premises directories

If your organization uses an on-premises directory service, you can synchronize it with your Azure AD tenant to simplify your cloud-based administrative tasks and even provide your users with a more streamlined sign-in experience.

Generally speaking, identity provisioning and synchronization is a complex space. This has generated in the past some burden and hassle on-premises for the organizations to keep in sync all their identities silos resulting from the deployment of various Line of Business (LOB) solutions.

Directory synchronization is the first integration capability offered by Azure AD with your on-premises. As an IdMaaS offering, Azure AD provides, as anyone can imagine, many options, to support a myriad of customer configurations – from the very simple to the most complex one. (Regardless of your own specific situation, we strongly recommend leading with “simple” this space in a hybrid manner with the cloud.)

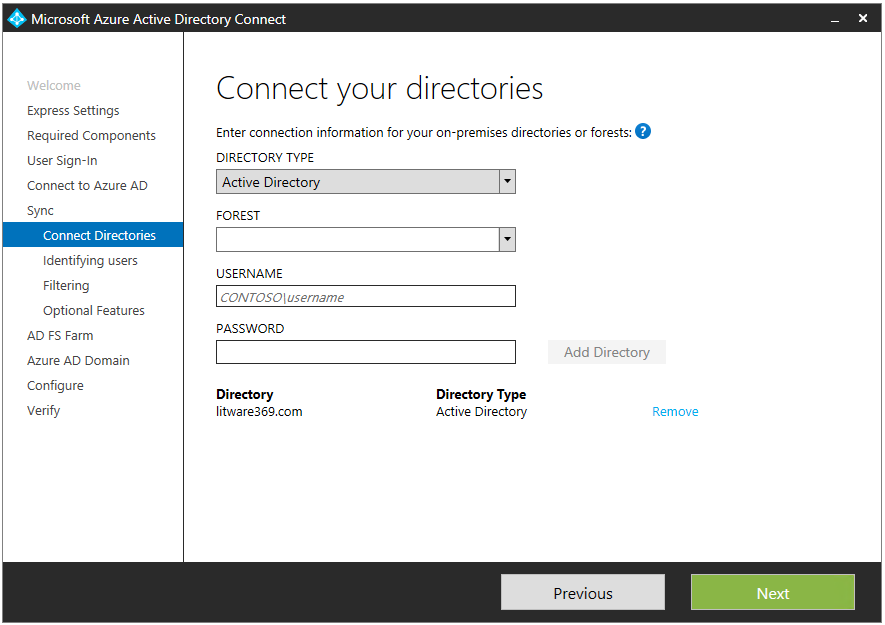
Azure AD indeed enables the support of on-premises Windows Server Active Directory (WSAD) mono and multi-forest environments as well as non-Active Directory directories environments. Thus, it has provided over the time multiple technical choices to both better accommodate the on-premises existing environments and to adequately sustain the subsequent identity provisioning and synchronization:

* Directory Sync Tool (DirSync),
* Azure Active Directory Sync Tool (Azure AD Sync),
* Microsoft Forefront Identity Manager (FIM) Sync Engine (hotfix 4.1.3493.0, or later) with the Azure AD Connector (deprecated),
* Azure Active Directory Module for Windows PowerShell (see earlier in this document),
* Azure AD Graph API.

Note For additional information, see the Microsoft MSDN article [Directory Integration Tools](https://msdn.microsoft.com/en-us/library/azure/dn757582.aspx)[[85]](#footnote-85).

This section consequently aims at describing the main situations, and in those contexts, providing recommendations and guidance for the selection of the right directory provisioning and/or synchronization tooling, when working with Azure AD.

**The now generally available** [**Azure Active Directory Connect (Azure AD Connect)**](http://www.microsoft.com/en-us/download/details.aspx?id=47594)**[[86]](#footnote-86) provides a single and unified wizard that streamlines and automates the overall onboarding process for both directory synchronization with on-premises AD mono-forest and multi-forest environments (including password (hash of hash) synchronization) and single sign-on if you want to.**



Note For additional information, see the blog post [Azure AD Connect & Connect Health is now GA!](http://blogs.technet.com/b/ad/archive/2015/06/24/azure-ad-connect-amp-connect-health-is-now-ga.aspxhttp:/blogs.technet.com/b/ad/archive/2015/06/24/azure-ad-connect-amp-connect-health-is-now-ga.aspx)[[87]](#footnote-87), and the Microsoft TechNet article [Azure Active Directory Connect](https://msdn.microsoft.com/en-us/library/azure/dn832695.aspx)[[88]](#footnote-88).

Directory provisioning refers to the creation and management of directory entries. In the context of Azure AD, directory provisioning is different from directory synchronization, in that objects that are provisioned are mastered in the Azure AD and can be edited online. Directory provisioning can be performed through Azure AD management or programming interfaces such as the Azure management portal, the bulk upload using .csv files, the Azure AD Module for Windows PowerShell cmdlets or the Azure AD Graph API.

While some form of directory synchronization can be implemented using these interfaces, this remains different from Azure AD directory synchronization where objects are mastered on-premises and the online object is a copy of the on-premises object and cannot be edited online.

Note Third party synchronization tools are not explicitly covered, as they typically fall under the above Azure AD Module or the Azure AD Graph API categories.

### Synchronizing your directory with Active Directory on-premises

#### About the DirSync tool

In order to stay with the aforementioned simplicity principle, Azure AD (and Office 365) initially came with a pre-packaged identity synchronization engine named the DirSync[[89]](#footnote-89) tool, based on the FIM product and customized for a single scenario allowing the synchronization with an Active Directory mono-forest environment: it was and can be used to replicate WSAD user accounts (and other Active Directory objects) in your Azure AD directory tenant, whether it is a standalone one (as enabled by the various Azure AD offerings) or the directory of, for instance, your Office 365 subscription.

Important note Neither the Active Directory (and Exchange) multi-forest environment synchronization - which is also a (very) common scenario for largest companies - nor the synchronization with other directories were and are covered by the DirSync tool.

Note For additional information, see the Microsoft MSDN article [Azure Active Directory Synchronization Tool (DirSync)](https://msdn.microsoft.com/en-us/library/azure/dn790211.aspx)[[90]](#footnote-90).

Unlike manually created accounts, accounts created by the DirSync tool are fully populated with user account information from Active Directory. This enables service administrators keeping Azure AD objects updated with changes made in the on-premises WSAD.

**Note** For a list of attributes that are synchronized with the current DirSync tool, see the Microsoft TechNet article [DirSync: List of Attributes that are Synced by the Windows Azure Active Directory Sync Tool](http://social.technet.microsoft.com/wiki/contents/articles/19901.dirsync-list-of-attributes-that-are-synced-by-the-windows-azure-active-directory-sync-tool.aspx)[[91]](#footnote-91).

Moreover, starting with version 1.0.6385.0012 of DirSync[[92]](#footnote-92), password (hash of hash) synchronization can be provided.

Important note The Azure AD team regularly has updated the DirSync client with new features and functionality. Not all additions are applicable to all audiences.  To keep track of the versions that have been released, and to understand whether you may need to update to the newest version or not, see the Microsoft TechNet Wiki article [Azure Active Directory Sync tool - Version Release History](http://social.technet.microsoft.com/wiki/contents/articles/18429.windows-azure-active-directory-sync-tool-version-release-history.aspx)[[93]](#footnote-93).

Note Organization who are already running directory synchronization and single sign-on (aka federation) in a single AD forest may decide that password (hash of hash) synchronization is sufficient to meet their business requirements. A transition path is available for them. For more information on this process, see the Microsoft TechNet wiki article [DirSync: How To Switch From Single Sign-On To Password Sync](http://social.technet.microsoft.com/wiki/contents/articles/17857.aad-sync-how-to-switch-from-single-sign-on-to-password-sync.aspx)[[94]](#footnote-94).

Directory synchronization is not something that is new for Azure AD. The DirSync tool is built on top of FIM. The configuration of directory synchronization has been simplified for the Azure AD environment.

**Note** For details pertaining to this topic, see the Microsoft TechNet articles [Directory synchronization roadmap](http://technet.microsoft.com/en-us/library/hh967642.aspx)[[95]](#footnote-95) and [Manage directory synchronization](http://technet.microsoft.com/en-us/library/jj151821.aspx)[[96]](#footnote-96).

There is no manual configuration that you need to be concerned with, everything being configured via wizards.

Note For more information on how to proceed with the installation of DirSync, see the Microsoft TechNet Wiki articles [HowTo: Install the Azure Active Directory Sync Tool (now with Pictures!)](http://social.technet.microsoft.com/wiki/contents/articles/19098.howto-install-the-windows-azure-active-directory-sync-tool-now-with-pictures.aspx)[[97]](#footnote-97) and [Best Practices for Deploying and Managing the Azure Active Directory Sync Tool](http://social.technet.microsoft.com/wiki/contents/articles/17370.best-practices-for-deploying-and-managing-the-windows-azure-active-directory-sync-tool.aspx)[[98]](#footnote-98).

This said some customers may have in this context a requirement to scope what objects are synchronized from their on-premises Active Directory to their Azure AD directory tenant. Common requests in this area are typically:

* The ability to exclude an Active Directory domain from the scope,
* The ability to exclude an organizational unit (OU) from the scope,
* The ability to exclude specific objects from the scope, based on attribute-level filtering.

Directory synchronization scoping is something supported through the DirSync tool at the following levels:

* **Domain-based**. You can use this filtering type to manage the properties of the source AD management agent (connector) in the DirSync tool. This type enables you to select which domains are allowed to synchronize to the cloud.
* **Organizational unit–based**. You can use this filtering type to manage the properties of the source AD management agent (connector) in the DirSync tool. This filtering type enables you to select which OUs are allowed to synchronize to the cloud.
* **User attribute–based**. You can use this filtering method to specify attribute-based filters for user objects (and user objects only). This enables you to control which objects should not be synchronized to the cloud.

Important note Preventing the replication of certain attributes to Azure AD is not supported with the DirSync tool. All attributes must be part of the scope.

See the related instructions to completely setup the directory synchronization for your domain(s) within your Azure AD directory tenant.

#### Considering first the Azure AD Connect tool

As previously mentioned, the DirSync tool was intended for on-premises AD single-forest scenarios. However, many customers are operating with more than one on-premises Active Directory forest for a variety of reasons, such as:

* Multiple account forests, where user accounts exist in multiple Active Directory forests;
* Account and resource forests, where the Exchange organization is typically hosted in a resource forest model.

Multi-forest topologies can be supported through the Azure AD Sync tool initially released in September 2014[[99]](#footnote-99). This tool that was considered as the successor of DirSync is flexible, and can accommodate most Active Directory and Exchange multi-forest scenarios:

* **Single Account Forests**, single or multiple Exchange resource forest(s).
* **Multiple Account Forests**, with no on-premises Exchange.
* **Multiple Account Forest**, single or multiple Exchange resource forest(s).

Note For additional information, see the Microsoft MSDN article [Azure Active Directory Sync](https://msdn.microsoft.com/en-us/library/azure/dn790204.aspx)[[100]](#footnote-100).

This is anawaited feature was that previously only available with the [Azure AD connector](http://www.microsoft.com/en-us/download/details.aspx?id=41166)[[101]](#footnote-101) and Microsoft Forefront Identity Manager (FIM) 2010 R2.

Beyond this key characteristic, Azure AD Connect includes a rich set of sync and write-back capabilities:

* Enable your users to perform self-service password reset in the cloud with write-back to on-premises AD.
* Enable provisioning from the cloud with user write back to on-premises AD.
* Enable write back of “Groups in Office 365” to on-premises distribution groups in a forest with Exchange.
* Enable device write back so that your on-premises access control policies enforced by AD FS can recognize devices that registered with Azure AD. This includes the recently announced support for Azure AD Join in Windows 10.

Note For more information, see the whitepaper [Azure AD & Windows 10: better Together for Work and School](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[102]](#footnote-102).

Note For version release history on AAD Connect, see the article [Azure AD Connect: Version Release History](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-version-history/)[[103]](#footnote-103).

* Sync custom directory attributes to your Azure AD tenant and consume it from your cloud applications.

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Stay on existing DirSync tool** | **Upgrade to new DirSync tool** | **Migrate or deploy the Azure AD Connect tool** |
| Existing DirSync tool’s customers | Remain on current deployment if:   * No issues and meets needs. * In a supported configuration. * Have no requirements for new capabilities. | Upgrade to the latest DirSync tool if:   * Performance improvements are a factor * Directory extensions sync is needed * Password write back is needed * Deletion prevention is needed * Log shipping to cloud (support and troubleshooting) is needed | Migrate to the Azure AD Connect tool for:   * AD Multi-Forest sync is needed * Removal of unsupported DirSync configurations is required * Attribute filtering is needed * Enhanced security permission requirements |
| New customers | N/A | Office 365 customers will default here as of this writing | Azure AD Premium customers likely to default here |

Azure AD Connect is replacing both the DirSync tool and the Azure AD Sync tool (download), and allows in this context upgrading or migrating your existing DirSync or Azure AD Sync deployment quickly and easily with little or no impact.

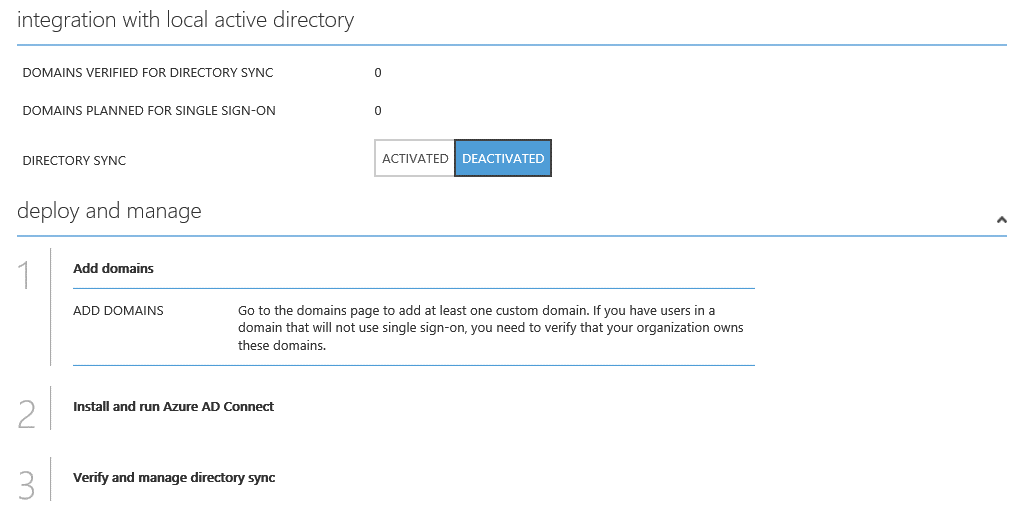
Azure AD Sync is the sync engine of Azure AD Connect and **Azure AD Connect is now THE one stop shop for connecting your on-premises directories to Azure AD, whether you are evaluating, piloting, or in production.**

Note For information on the supported topologies, see the article [Topologies for Azure AD Connect](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-topologies/)[[104]](#footnote-104).

**Generally speaking, and considering the above, the Azure AD Connect should be the preferred solution for directory synchronization.**

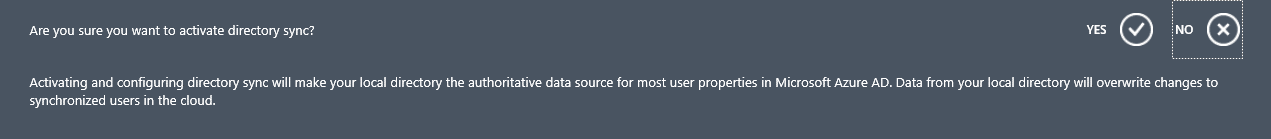
Note For additional information, see the Microsoft article [Integrating your on-premises identities with Azure Active Directory](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/)[[105]](#footnote-105).

Setting up directory synchronization for domain(s) within your Azure AD directory tenant with Azure AD Connect requires to conduct a few steps as outlined under the section **DIRECTORY INTEGRATION** for the selected directory in the Azure management portal.



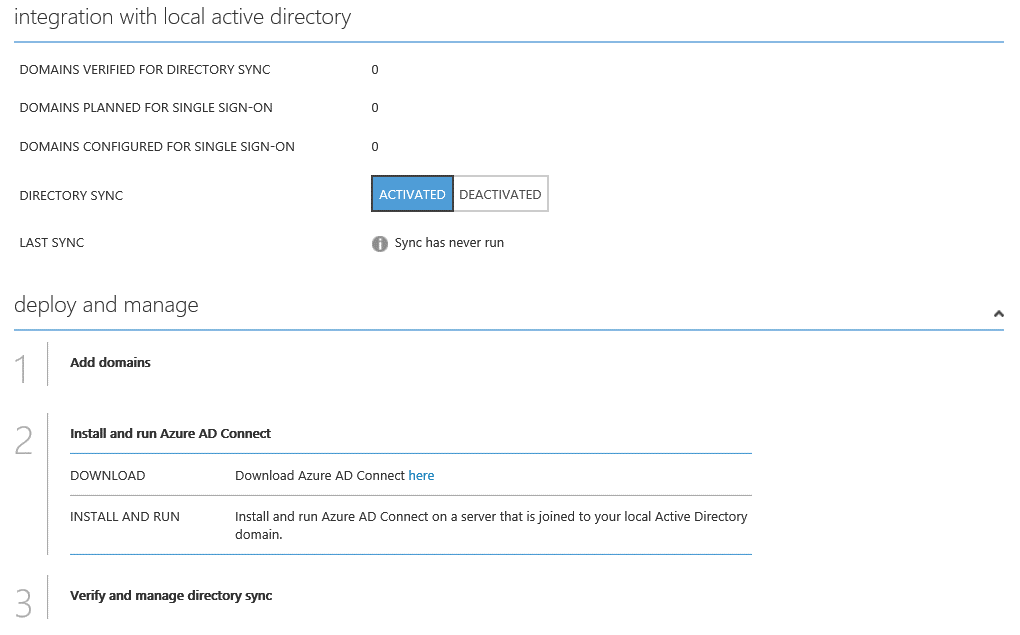
The first step consists in activating directory synchronization by clicking **ACTIVATED** and then **SAVE** at the bottom of the tray.

This should be considered a long-term commitment to coexistence scenarios between your on-premises WSAD and your Azure AD directory tenant in the cloud.



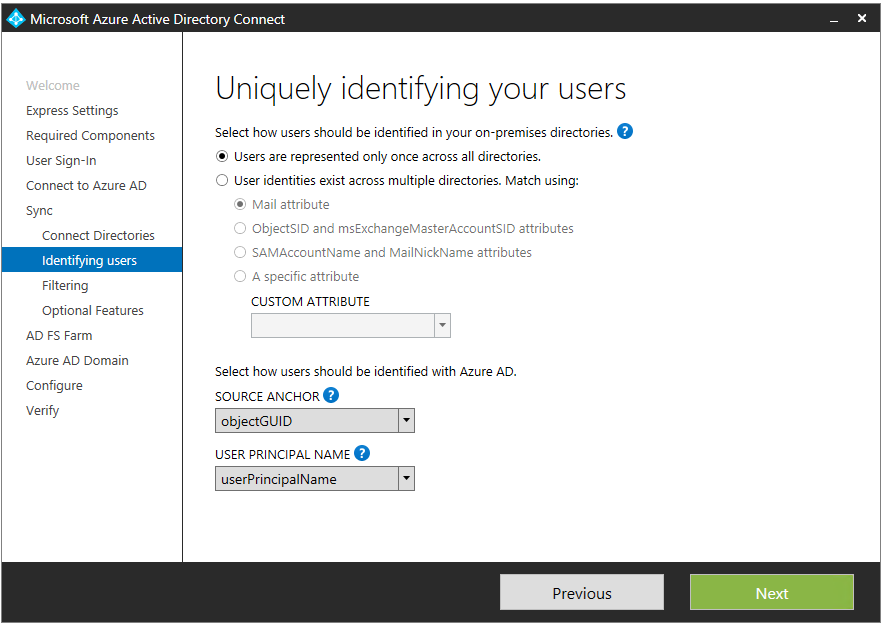
This first operation results in enabling the DirSync Web Service endpoint (known as AWS). This endpoint provides support for batch methods as well as proprietary sync features. It is thus only available to Azure AD Connect (as well as the aforementioned DirSync tool, the Azure AD Sync tool, and the Azure AD Connector for FIM). This interface is not available to support custom synchronization solutions.

After directory synchronization has been activated, you will need to add at least one custom domain. This is the second step. Synchronized objects are mastered on-premises and can only be edited using on-premises applications. The online objects are a copy of the on-premises objects with which they’re synced.



After ensuring that both your on-premises and cloud environments are ready for directory synchronization as per step two – notably see the Microsoft TechNet article [Prepare for directory synchronization](http://technet.microsoft.com/library/jj151831.aspx)[[106]](#footnote-106) -, you can then download [Azure AD Connect](http://www.microsoft.com/en-us/download/details.aspx?id=47594)[[107]](#footnote-107) installation package (*AzureADConnect.msi*) and install it. This is the third step.

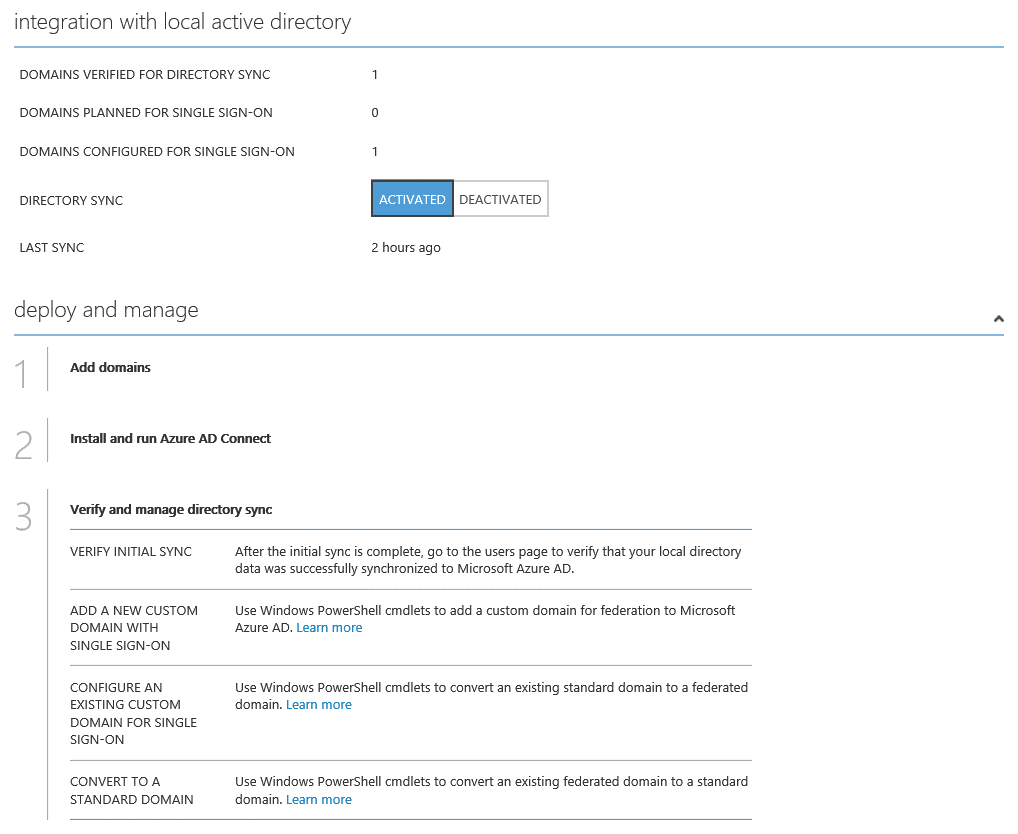
Specify in the Azure AD Connect wizard all the setting parameters that relate to your own configuration.



Important note Users in different AD forests will require a different UPN suffix. In other words, it is not possible to provide a single UPN domain for all users, across all forests. For example, you may not assign *corpfabrikam.com* as a UPN suffix for all users. Users in Forest A will be assigned a UPN suffix of *ForestA.com* and users in Forest B will be assigned a UPN suffix of *ForestB.com*. Shared UPN namespaces across forest are not supported by design.

For more information, see the (old) Microsoft TechNet articles [Considerations for Deploying Forest Trust](http://technet.microsoft.com/en-us/library/dd560680%28v=WS.10%29.aspx)[[108]](#footnote-108) and [Additional Configuration for Functionality Across Forests (Multiple Forest Considerations in Windows 2000 and Windows Server 2003)](http://technet.microsoft.com/en-us/library/cc779566%28v=WS.10%29.aspx)[[109]](#footnote-109) (search for "Shared UPN").

Once the configuration is completed, you can the verify that the initial sync is complete and manage the directory sync over the time.



Note The [Azure Active Directory Connect Health (Azure AD Connect Health)](https://msdn.microsoft.com/en-us/library/azure/dn906722.aspx)[[110]](#footnote-110) cloud based service in the [new Azure Portal](https://portal.azure.com/)[[111]](#footnote-111) 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.

While the currently available release in GA focusses on AD FS, a public preview of Connect Health for sync now allows you to monitor and gain insights into the sync service of Azure AD Connect. For more information, see the blog post [Azure AD Connect Health for sync is now in Public Preview!](http://blogs.technet.com/b/ad/archive/2015/11/05/azure-ad-connect-health-for-sync-is-now-in-public-preview.aspx)[[112]](#footnote-112).

Deployment integration with Azure AD Application proxy, additional sync and sign on options will be also added in the future. It represents a key part of our effort to help you monitor and secure your cloud and on-premises identity infrastructure.

Azure AD Connect Health is a feature of the Azure AD Premium edition (see later in this document) 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 the article [Monitor your on-premises identity infrastructure in the cloud](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-health/)[[113]](#footnote-113).

#### When the Azure AD Connector for FIM may be still considered

**For multi-forest scenario, the Azure AD Connector is being deprecated in favor of the Azure AD Connect tool.**

Generally speaking, and as outlined before, the Azure AD Connect tool use should be the preferred solution. The primary reasons are listed hereafter:

* The Azure AD Connect tool has been designed to be easy to deploy and its configuration is completely automated through a wizard.
* In case of issues with directory synchronization, troubleshooting of the Azure AD Connect tool will typically be easier. The deployment of the Azure AD Connector is a custom task, which is more complex and can be associated with configuration errors. The deployment and maintenance is more effort intensive and therefore more costly.
* No licensing requirements apply for the Azure AD Connect tool, while a FIM server license and possibly Visual Studio licenses are required for the Azure AD Connector.

Important note Azure AD Premium incudes the usage rights for FIM server licenses and CALs. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[114]](#footnote-114).

**Using the Azure AD connector with FIM 2010 R2 remains available for existing customers.** Organizations can thus continue to completely control partitioning of information between on-premises and the cloud, support AD multi-forest environments (as Azure AD Connect does) and support other directories and data sources other than AD – for example OpenLDAP or SAP (as Azure AD Connect will).

**New deployments on the basis of this solution are however no longer recommended.**

The connector is available on the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=41166)[[115]](#footnote-115).

Important note The Azure AD connector does not provide password (hash of hash) sync support.

Important note The Azure AD Connector provides support for directory synchronization only. In other words, the Azure AD Connector does not cover licensing or service provisioning. For Office 365 customers, they will still have to assign licenses to their users in a second step, after directory synchronization completes – which can be achieved through custom PowerShell commands or the Azure AD Graph API.

It is recommended to deploy the Azure AD Connector on a dedicated FIM instance. While the deployment of the Azure AD on an existing FIM 2010 R2 server is possible (but not supported), it will also increase the complexity of the configuration and make troubleshooting and maintenance more difficult.

Note For more information, see the Microsoft TechNet article [Azure Active Directory Connector for FIM 2010 R2 Technical Reference](http://technet.microsoft.com/en-us/library/dn511001(v=ws.10).aspx)[[116]](#footnote-116).

#### Other options to potentially consider

As you already know, the Azure AD Module for Windows PowerShell allows administrators to perform a variety of management tasks from the command line, including user management, group and group membership management and license management.

The Azure AD Graph API enables similar functions, through a REST-based API interfaces. Likewise, it allows accessing the most common properties of all object types in the directory. The [MSDN documentation](http://msdn.microsoft.com/library/azure/hh974478.aspx)[[117]](#footnote-117) describes these properties and shows which ones are write-able. It supports managing all directory objects including *Users*, *Groups*, *Contacts* (delete/update), user license assignment, and managing user’s manager and direct report relationships.

Through these two interfaces, you can automate provisioning operations such as the creation, modification or deletion of objects in your Azure AD directory tenant.

For Office 365 customers, whilst they also allow the creation of Exchange mailboxes through license assignment, they do not permit the creation of mail-enabled groups or contacts. The management of Exchange objects is not covered.

Mail-enabled objects need to be created through Exchange Online remote PowerShell, after objects have been replicated from the Azure AD directory tenant to the Exchange Online directory.

Note Exchange Online remote PowerShell is in no way tied to the Azure AD Module for Windows PowerShell. By connecting to the Microsoft Exchange Online services, you connect to the Microsoft Exchange Online datacenter's server environment, i.e. a server-side session, which contains the commands used in the cloud-based service. In other words, a remote PowerShell interface is available to you so that you can access the Exchange Online configuration information using a separate set of Windows PowerShell cmdlets. For additional information, see the article [Connect Windows PowerShell to the Service](http://help.outlook.com/en-us/140/cc952755.aspx)[[118]](#footnote-118) and the blog post [Using Exchange Management Shell to manage your Exchange Online and Exchange On Premises Environment](http://blogs.technet.com/b/ilvancri/archive/2012/03/17/3487056.aspx)[[119]](#footnote-119).

Using Exchange Online remote PowerShell, administrators can manage Exchange Online objects and properties, either for automation purposes or to manage items that are otherwise not exposed through the portal.

Note Exchange Online remote PowerShell offers the same PowerShell cmdlets as Exchange Server 2010 Service Pack 1 (SP1) and above, with certain commands and parameters disabled because these features do not apply in the hosted environment. For a list of the cmdlets available to Exchange Online administrators, see [Reference to Available PowerShell Cmdlets in Exchange Online](http://help.outlook.com/en-us/140/dd575549.aspx)[[120]](#footnote-120).

Be aware that theses interfaces do not provide the same set of capabilities as the previously discussed directory synchronization tools provided by Microsoft. More specifically:

* These interfaces only provide access to a subset of attributes that can be managed through the Azure AD Sync tool (or the DirSync tool or the Azure AD connector for FIM).
* Service-side throttling is applied on these interfaces in order to protect the service and the customers against large batches of commands. This may slow down provisioning / synchronization of users, and each full synchronization cycle may take a very long time to complete.
* Azure AD Module for Windows PowerShell doesn’t provide mechanisms to enumerate changes that occurred in the directory tenant, making it not well suited to directory synchronization processes. (The Azure AD Graph API supports the differential query since November 2012.)
* From a service perspective, objects provisioned through the cmdlets of Azure AD Module for Windows PowerShell will not appear as “synchronized” objects.

Consequently, the use of interfaces for object provisioning purposes should currently be limited to scenarios where:

* A limited number of objects need to be managed.
* Exchange Hybrid (“rich coexistence”) is not required for Office 365 customers. Directory synchronization is available only through the DirSync tool or the Azure AD Connector. Directory Synchronization is mandatory to support certain features such as Exchange hybrid coexistence.

As such, the Azure AD Module for Windows PowerShell (and potentially the Azure management portal) can be recommended to customers who only need cloud identities and do not require a synchronization solution at all – falling in the “zero on-premises hardware” category.

The following table synthetizes the available options for on-premises AD single or multi-forest scenarios:

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Azure AD Connect** | **Windows PowerShell provisioning** | **Azure AD Graph API provisioning** |
| Cloud identities:   * No Federation * No Exchange coexistence for Office 365 customers | Recommended | Available  Performance limitations may apply | Available  Performance limitations may apply |
| Federated identities | Recommended | Available | Available (as per version 2013-11-08 and above[[121]](#footnote-121)) |
| Exchange Hybrid deployments (“rich coexistence”) for Office 365 customers | Required | Not available  Required attributes are not exposed | Not available  Required attributes are not exposed |

### Synchronizing your directory with non-AD directories on-premises

Current version of the Azure AD Connect tool does not provide a support for non-AD directories (LDAP directory, SQL database, and others).

Unlike the Azure AD Connect tool, the Azure AD Connector does not require an Active Directory to synchronize from. (It uses the FIM Metaverse as a source). Consequently, almost any directory or combination of directories may be used as a synchronization source, provided that a FIM management agent (or connector) is available to support this directory or directories.

The Microsoft TechNet article [Management Agents in FIM 2010 R2](http://technet.microsoft.com/en-us/library/jj863241(v=ws.10).aspx)[[122]](#footnote-122) provides a list of management agents that are available with FIM such as the [Forefront Identity Manager Connector for Generic LDAP](http://www.microsoft.com/en-us/download/details.aspx?id=41163)[[123]](#footnote-123) for LDAP directories.

Note The next version of FIM is currently [Microsoft Identity Manager (MIM) 2016](http://www.microsoft.com/en-gb/server-cloud/products/microsoft-identity-manager/default.aspx)[[124]](#footnote-124).

Alternatively, it is also possible to develop custom management agents, to use other interfaces such as text files, or to leverage management agents that are provided by third party vendors or in the public domain as open source solutions such as the [OpenLDAP Extensible Management Agent (XMA)](http://sourceforge.net/projects/openldap-xma/) project on SourceForge[[125]](#footnote-125).

As also discussed in the previous section, Azure AD Module for Windows PowerShell and the Azure AD Graph API may also be used to automate the provisioning and maintenance of Azure AD identities.

The Azure AD Module for Windows PowerShell provisioning can be recommended today, for customers who have extensive scripting experience or are willing to work with a partner to develop a custom solution. In the latter situation, the Azure AD Graph API can be leveraged.

For instance, to create a federated user for Office 365, proceed with the following steps:

1. Open a Windows PowerShell prompt and import the module:

PS: C:\Windows\system32> Import-Module MSOnline

1. Establish a session with your Azure AD directory tenant with the **Connect-MsolService** cmdlet. You will be prompted to enter your admin credentials (such as *admin@xxx.onmicrosoft.com* and password) to authenticate against your Azure AD directory tenant.

PS: C:\Windows\system32> Connect-MsolService

1. Obtain the unique string ID of the account/SKU combination that will be needed to assign a license, for example “*idmgt:ENTERPRISEPACK*” in our configuration with the **Get-MsolAccountSku** cmdlet.

PS C:\Windows\system32> Get-MsolAccountSku

1. Create the user with the **New-MsolUser** cmdlet:

PS C:\Windows\system32> New-MsolUser -DisplayName user1 –UserPrincipalName user1@corpfabrikam.onmicrosoft.com -UsageLocation FR -BlockCredential $false –ImmutableId 81372

1. Set the user’s license with the **Set-MsolUserLicense** cmdlet:

PS: C:\Windows\system32> Set-MsolUserLicense -UserPrincipalName user1@corpfabrikam.onmicrosoft.com -AddLicenses "idmgt:ENTERPRISEPACK"

Several third-party solutions built on these interfaces are available today, providing a simple solution for such scenarios. As an example, we can mention the [Optimal IdM](http://www.optimalidm.com/)[[126]](#footnote-126) solution.

This said, keep in mind notably that:

* These two interfaces were not designed for directory synchronization
* The operations will take longer time to complete due to server-side throttling,
* Certain features are not supported with the provisioning based on these interfaces.

The following table synthetizes the available options for on-premises non-AD directories scenarios:

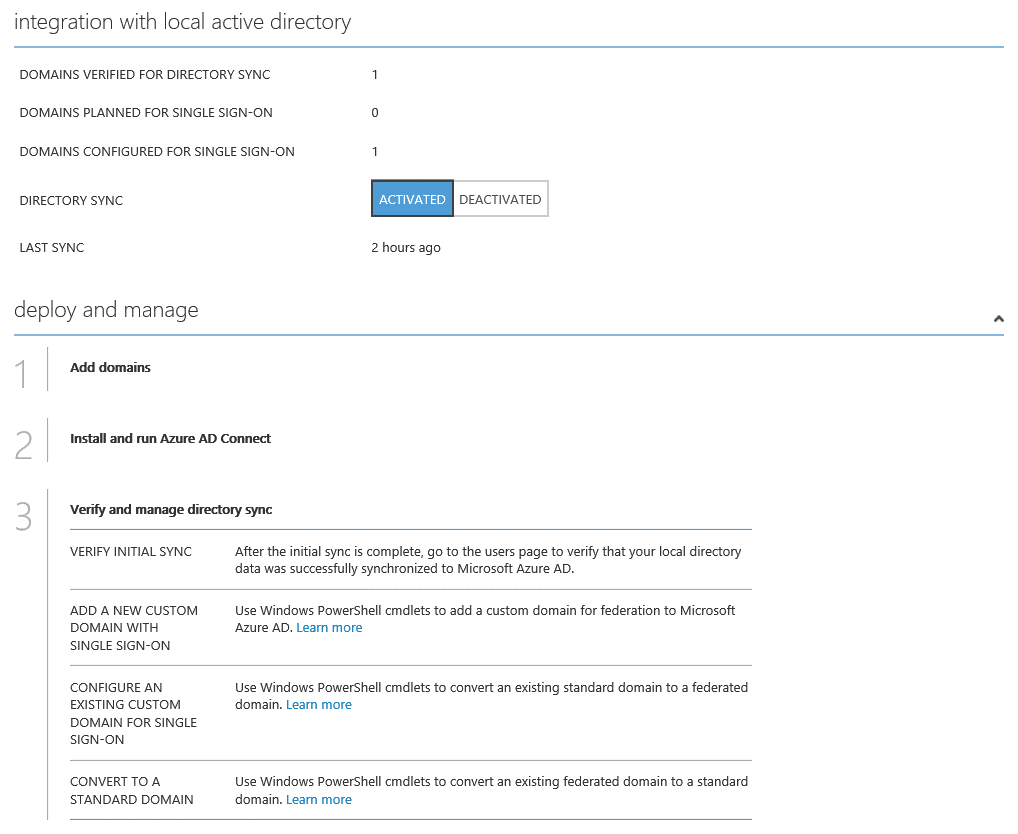
|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Azure AD Connector** | **Windows PowerShell provisioning** | **Azure AD Graph API provisioning** |
| Cloud identities   * No Federation | Available | Available  Performance limitations may apply | Available  Performance limitations may apply |
| Federated identities with a supported on-premises Security Token Services (STS) | Available  Non-AD synchronization through FIM 2010 R2 provided that a FIM management agent is available to support the on-premises directory or directories. | Available | Available (as per version 2013-11-08 and above) |

For Office 365 customers, Exchange coexistence is not available in non-AD directories scenarios since by definition customer cannot have Exchange server in this case.

## Federating your directory with the on-premises directories

This section as its title indicates addresses the identity federation topic (aka single sign-on) from the Azure AD perspective, which is the second integration capability provided by Azure AD.

Setting up identity federation for domain(s) within your Azure AD directory tenant requires to conduct a few steps as outlined in the classic Azure management portal.



Identity federation in general is also a broad topic, with many facets, depths of understanding, protocols, standards, tokens, etc. As an illustration, [Wikipedia](http://en.wikipedia.org/wiki/Federated_identity)[[127]](#footnote-127) defines identity federation as follows:

“*Federated identity, or the ‘federation’ of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration.*”

As such, it requires preparation to be successful in this area and, more specifically in the context of Azure AD, to fulfill the requirements for this integration capability. This is the purpose of the step two in the above snapshot.

Moreover, as previously outlined, whilst single sign-on (aka federation) is not required for directory synchronization (but it will provide a richer user experience), directory synchronization is however a requirement for federation.

Hence, the implementation of directory synchronization is needed in order to keep the on-premises identities in sync with the organization’s Azure AD directory tenant.

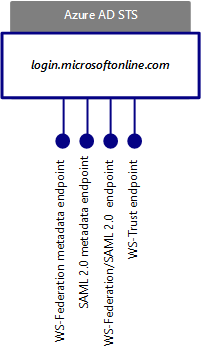
One of the benefits is that it enables controlling and managing the corporate user accounts in the traditional way through the existing tooling that accompanies the on-premises identity infrastructure.

This one piece really does provide seamless user management between the on-premises and Azure AD environments. See the previous section to see how to synchronize your directory with your on-premises directory.

When an organization leverages these two integration capabilities, i.e. directory synchronization and federation (also called single sign-on), its identity management capability are stretching over both an on-premises deployment and a cloud deployment. This ability to operate across both on-premises and cloud deployments in a hybrid mode enables an organization to easily take advantage of cloud (SaaS) applications while all of its existing identity management processes and existing on-premises applications can continue unaffected. This aspect is critical for some organizations that need to comply with business or regulatory requirements that mandate that certain critical information, such as passwords, be maintained in on-premises servers.

### Endpoints to federate your directory with your on-premises STS

Azure AD publishes at *login.microsoftonline.com* level several endpoints that serve for establish a federation and do single sign-on with an on-premises identity infrastructure:



Azure AD publishes a federation metadata document for these addressable endpoints. For that purpose, Azure AD publishes two metadata endpoints to federate your directory with your on-premises supported STS:

1. One endpoint for WS-\* based protocols published at the following URL:

<https://nexus.microsoftonline-p.com/federationmetadata/2007-06/federationmetadata.xml>.

Note The general syntax and semantics of these metadata are defined in the [OASIS Web Services Federation Language (WS-Federation) Version 1.2](http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf)[[128]](#footnote-128). It covers the configuration data (endpoint URLs, key material for verifying signatures, etc.) to establish trusts between WS-\* entities.

1. Another endpoint for the SAML 2.0 protocol published at the following URL:

<https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>

Note The general syntax and semantics of metadata are defined in the [Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)[[129]](#footnote-129). It covers the configuration data (endpoint URLs, key material for verifying signatures, etc.) to establish trusts between SAML 2.0 entities.

As per the above metadata, 2 public endpoints are published by Azure AD for the interaction with organization’s on-premises identity infrastructure:

1. One multipurpose endpoint located at: <https://login.microsoftonline.com/login.srf>. This endpoint is indeed:
2. A passive endpoint for web (browser) based clients on the WS-Federation protocol.
3. A passive endpoint for web (browser) based clients on the SAML 2.0 web browser single sign-on profile and the SAML 2.0 web browser single sign-out profile.
4. An active endpoint based on the SAML 2.0 Enhanced Client or Proxy (ECP) profile.
5. Another endpoint located at <https://login.microsoftonline.com/extSTS.srf>. This is specifically a WS-Trust-based active endpoint for smart clients.

The former endpoint is the one that renders the credential user interface for Azure AD and that triggers a home realm discovery (HRD) / where are you from (WAYF) process for federated identities as previously illustrated.

### Supported on-premises Security Token Services (STS) for federating your directory

As of writing, Active Directory Federation Service (AD FS), as well as a [list of third-party identity providers’ implementation](http://technet.microsoft.com/en-us/library/jj679342.aspx)[[130]](#footnote-130) enable this integration capability.

Above federation standards, i.e. WS-\* (WS-Federation and WS-Trust) or SAML 2.0 are indeed complex and each implementation tends to have its own “specificity”. This may introduce (slight) differences in the way various features work and some may break resulting in unpredictability of customer experience due to the use of non-tested configurations even if interoperability profiles greatly help in reducing the probability of such side-effects.

In this context, the [Works with Office 365 – Identity](http://blogs.office.com/2014/01/30/the-works-with-office-365-identity-program-now-streamlined)[[131]](#footnote-131) 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)[[132]](#footnote-132), thus enabling a predictable and short qualification path.

The related [program guide](http://www.microsoft.com/en-us/download/details.aspx?id=41185)[[133]](#footnote-133) provides:

1. A first paper that details the agreement for STSs such as AD FS to Interop with Azure AD using the WS-Federation and WS-Trust protocols.
2. A second paper specifies the scenarios for STS testing that Microsoft use for qualification in the Works with Office 365 - Identity program.

It also provides the [Office 365 SAML 2.0 Federation Implementer’s Guide v1.0](http://go.microsoft.com/?linkid=9844221)[[134]](#footnote-134) in terms of implementation using a SAML 2.0 compliant SP-Lite profile STS.

As seen in the previous section, directory synchronization options differ whether your on-premises identity infrastructure relies on WSAD or not.

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

Since directory synchronization is mandatory with federation, the following table provides a comprehensive overview of the possible scenarios with the aforementioned technologies.

|  |  |  |
| --- | --- | --- |
|  | **Active Directory source**  **Directory Sync through the Azure AD Connect tool (or the DirSync tool or the Azure AD Connector)** | **Non-AD directory source**  **Directory sync or provisioning to be implemented using FIM + Azure AD Connector or custom solutions** |
| AD FS  (WS-Federation, WS-Trust) | Available   * Supports web clients * Supports rich clients | Not available   * AD FS only supports Active Directory sources for authentication * Federation chaining or protocol conversion through AD FS is not supported |
| Shibboleth 2  (SAML 2.0) | Available   * Supports web clients * Supports rich clients (only Office applications w/ below restrictions)   For Office 365 customers:   * Supports Office 2010 applications (Excel, PowerPoint, and Word 2010) * Supports Office 365 ProPlus/Office 2013 Windows client applications (Excel, OneNote, PowerPoint, and Word 2013) (1) * Supports Outlook 2010 (2)/Outlook 2013 (1) or (2) * Supports Exchange Active Sync (EAS), POP, IMAP (2) * Does not support Lync 2010 * Supports Lync 2013, Skype for Business, Office Subscription, CRM (1) | Available   * Supports web clients * Supports rich clients (only Office applications w/ below restrictions)   For Office 365 customers:   * Supports Office 2010 applications (Excel, PowerPoint, and Word) * Supports Office 365 ProPlus/Office 2013 Windows client applications (Excel, OneNote, PowerPoint, and Word) (1) * Supports Outlook 2010 (1)/Outlook 2013 (1) or (2) * Supports Exchange Active Sync (EAS), POP, IMAP (2) * Does not support Lync 2010 * Supports Lync 2013, Skype for Business, Office Subscription, CRM (1) |
| Other STS | Solutions along with their related scope listed on the Microsoft TechNet article [Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on](http://technet.microsoft.com/en-us/library/jj679342.aspx)[[135]](#footnote-135).  Generic WS-\* or SAML 2.0 support is provided through the aforementioned Works with Office 365 – Identity program. | Solutions along with their related scope listed on the Microsoft TechNet article Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on.  Generic WS-\* or SAML 2.0 support is provided through the aforementioned Works with Office 365 – Identity program. |

(1) Requires the modern authentication (a.k.a. Active Directory Authentication Library (ADAL) based authentication stack) for Office 365 ProPlus/Office 2013.

(2) Requires installation of the Shibboleth 2 Enhanced Client Proxy (ECP) extension.

The rest of this section further discusses the federation with AD FS and Shibboleth 2.

Once successfully configured, the federated domain(s) are managed via the cmdlets of the Azure AD Module for Windows PowerShell.

### Federating your directory with AD FS

As of writing, the primary option in terms of enterprise identity providers for the single sign-on (aka federation) feature of Azure AD is Active Directory Federation Services (AD FS) that the organization deploys on-premises and then configures Azure AD to securely communicate with.

AD FS in Windows Server 2012 R2 is a component of the Windows Server platform and, as such, the right to use it is included in the associated license costs. Same is true for legacy versions of AD FS (AD FS 2.0 and AD FS in Windows Server 2012),

Important note As far as the legacy version AD FS 2.0 is concerned, the AD FS role available in Windows Server 2008 or in Windows Server 2008 R2 doesn’t correspond to AD FS 2.0; this is the previous version 1.1 instead. The AD FS 2.0 software package for your specific operating system version (either Windows Server 2008 or Windows Server 2008 R2) is the *AdfsSetup.exe* setup file. To download this file, go to [Active Directory Federation Services 2.0 RTW](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=10909)[[136]](#footnote-136). For Windows Server 2012, the AD FS server role includes the same functionality and feature set that is available in AD FS 2.0.

Important note As of writing, and as far as legacy version AD FS 2.0 is concerned, the update rollup 3 for AD FS 2.0 is available. This update rollup includes hotfixes and updates for AD FS 2.0 RTW that are of special interest in the context of this paper for the single sign-on feature of Office 365. For more information about this update rollup and its download, please see article [2790338](http://support.microsoft.com/kb/2790338) Description of Update Rollup 3 for Active Directory Federation Services (AD FS) 2.0[[137]](#footnote-137).

The Microsoft TechNet article [Checklist: Use AD FS to implement and manage single sign-on](http://technet.microsoft.com/en-us/library/jj205462.aspx)[[138]](#footnote-138) provides instructions for Azure AD administrators who want to provide their Active Directory users with single sign-on experience by using AD FS as their preferred STS. It covers AD FS on Windows Server 2012 R2 as well as AD FS on legacy versions of Windows Server.

The white paper [Azure AD/Office 365 Single Sign-On (SSO) with AD FS in Windows Server 2012 R2](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[139]](#footnote-139) provides detailed information on planning and configuring the single sign-on feature for Azure AD/Office 365 with AD FS in Windows Server 2012 R2.

Likewise, as far as AD FS on legacy versions of Windows Server is concerned, the white paper [Microsoft Office 365 Single Sign-On (SSO) with AD FS 2.0](http://www.microsoft.com/en-us/download/details.aspx?id=28971)[[140]](#footnote-140) covers the same topics from an AD FS 2.0 perspective.

These two papers indeed aim at providing a better understanding of the different single sign-on deployment options for Azure AD (and the services in Office 365) with AD FS, how to enable single sign-on using corporate AD credentials and AD FS to Azure, the services in Office 365, and the different configuration elements to be aware of for such deployment.

Note In AD FS in Windows Server 2012 R2, the role of a federation server proxy is handled by a new Remote Access role service called Web Application Proxy (WAP). To enable your AD FS for accessibility from outside of the corporate network (in other words, to configure extranet access), which is the purpose of deploying a federation server proxy in AD FS on legacy versions of Windows Server, you can deploy one or more Web Application Proxies for AD FS in Windows Server 2012 R2. For more information about the Web Application Proxy, see the Microsoft TechNet [Web Application Proxy Overview](http://technet.microsoft.com/en-us/library/dn280944.aspx)[[141]](#footnote-141).

### Federating your directory with other on-premises STS

As outlined before, in addition to AD FS, support for additional STS has been added, so that organizations may continue to use their existing on-premises identity infrastructure for single sign-on with Azure AD and the Microsoft services such as Office 365, Dynamics CRM Online, and other, whether this identity infrastructure is based on AD or on non-AD directories. For organizations that already have a federated SSO infrastructure in place, it is indeed highly desirable to reuse it for Azure AD.

Shibboleth 2 is one of these additional identity providers. Shibboleth 2 (as a reference to the Hebrew word "shibbóleth” and the related Biblical use, i.e. to discover hiding members of the opposing group) was designed to fill higher education needs in terms of identity federation and attributes propagation for a number of partners. The Shibboleth project was initiated by the [Internet2/MACE (Middleware Architecture Committee for Education)](http://middleware.internet2.edu/MACE)[[142]](#footnote-142) in 2000. The project now hosted by the [Shibboleth Consortium](http://shibboleth.net/)[[143]](#footnote-143) refers to both a specification and an open source project that implements them as a distributed system.

As of today, considering its origin, the Shibboleth 2 Identity Management system is notably and unsurprisingly leveraged by many educational and research institutions around the world. Shibboleth 2 supports different data sources (Active Directory, other LDAP directory, SQL databases, etc.) that can be used as an identity repository.

Shibboleth 2 is an implementation of identity provider using the OASIS SAML 2.0 protocol to provide Web single sign-on across or within organizational boundaries.

As previously noticed, the sign-in service of Azure AD supports the SAML 2.0 web browser single sign-in profile, the SAML 2.0 web browser single sign-out profile, as well as and the Enhanced Client or Proxy (ECP) profile.

Note The SAML 2.0 ECP profile is an adaptation of the SAML 2.0 browser single sign-in profile with the parts that were designed around the limitations of a browser removed. In other words, in the SAML 2.0 ECP profile, the user agent is assumed to be something more than a browser (or perhaps a browser with a plugin for example).

Note These profiles supports various possible deployment models. The ones implemented here are the HTTP-Redirect and HTTP-POST bindings specified in the document [Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)[[144]](#footnote-144). For more information, see the Microsoft MSDN articles [Single Sign-on (SAML Protocol)](http://msdn.microsoft.com/en-us/library/windowsazure/dn195589.aspx)[[145]](#footnote-145) and [Single Sign-out (SAML Protocol)](http://msdn.microsoft.com/en-us/library/windowsazure/dn195588.aspx)[[146]](#footnote-146).

Shibboleth 2 supports the two profiles and related deployment model if any.

Beyond the Shibboleth 2 support, it should be noted that generic SAML 2.0 support is not provided today.

Shibboleth 2 provides cross-domain (web) single sign-on (aka federation) with Microsoft and non-Microsoft federation solutions.

The white paper [Azure AD/Office 365 Single Sign-on (SSO) with Shibboleth 2.0](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[147]](#footnote-147) provides information on planning and configuring the single sign-on feature for Azure AD with Shibboleth 2. It has the exact same objectives of the aforementioned white paper on AD FS 2.0 but with the Shibboleth 2 technology.

The information provided is based on our experience in setting up a test Shibboleth 2 implementation, and is not intended to be an exhaustive guide to installing and configuring Shibboleth 2. Shibboleth 2 is a third-party product and therefore Microsoft does not provide support for the deployment, configuration, troubleshooting, best practices, etc. issues and questions regarding Shibboleth 2.

Note For information on the prerequisites as well as on the installation and the configuration of a Shibboleth IdP, we invite you to visit complementarily the documentation made available by the [Shibboleth Community](https://wiki.shibboleth.net/confluence/display/SHIB2/Installation)[[148]](#footnote-148).

# Many applications, one identity repository

## Discovering all cloud applications in use within your organization

Many organizations rely upon Software-as-a-Service (SaaS) applications like Office 365, Box and Salesforce, and many others.

Imagine indeed a business requires a new application to enhance the relationships with customers, and the key points regarding this application are a limited budget and a short time frame to deliver it. This leads the IT considering a public cloud application, which brings interesting capabilities like scale economies, time-to-market and unlimited scalability.

Furthermore, with the ability to subscribe at any time a cloud application to quickly help answering some business imperatives, campaigns, etc., with the freedom of choice, the flexibility, the perceived non-dependency on IT such an open marketplace on the Internet provides to entities within an organization, many more SaaS applications are also potentially in use as IT estimates. This situation leads organizations towards a “Shadow IT” with all the concerns about unauthorized access to corporate data, possible sensible data leakage and other security risks inherent in the SaaS applications in use. Without exactly knowing how many cloud applications or which applications are being used, even getting started building a plan to deal with these risks seems daunting…

The Cloud App Discovery service of Azure AD constitutes a first step to help IT having an accurate visibility into which cloud application are in use within the organization. IT can then take steps to integrate the SaaS applications in use with Azure AD through the Application Access Enhancements for Azure AD (see next section).

This service is available in the new Azure portal at <https://portal.azure.com/>. The portal allows you to add the Cloud App Discovery tile to your Startboard.

Important note This service is only available when you enable the premium edition of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[149]](#footnote-149).

Once added, this service allows your IT to:

* See the applications which were detected, and track application usage over time.
* See the number of users using a particular application, and the identities of those users.
* See the number of agents that are reporting data to the Cloud App Discovery service.
* Sort applications by number of requests, volume of data, or the number of users using the application.
* Control which applications to collect data on.
* Export data to an offline store for custom analysis.

Note For more information, see the blog posts [Azure Cloud App Discovery is now GA](https://appdiscovery.azure.com/)[[150]](#footnote-150) and [Azure Cloud App Discovery GA and our new Privileged Identity Management service](http://blogs.technet.com/b/ad/archive/2015/05/04/azure-cloud-app-discovery-ga-and-our-new-privileged-identity-management-service.aspx)[[151]](#footnote-151), as well as the Microsoft TechNet wiki article [Cloud App Discovery - Frequently Asked Questions](http://social.technet.microsoft.com/wiki/contents/articles/24037.aad-cloud-app-discovery-preview-frequently-asked-questions.aspx)[[152]](#footnote-152).

To achieve the above, and thus in order to discover the cloud applications in use, and thus to collect application usage information, the Cloud App Discovery service uses an agent. This agent can be deployed on all (or some representative) machines in the organization that run Windows 7 and above.

The agent captures HTTP usage information, i.e. URLs, headers and metadata for HTTP/HTTPs accesses originating from the machine on which it runs. This allows the agent to capture requests to all cloud applications accessed over HTTP or HTTPs.

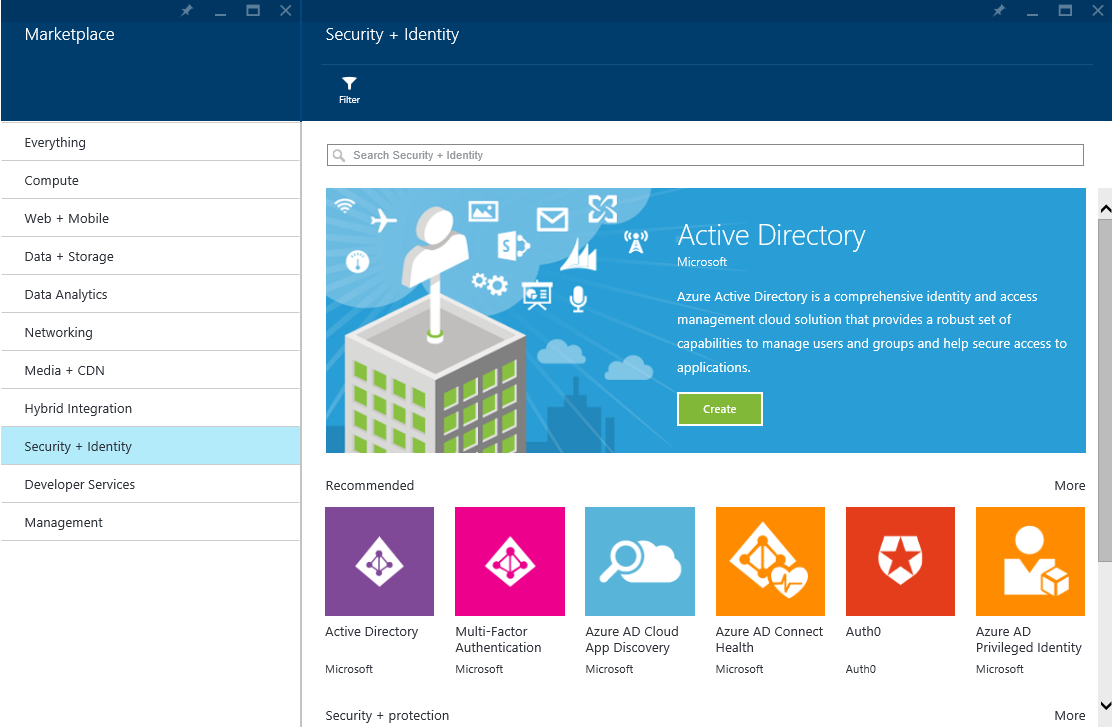
Note Every access to an application’s web site typically includes multiple different requests to the site to retrieve different parts of the web-page. The browser will actually make over dozens of additional web requests for content like pictures, social plugins and other resources. See the snapshot below.

For known cloud applications in the database, the Cloud App Discovery service includes an optimization that only counts webpage loads once so that the Cloud App Discovery Service can ignore counting every access to various elements of the webpage. However, this is an area we’re looking to continue to make improvements on.

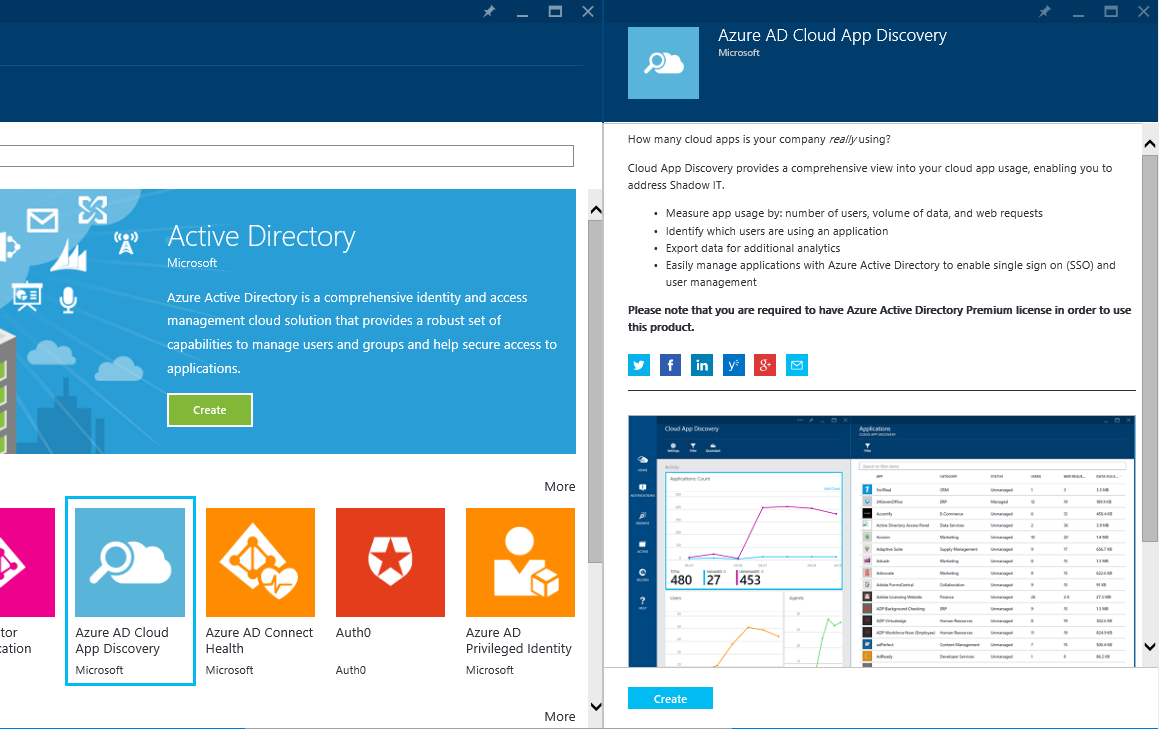
The agent also captures the username of the user on the machine. The agent sends the collected traffic over a secure, encrypted channel to the Cloud App Discovery service. The data in the service is only visible to the administrators of the tenant. Each tenant admin can only see the data for their tenant, and no other tenant’s.

To start using the Cloud App Discovery service and deploying the agent on the windows machines, proceed with the following steps:

1. **Open** a browsing session and navigate to the new Azure Portal at <https://portal.azure.com/>.
2. **Click** **Sign in** and enter the credentials for a global administrator account of your organization that has a trial or paid subscription to Azure AD Premium.
3. Select **Marketplace**, and then select **Security + Identity**, or search for it by typing “*Identity*”.

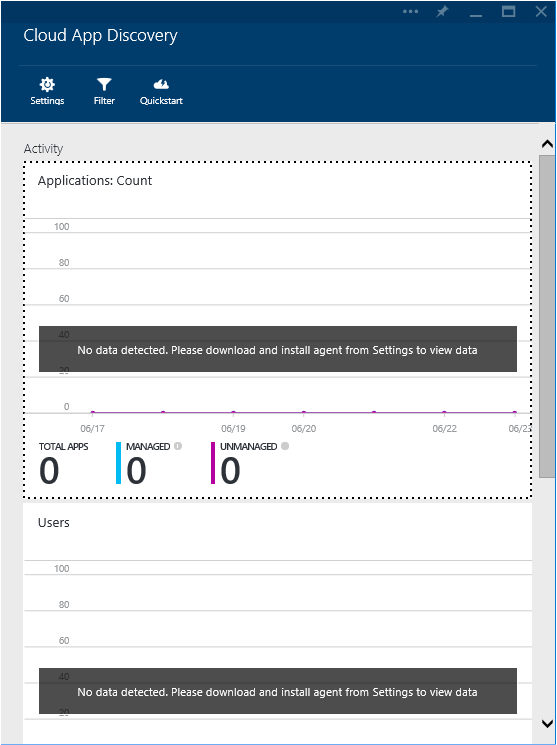


1. Click **Azure AD Cloud App Discovery**. An introductory blade opens up.

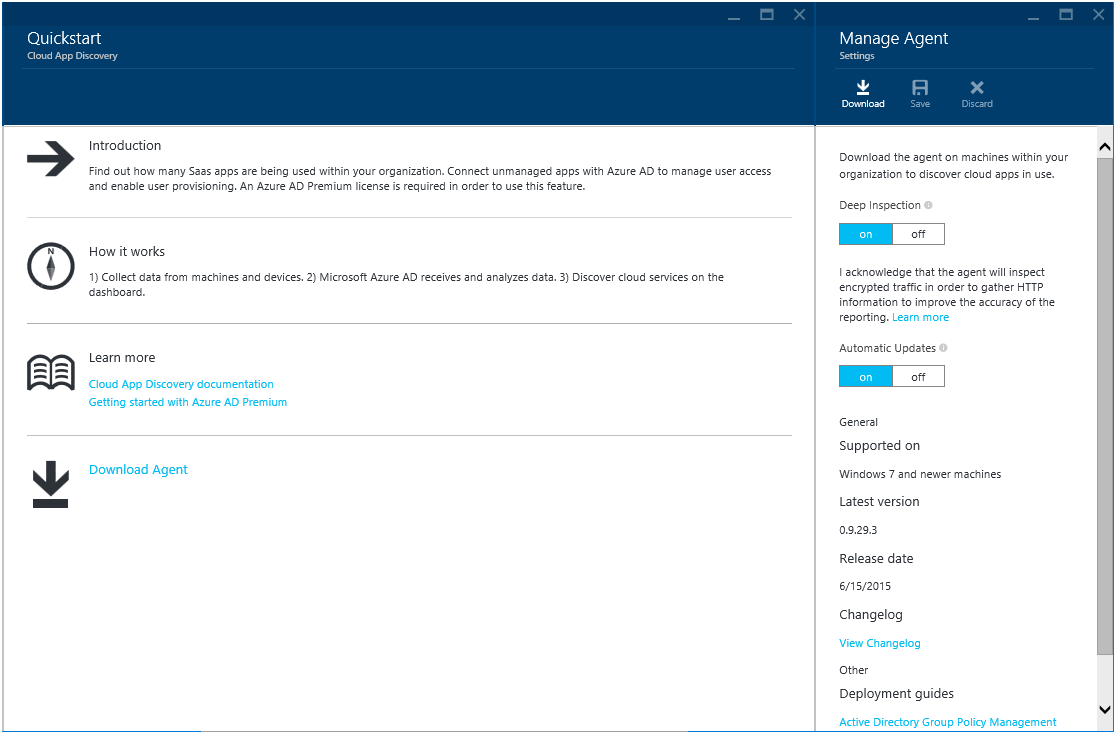


Note A blade is one piece of the overall view. You can think of a blade as a window.

1. Click **Create**. This will open another blade with your Cloud App Discovery information.



1. On the Cloud App Discovery blade, click **Quickstart**., and then the **Download Agent**.



1. **Click** **Download** to download the ZIP file (*Microsoft Cloud App Discovery Endpoint Agent.zip*). The ZIP file contains the setup file (*EndpointAgentSetup.exe* file) that should be installed on the targeted machine for cloud applications discovery, and a certificate used to authenticate to your Azure AD tenant in the cloud.
2. After installing the agent on a machine where the user has been accessing applications, data typically shows up within 10 minutes in the Cloud App Discovery dashboard.

Note For a complete step-by-step walkthrough of the management experience in the new Azure portal, and the installation of the agent, see the Microsoft MSDN article [Cloud App Discovery](https://msdn.microsoft.com/en-us/library/azure/mt143581.aspx)[[153]](#footnote-153).

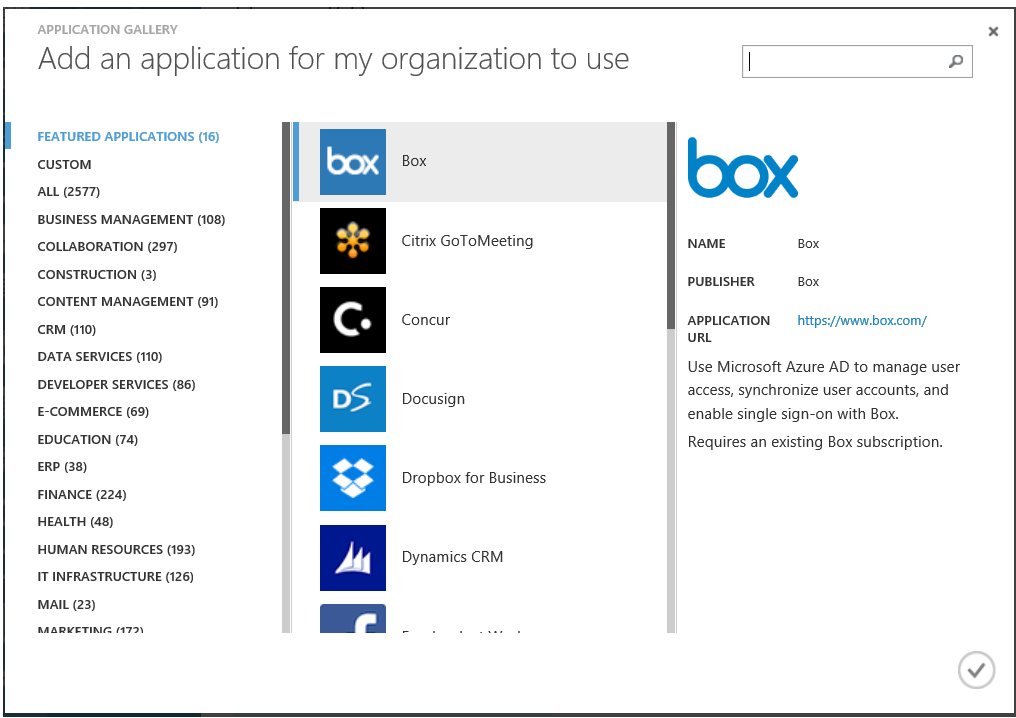
The Cloud App Discovery service can be further configure to route the data collected to an Azure Blob storage in order to perform analytics on the data in tools like Excel and [Power BI](http://www.microsoft.com/en-us/powerbi/default.aspx)[[154]](#footnote-154).

Note For a complete walkthrough for the dashboard, see the blog post [Cloud App Discovery: Now with Excel and Power BI Support](http://blogs.technet.com/b/ad/archive/2014/10/01/more-news-on-cloud-app-discovery.aspx)[[155]](#footnote-155).

## Leveraging pre-integrated popular SaaS applications

The Application Access Enhancements for Azure AD simplifies managing access to thousands of pre-integrated cloud SaaS applications (and more in the coming months) and introduces security and access governance controls that enable IT to centrally manage users' access across them.

As part of these free enhancements for Azure AD, the [Azure AD application gallery](http://azure.microsoft.com/en-us/marketplace/active-directory/all/)[[156]](#footnote-156) provides a wide variety of popular pre-integrated SaaS applications that your users can single sign-on to from Azure AD today. This includes Microsoft's cloud apps and services like Office 365, and Dynamics CRM Online and third party applications like Salesforce and Box that you may already be using and want to connect to Azure AD.



Several types of applications[[157]](#footnote-157) appear in the application gallery, covering the whole spectrum in terms of application integration capabilities:

* **Microsoft applications**. Microsoft applications like Office 365 and Dynamics CRM Online are present in the application gallery. There is no configuration required to connect Office 365 applications. For example, all you need to do is follow the sign up link in the application gallery to sign up using your Azure AD account, and the Office365 does the rest.
* **Third-party applications that support federated single sign-on and automated user account provisioning**. Many of the larger and more advanced cloud services support federation and expose API's we can use for user provisioning. This includes **featured applications** like Salesforce, Box, and Google Apps. You can configure Azure AD to push user accounts to these application. Once this application is selected and added, you will be guided through a simple process to connect Azure AD to your applications for provisioning and single sign-on.

Microsoft is working with key partners in the ecosystem to establish these connections, meaning you no longer have to continually update user records in multiple systems.

* **Third-party applications that support federated single sign-on**. These applications support federation so that users do not need to have another password but do not have exposed API's for user provisioning. Once this kind application is added, the service walks you through a guided tour with step by step instructions on how to configure each specific application to work with Azure AD.
* **Third-party applications that support password-based single sign-on**. Azure AD includes password vaulting capabilities and we use these plus a browser helper object to provide a single sign-on experience for cloud services that only support signing in with a username and password. This means that even for this relatively unsophisticated services, we can automate the users sign in process, using credentials that can either be provided by an administrator or by the user upon first-time use.

The application gallery indicates which of these features are supported in the application description, as well as provide a link to learn more about the application including any prerequisites.

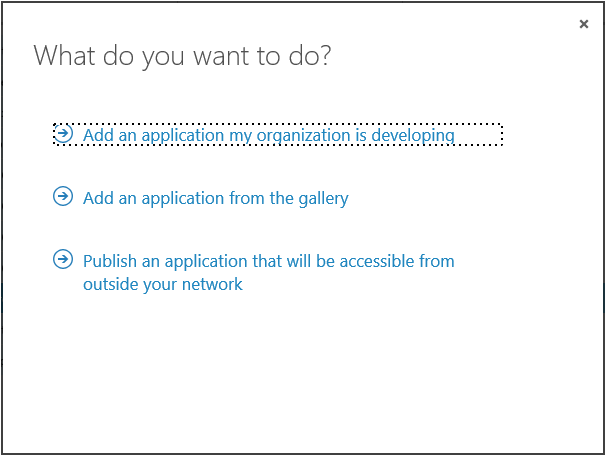
As mentioned before, the Application Access Enhancements for Azure AD enable to add [thousands](http://azure.microsoft.com/en-us/marketplace/active-directory/)[[158]](#footnote-158) of cloud pre-integrated SaaS applications like ADP, Concur, Google Apps, Salesforce.com and others, regardless of the public cloud they are hosted on. The pre-integrated SaaS applications are preconfigured via an application gallery with all the parameters needed to at least provide a seamless sign-in experience with them.  Let’s see how to add such a SaaS application.

### Adding a SaaS application from the gallery

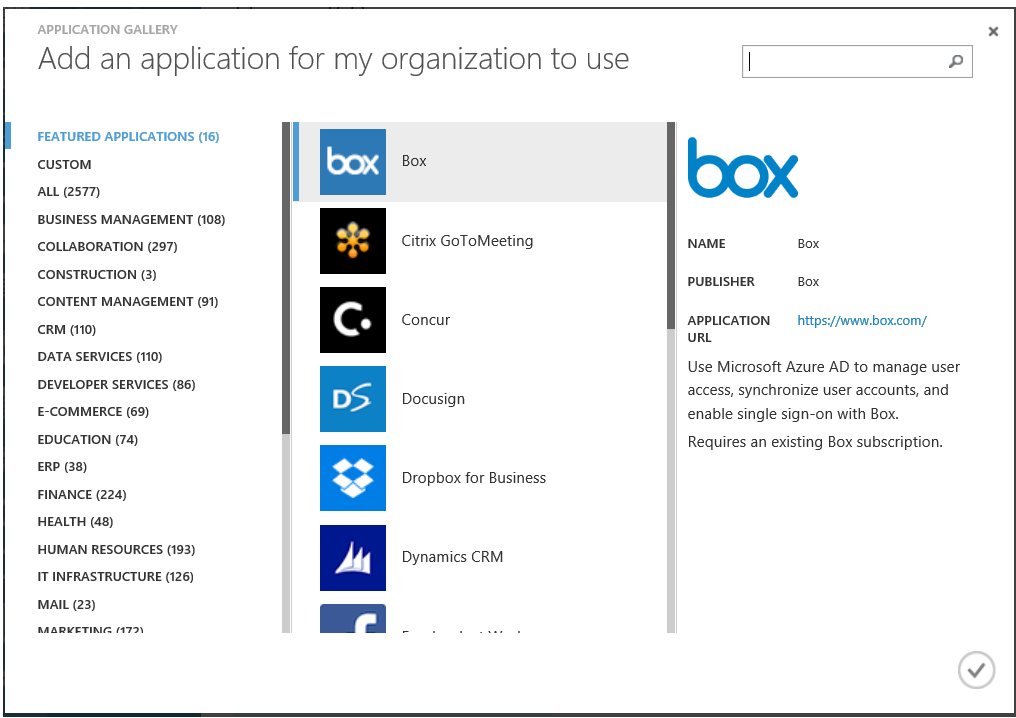
With a few simple steps, you can select from the list of applications that are pre-integrated in the application gallery.

To add an application from the application gallery, proceed with the following steps:

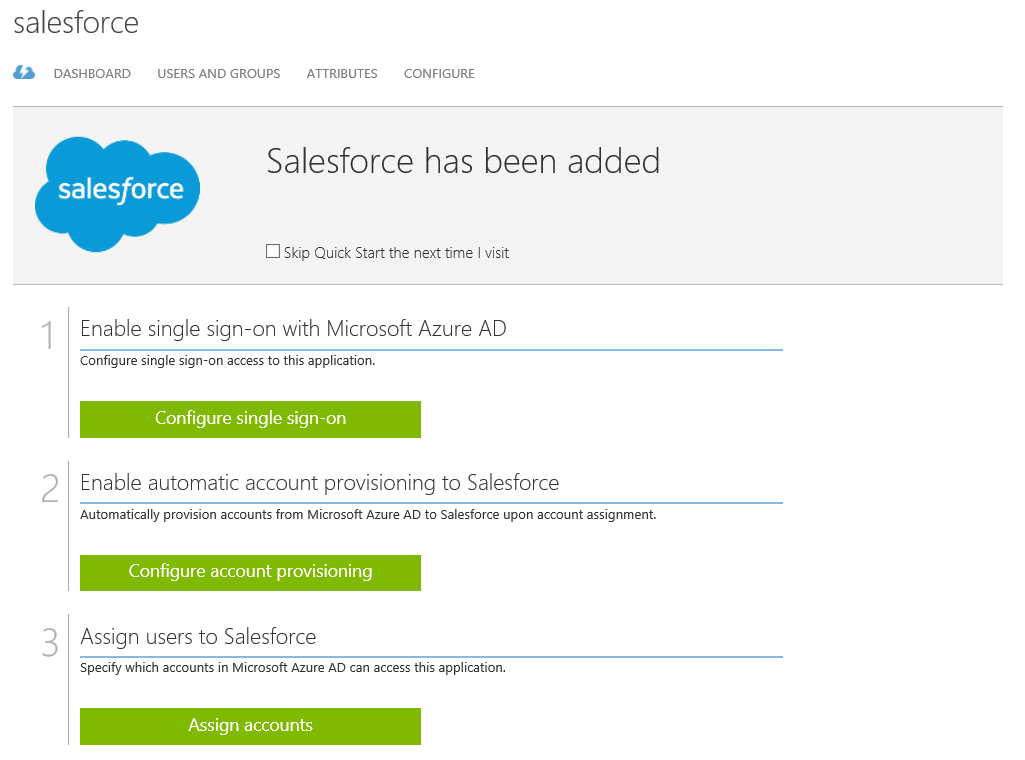
1. Sign into the classic Azure management portal as the administrator of the directory to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which you want to add a pre-integrated SaaS application.
3. Click **APPLICATIONS** in the **active directory**.
4. Click **ADD** in the tray of the bottom. A **What do you want to do?** dialog brings up.



1. Click **Add an application for my organization to use**.
2. Select in the application gallery the SaaS application of your choice to integrate with, for example in this illustration the application Salesforce under the category **FEATURED APPLICATIONS**.



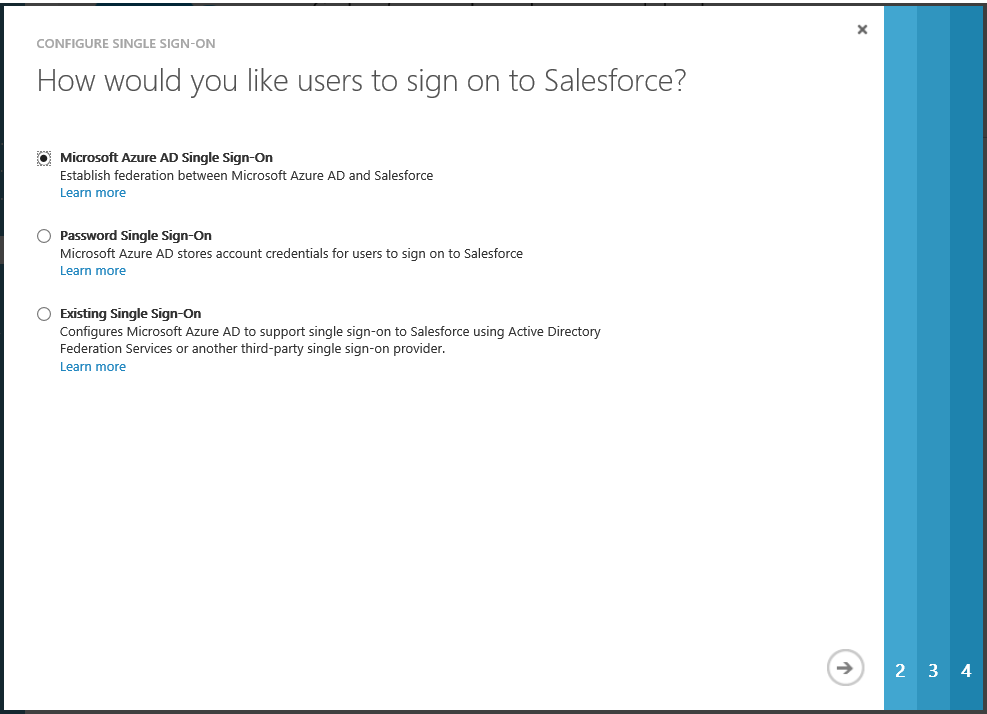
1. Validate the addition by clicking the check mark icon on the bottom right.



1. Once the application is added to your directory, you can then quickly configure it for use.

As aforementioned, **the related steps depend on the application capabilities and more especially whether it uses federation or password vaulting, and whether it supports automatic provisioning of users or not**.

In this illustration, **Configure single sign-on** enables you to specify how you would like users to sign on to that app. The next steps depend on the selected options.



As illustrated here, and in accordance to the previously discussed integration options, Azure AD supports three different modes for single sign-on:

1. **Microsoft Azure AD Single Sign-On**. This enables users to be automatically signed in to the application by Azure AD **using the user account information from Azure AD**.
2. **Password Single Sign-On**. This enables users to be automatically signed in to the application by Azure AD **using the user account information from the application**. By using a custom browser plugin or a custom browser app on iOS and Android, we automate the user's sign in process via securely retrieving application credentials from the directory
3. **Existing Single Sign-On**. This allows you to add links to the application independently of the single-sign on method. For example, if the application is configured to authenticate users using AD FS or another solution on-premises, when users will access that link, they will be authenticated using AD FS, or whatever existing single sign-on solution is provided by the application.

Note For additional information regarding Salesforce, you can watch the Channel 9 demo video [Integrating Salesforce with Azure AD: How to enable Single Sign-On (1/2)](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Integrating-Salesforce-with-Azure-AD-How-to-enable-Single-Sign-On-12)[[159]](#footnote-159).

If supported by the application, **Configure account provisioning** allows you to configure the automatic user provisioning with the application from your Azure AD tenant.



Note For additional information, you can watch the Channel 9 demo video [Integrating Salesforce with Azure AD: How to automate User Provisioning (2/2)](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Integrating-Salesforce-with-Azure-AD-How-to-automate-User-Provisioning-22)[[160]](#footnote-160).

Note For more information, see the Microsoft MSDN article [Application access capabilities for Azure Active Directory](https://msdn.microsoft.com/library/azure/dn308588.aspx)[[161]](#footnote-161).

[**Detailed integration tutorials**](https://msdn.microsoft.com/en-us/library/azure/dn893637.aspx)**[[162]](#footnote-162) are available to show you how to configure Azure Active Directory single sign-on for third party SaaS applications.** The tutorialsfor Salesforce[[163]](#footnote-163), Salesforce Sandbox[[164]](#footnote-164), Box[[165]](#footnote-165), Google Apps[[166]](#footnote-166), and Citrix GoToMeeting[[167]](#footnote-167), Concur[[168]](#footnote-168), Workday[[169]](#footnote-169), Jive[[170]](#footnote-170), DocuSign[[171]](#footnote-171), Servicenow[[172]](#footnote-172), and Dropbox for Business[[173]](#footnote-173) are simply a few of the more than hundred of tutorials available.

For those of you who are using Office 365, you will find that the Office 365 application access is automatically supported within the Azure management portal and no additional configuration is required.

Note For more information, see Microsoft TechNet article [Best Practices for Managing the Application access enhancements for Azure Active Directory](http://social.technet.microsoft.com/wiki/contents/articles/18409.best-practices-for-managing-the-application-access-enhancements-for-windows-azure-active-directory.aspx)[[174]](#footnote-174).

Once your application has been configured to use Azure AD, then it is almost ready to use. As a security control, Azure AD will not allow users to have an access into the application unless they have been granted access. Users may be granted access directly, or through a group that they are a member of. You can follow the directions outlined in section § Managing access to applications to quickly assign it to your employees.

For the moment, let’s consider some additional features regarding your ability to further configure the SaaS application.

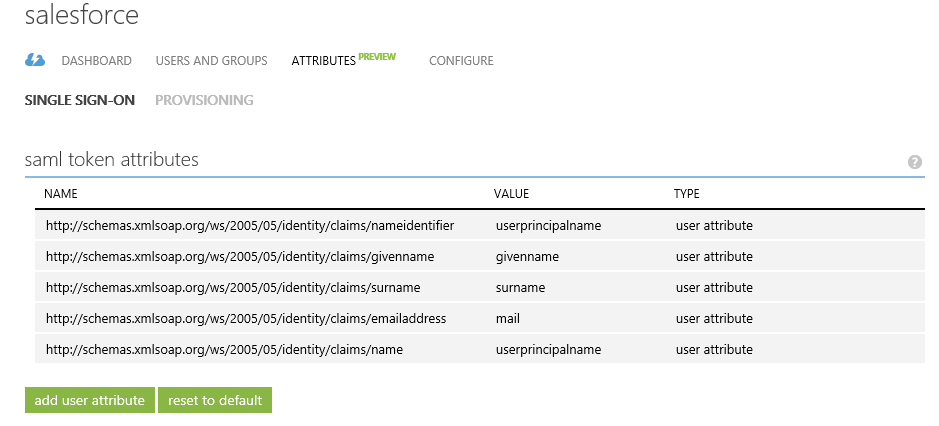
### Defining SAML token attributes

The SAML token attributes for SaaS application feature, also known as claims transformation language, allows you to manipulate existing claim assignments or add additional claim assignments for SAML 2.0 based authentication for a SaaS application in Azure AD.

Using SAML token attributes, you can:

* Select from a list of attributes defined in Azure AD.
* Add a claim with a constant value.
* Use built-in functions to form custom claims.
* Restore default claims for an application.

SAML token attributes is available on pre-integrated SaaS applications listed in the application gallery, and that support federated single sign-on.

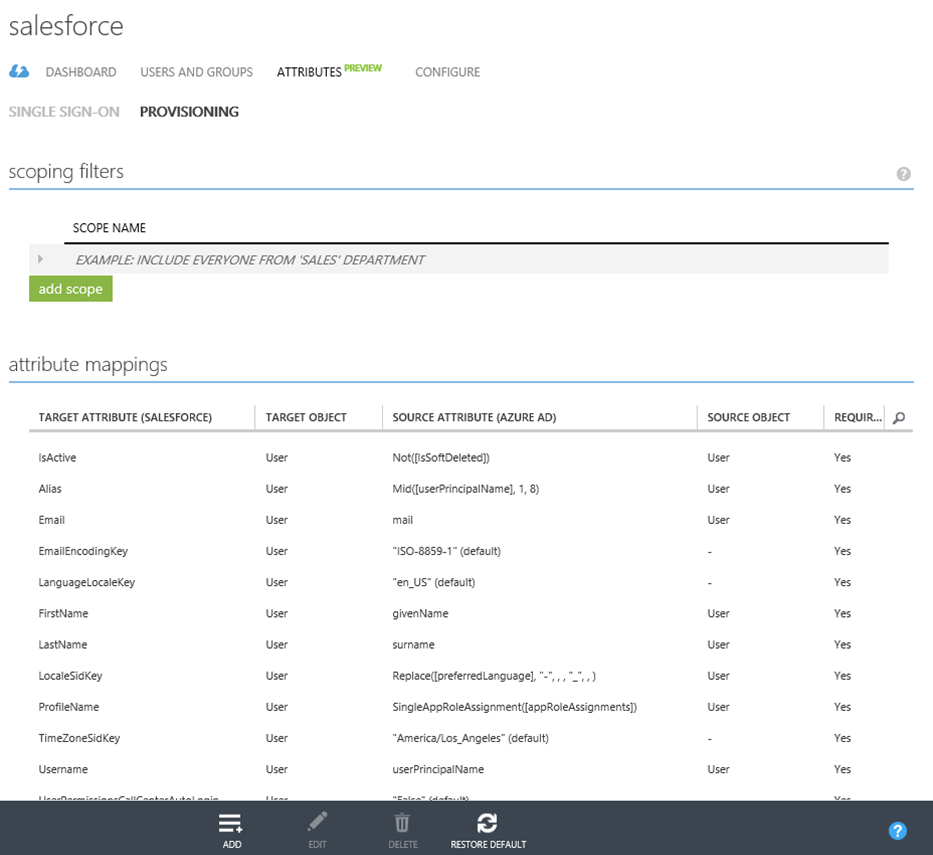


### Customizing attribute mappings

When using Azure AD to provide user provisioning to third-party SaaS applications, the classic Azure Management Portal controls the attribute values in form of a configuration called “attribute mapping”.

There is a preconfigured set of attribute mappings between Azure AD user objects and each SaaS application’s user objects, however, you can customize the default attribute mappings according to your business needs. This means that you can change or delete existing attribute mappings or create new attribute mappings. In other words, this feature (in public preview as of this writing) gives you the ability to customize which set of attributes from Azure AD will get synced into the considered SaaS application you are using Azure AD to manage.

Note For additional information, see the blog post [Azure AD Custom Attribute Mapping for SaaS App User Provisioning](http://blogs.technet.com/b/ad/archive/2015/01/07/azure-ad-custom-attribute-mapping-for-saas-app-user-provisioning.aspx)[[175]](#footnote-175) and the Microsoft MDSN articles [Customizing Attribute Mappings](https://msdn.microsoft.com/en-us/library/azure/dn872469.aspx)[[176]](#footnote-176) and [Writing Expressions for Attribute Mappings in Azure Active Directory](https://msdn.microsoft.com/en-us/library/azure/dn891618.aspx)[[177]](#footnote-177).



You will probably notice that some mappings are labeled as "calculated," which means that we are taking the information of one or more source attributes and then modifying them into the desired format for the target attribute. You will be able to edit and define your own calculated mappings in a future update.

The other type of mapping is labeled as "default." Rather than mapping an attribute from Azure AD, default mappings instead fill the target attribute with a constant value. You will also be able to edit default mappings in future releases of this feature.

## "Bringing Your Own Application" (BYOA)

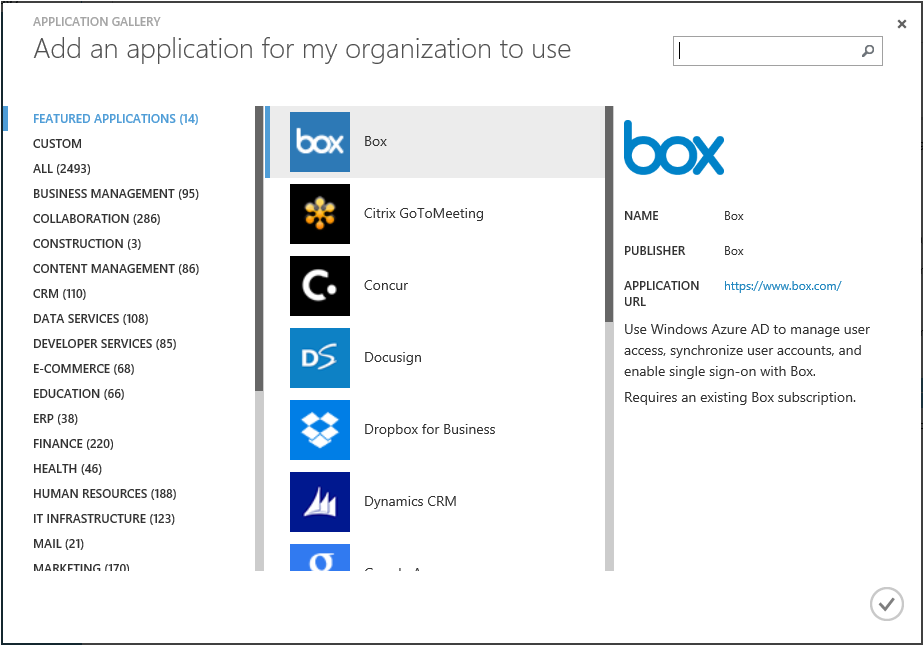
Besides the ability to easily configure pre-integrated SaaS applications from the app gallery, you may desire the ability to onboard any applications you need in a self-service fashion. This can include custom applications that your organization has developed, third-party web applications that your organization has deployed to servers you control, or SaaS applications that you use but have not yet been on-boarded to the application gallery.

Since the end of last year, you are provided with such an ability to configure any custom application.

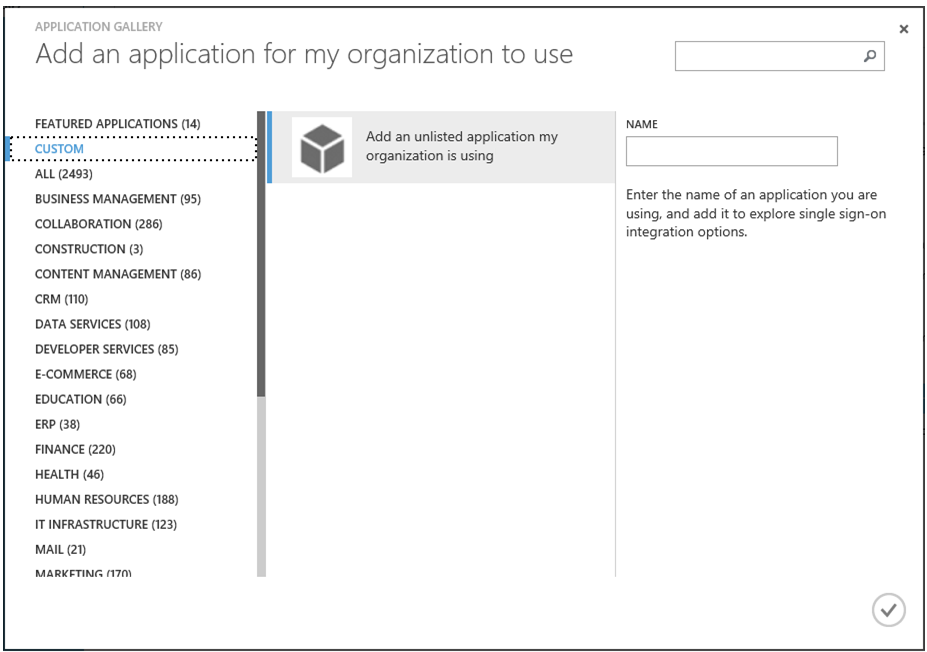
Note For more information, see the blog post [Wrapping up the year with a boat load of Azure AD news!](http://blogs.technet.com/b/ad/archive/2014/12/11/wrapping-up-the-year-with-a-boat-load-of-azure-ad-news.aspx)[[178]](#footnote-178).

To integrate a custom application, proceed with the following steps.

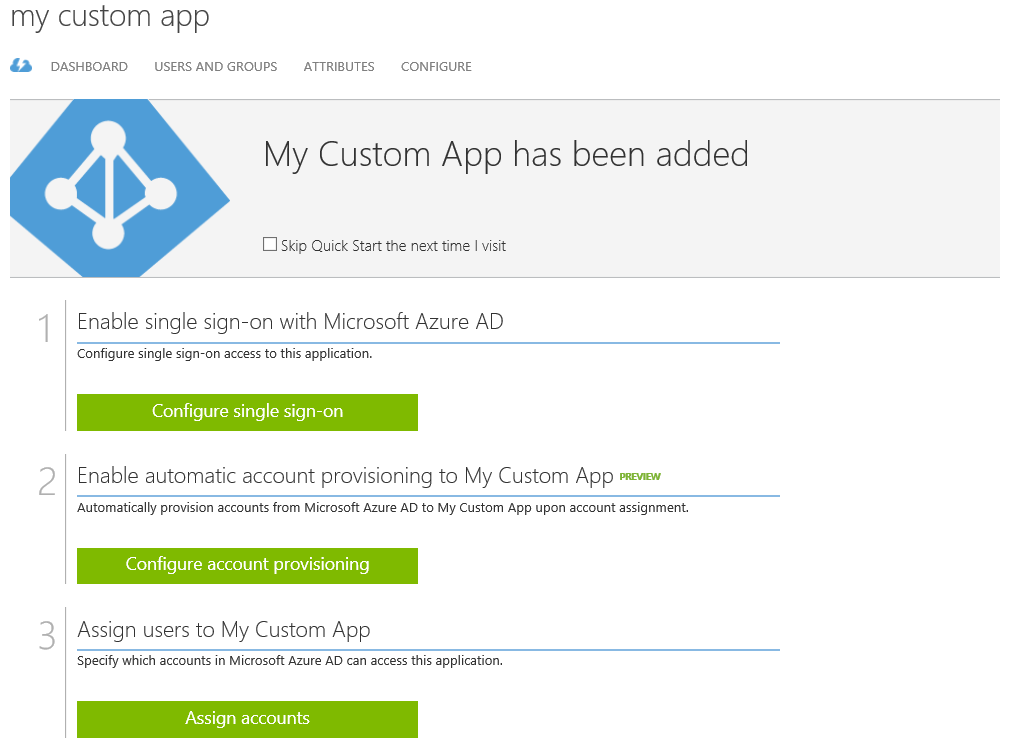
1. Inside of the Azure management portal, and as already illustrated, click **APPLICATIONS** in the organization’s directory for which you want to add a custom application.
2. Click **ADD** at the bottom of the tray.



1. Click **CUSTOM**.



1. Type a name for the custom application to add, for example “*My Custom App*”, and then click the check mark icon on the bottom right. The following resulting screen is displayed.



As you can see, adding a custom application provides a very similar experience to the one available for pre-integrated SaaS applications.

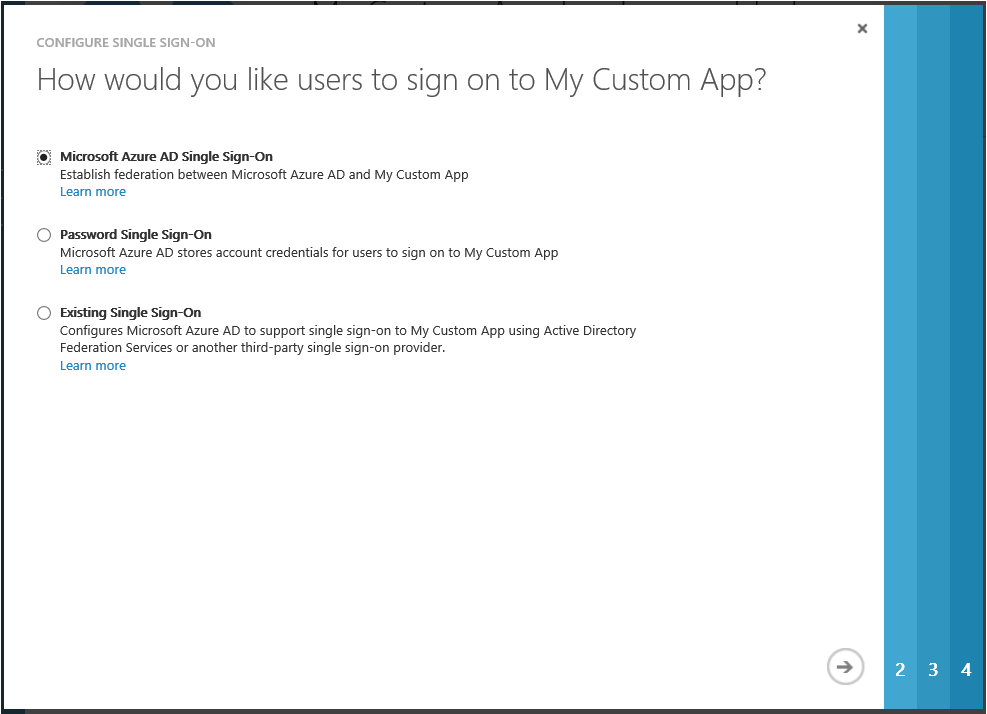
Let’s see how to configure single sign-on.

### Configuring single sign-on

Configuring single sign-on for a custom application also provides a very similar experience to the one available for pre-integrated SaaS applications.

To start, proceed with the following steps.

1. On the resulting screen, select **Configure single sign-on**.



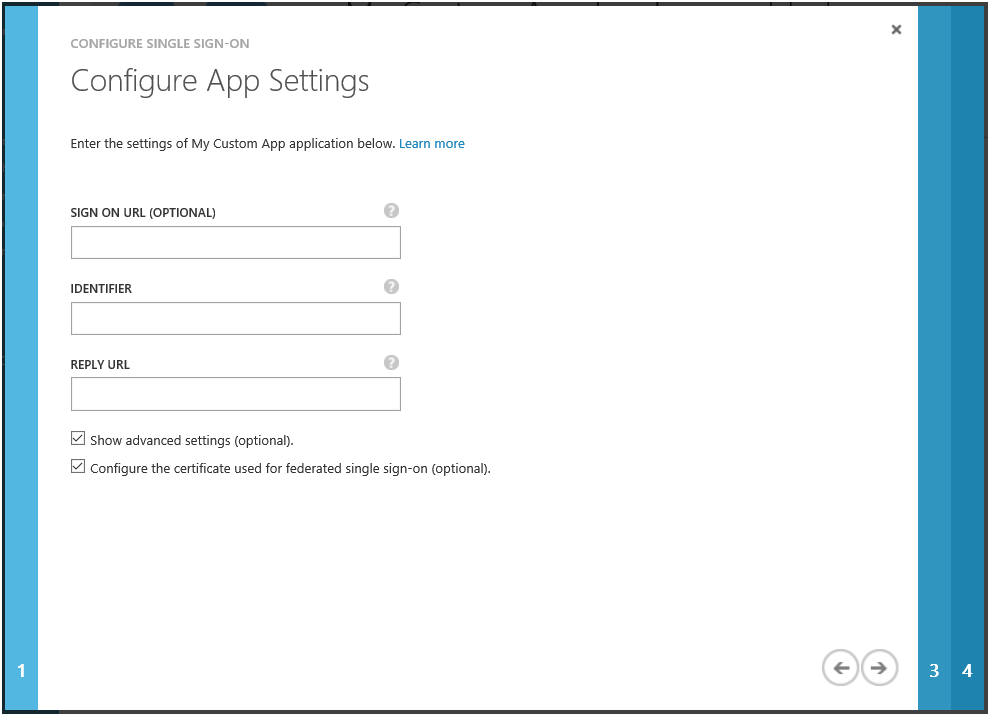
1. You are provided with the same three different modes for single sign-on you’ve already seen for adding a SaaS application:
2. **Microsoft Azure AD Single Sign-On**. This allows you to configure SAML 2.0 service provider-initiated sign-in with Azure AD for any application that supports it.

Note For additional information, see the blog post [“Bring your own app” with Azure AD Self-Service SAML configuration -> now in preview](http://blogs.technet.com/b/ad/archive/2015/06/17/bring-your-own-app-with-azure-ad-self-service-saml-configuration-gt-now-in-preview.aspx)[[179]](#footnote-179).

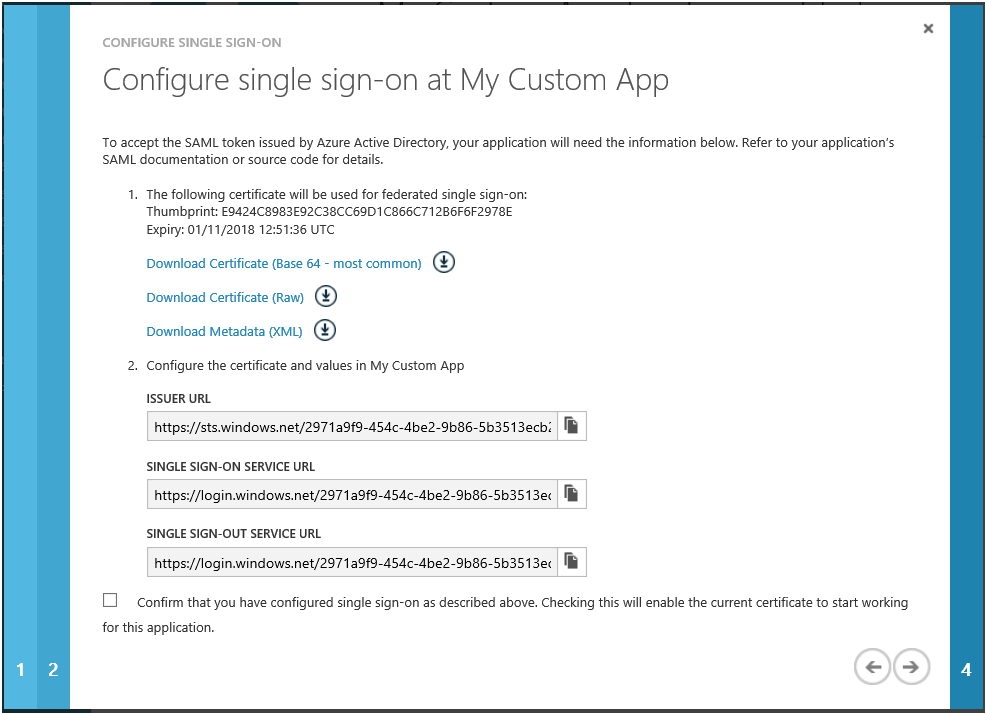
1. **Password Single Sign-On**. This allows you to configure password-based single sign-on for any application that has an HTML sign-in page.
2. **Existing Single Sign-On**. This allows you to add links to any application independently of single-sign on method. For example, if the application is configured to authenticate users using AD FS or another solution on-premises, when users will access that link, they will be authenticated using AD FS, or whatever existing single sign-on solution is provided by the application.

By using either of these options, you can also to enable other benefits of Azure Active Directory such as multi-factor authentication, and security and audit reporting (see later in this document).

To illustrate the process, let’s configure for example a SAML-based authentication. Select **Microsoft Azure AD Single Sign-On**, and then click the arrow icon at the bottom right. You will be prompted to enter three different URLs for the application.



1. Specify the application settings in terms of URLs. The tooltip icons in the dialog provide details about what each URL is and how it is used. After these have been entered, click the arrow icon at the bottom right.



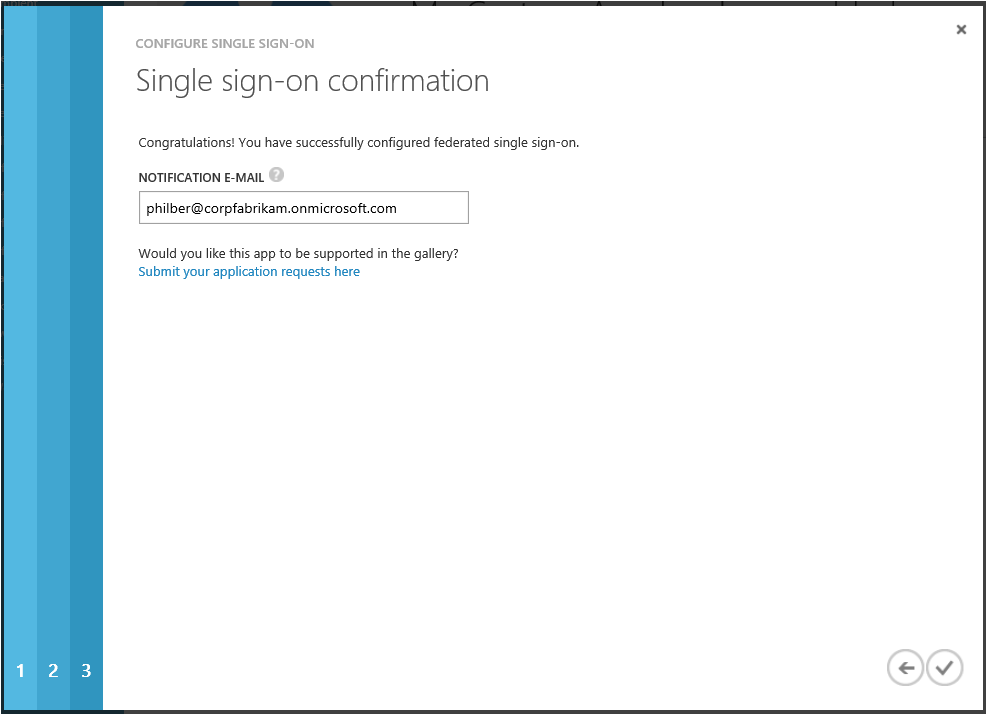
1. The above screen provides information about what needs to be configured on the application side to enable it to accept a SAML token from Azure AD.

Note Which values are required will vary depending on your custom application. The sign-on and sign-out service URL both resolve to the same endpoint, which is the SAML 2.0 request-handling endpoint for your Azure AD tenant. For more information, see the white paper [Leverage Azure AD for modern business applications](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[180]](#footnote-180). The Issuer URL is the value that appears as the "Issuer" inside the SAML token issued to the application.

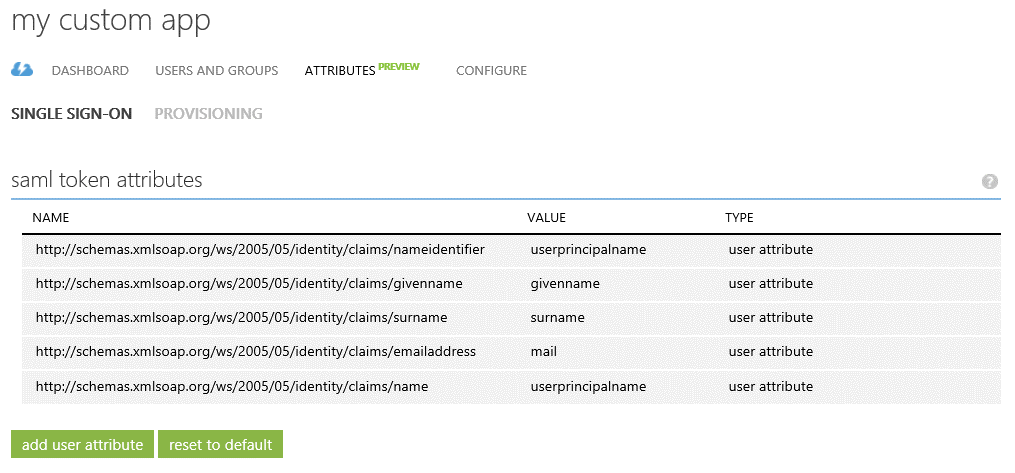
Click **Download certificate**.



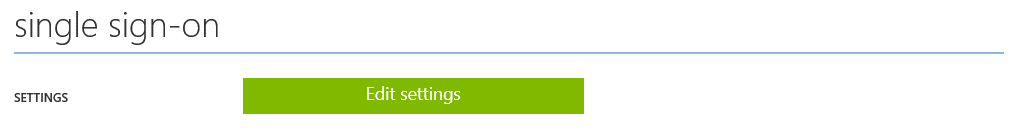
1. Configure your custom application to reflect the above information, and click the arrow icon at the bottom right.



1. Click the check mark icon to finalize the single sign-on configuration for the custom application.
2. Back to the resulting screen, click **ATTRIBUTES**. The SAML token attributes available on pre-integrated federated SaaS applications listed in the application gallery is also available here for your custom SAML 2.0 based application.



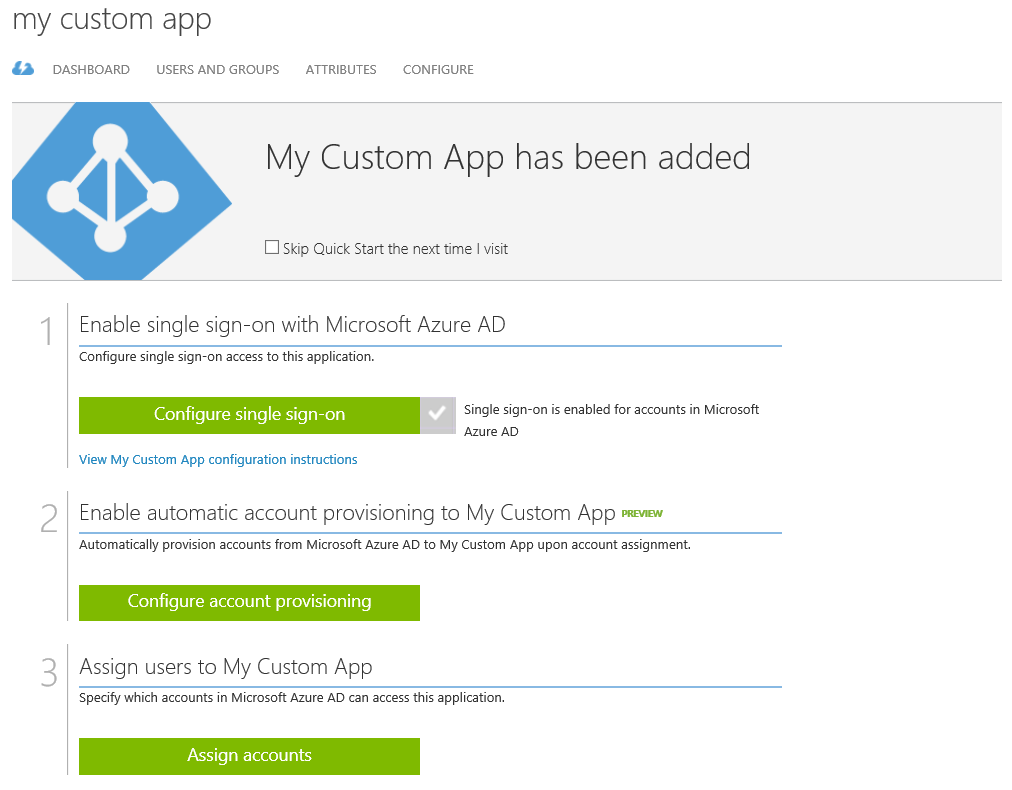
1. Click **CONFIGURE**.



1. Under **single sign-on**, click **Edit settings** to later update your configuration if needed.

### Configuring automatic provisioning

In addition to the above single sign-on capability, the Premium edition of Azure AD provides an automatic account provisioning capability in preview (see second option hereafter).



This capability is based on the support of the [Cross-domain Identity Management (SCIM) 2.0](http://www.simplecloud.info/)[[181]](#footnote-181) standard, i.e. an open API for managing identities and provisioning workloads.

Note For more information, see the blog posts [Azure AD Premium now supports SCIM 2.0!](http://blogs.technet.com/b/ad/archive/2015/11/17/azure-ad-premium-now-supports-scim-2-0.aspx)[[182]](#footnote-182) and [Azure AD: Helping you adding SCIM support to your applications](http://blogs.technet.com/b/ad/archive/2015/11/23/azure-ad-helping-you-adding-scim-support-to-your-applications.aspx)[[183]](#footnote-183).

It can be used in conjunction with the so-called "Bringing Your Own Application" (BYOA) capability discussed in this section to enable not only single sign-on (as per previous section) but also automatic user provisioning for a custom application. For that purpose, the considered custom application must provide or be fronted by a SCIM-based façade/web service. In other words:

* The custom application can support SCIM right out-of-the-box. If such an application us capable of accepting an access token from Azure AD, it will work with Azure AD of the box.

- or -

* A SCIM-based façade can be built to translate between Azure AD’s SCIM endpoint and whatever API, interface, or mechanism the custom application supports for user provisioning.

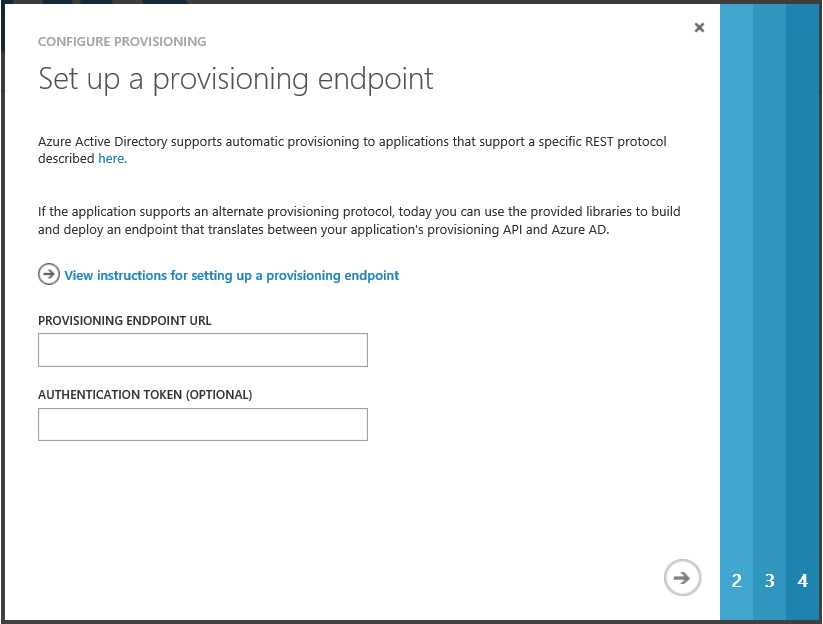
Note To ease the development, Common Language Infrastructure (CLI) libraries are provided as a [NuGet package](https://www.nuget.org/packages/Microsoft.SystemForCrossDomainIdentityManagement/)[[184]](#footnote-184) (Microsoft.SystemForCrossDomainIdentityManagement) to build a SCIM endpoint and translate SCIM messages.

In addition, a series of sample code packages to implement a SCIM-based provisioning façade and demonstrate the automatic provisioning capability is available on [GitHub](https://github.com/Azure/AzureAD-BYOA-Provisioning-Samples/tree/master)[[185]](#footnote-185). Theses sample code packages illustrate how to use the CLI libraries with "Bringing Your Own Application" (BYOA) for the provisioning scenarios outlined here.

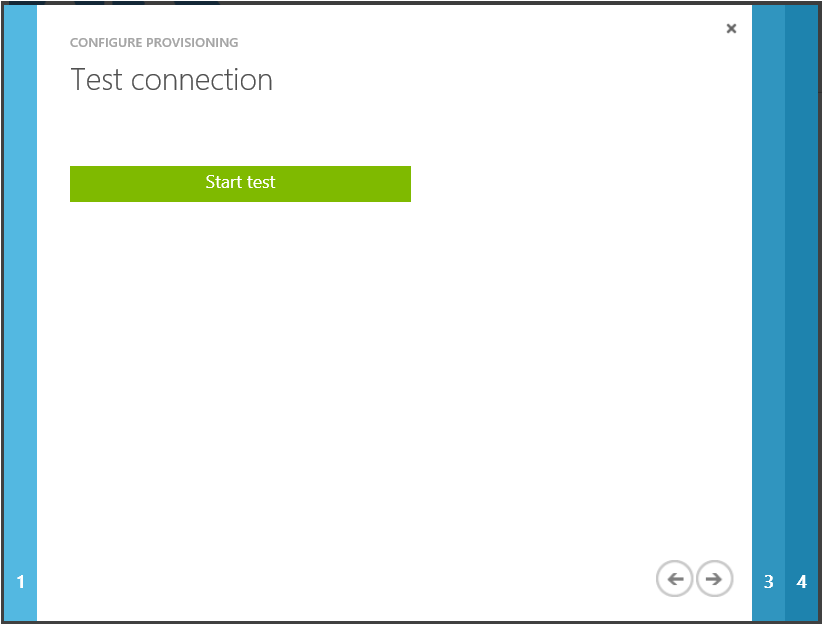
Once configured, Azure AD will send requests to create, modify and delete assigned users and groups to the configured SCIM-based provisioning endpoint, which can then honor those requests, and translate them into operations upon the identity store used by the custom application.

To illustrate the configuration process from an Azure AD perspective, proceed with the following steps:

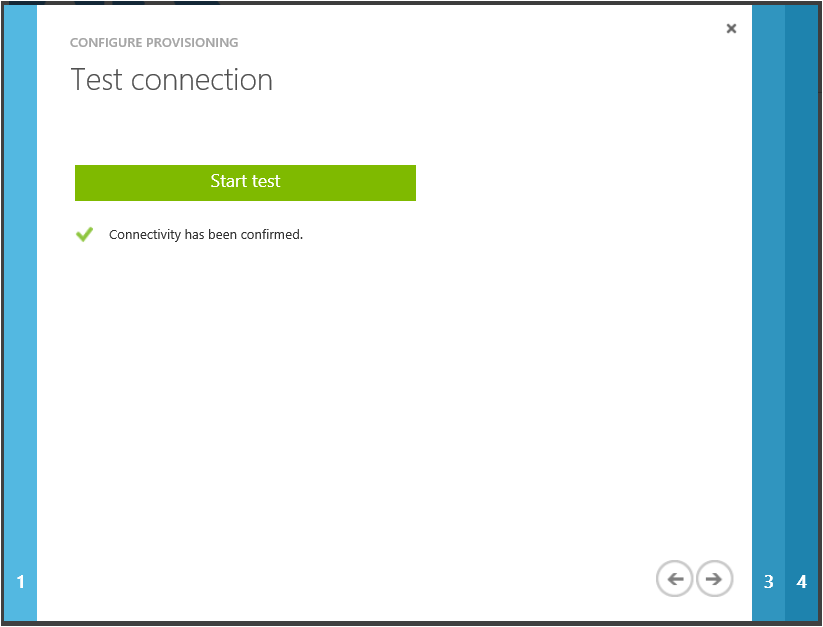
1. Click **Configure account provisioning** on the resulting screen. You will be prompted to enter the SCIM-based provisioning endpoint URL for the custom application.



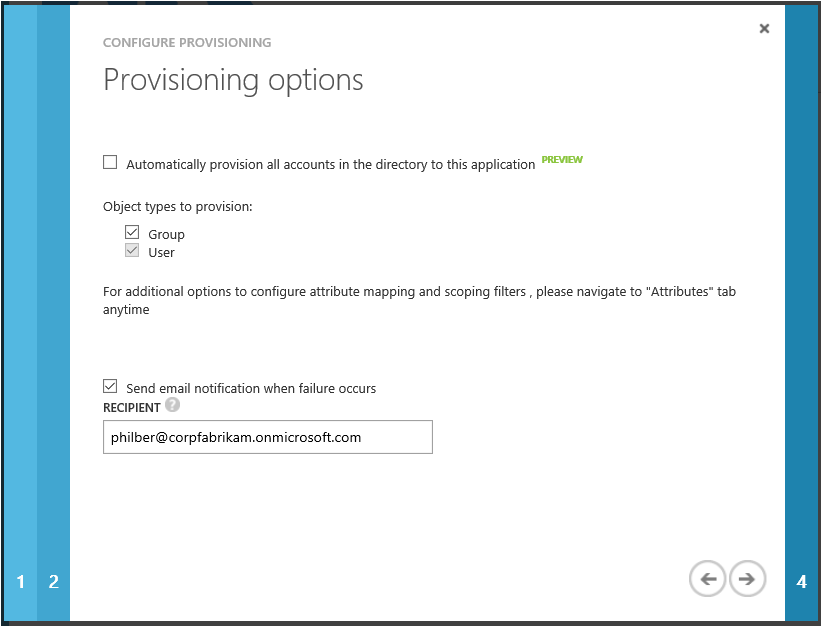
1. Once specified, click the arrow icon at the bottom right.



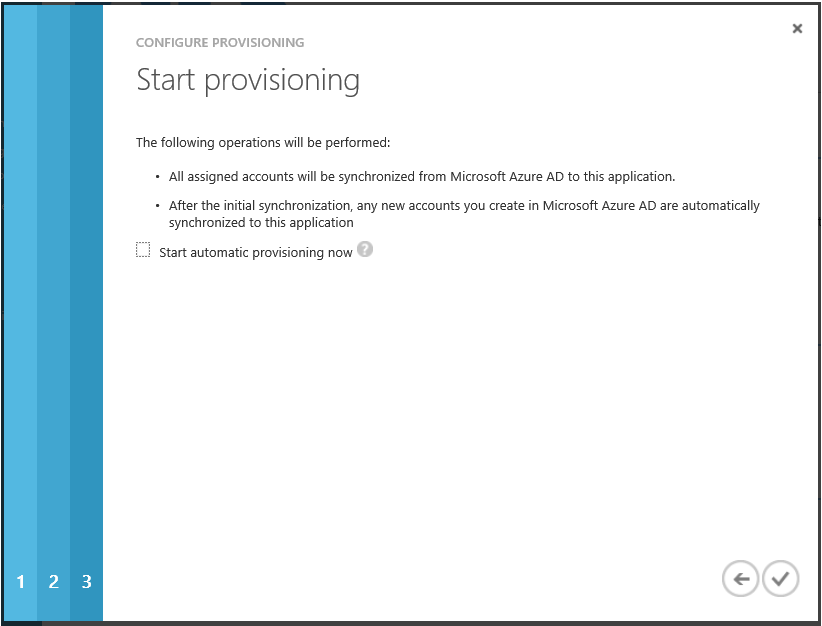
1. Click **Start test** to have Azure AD attempt to connect to the SCIM-based provisioning endpoint.



1. If the attempts to connect to the application succeed, and then click the arrow icon at the bottom right. Otherwise, use the displayed diagnostic information to fix the configuration.

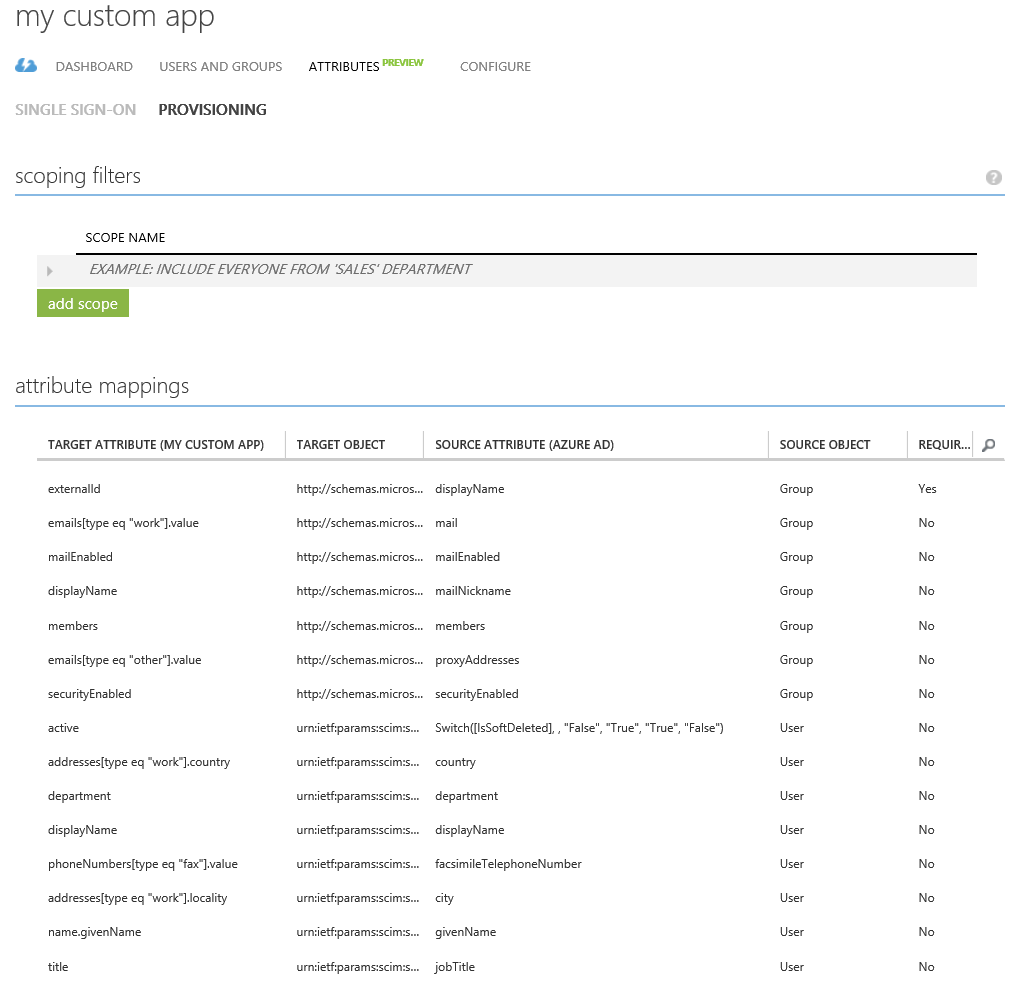


1. Click **Automatically provision all accounts in the directory to this application**, and then specify your provisioning options, and then click the arrow icon at the bottom right.

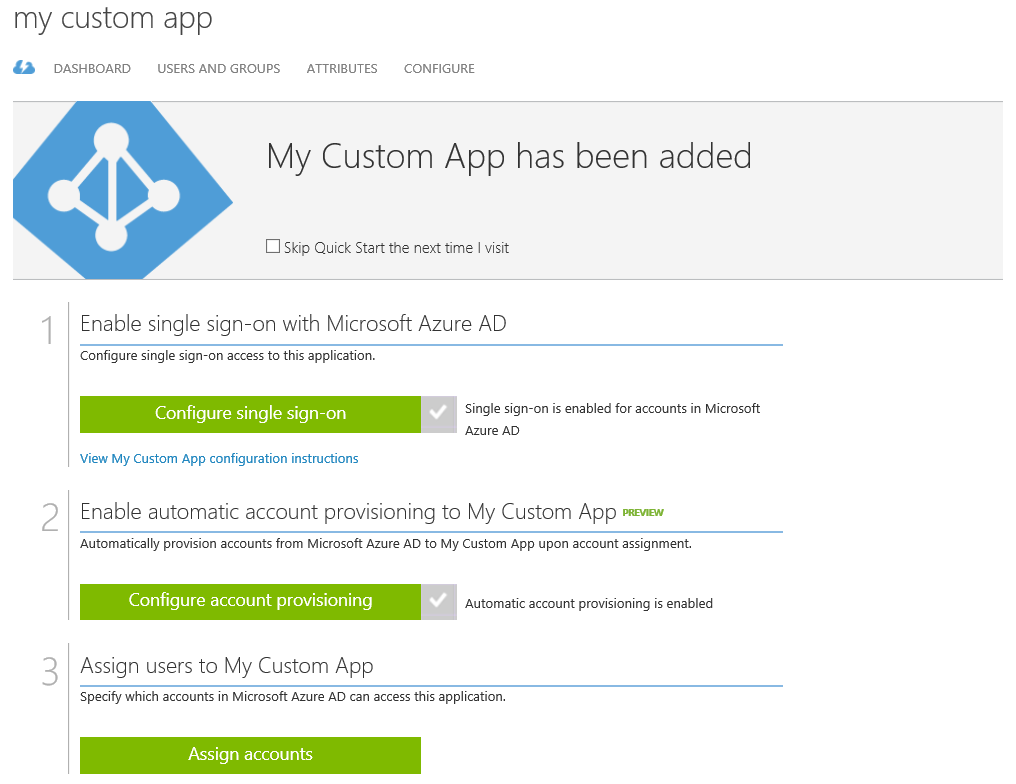


1. Optionally check **Start automatic provisioning now**, and then click the check mark to confirm that the configuration is done.
2. Back to the resulting screen, click **ATTRIBUTES**, and then **PROVISIONING** next to **SINGLE SIGN-ON**. Like with third-party SaaS applications, the classic Azure Management Portal controls the attribute values in form of a configuration called “attribute mapping”.

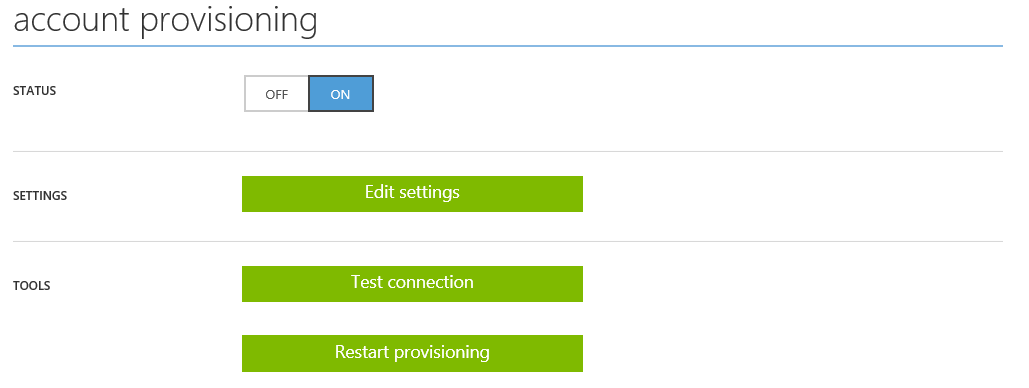
There is a preconfigured set of attribute mappings between Azure AD user objects and each custom application’s user objects, however, you can customize the default attribute mappings according to your business needs.



As noticed before for pre-integrated SaaS applications, Azure AD will not allow users to have an access into the custom application unless they have been granted access. Users may be granted access directly, or through a group that they are a member of.



1. In the resulting screen, click **Assign Accounts**. You can then follow the directions outlined in section § Managing access to applications to quickly assign it to your employees.
2. Once users and/or groups are assigned to the custom application, click **CONFIGURE**.



1. Under **account provisioning**, confirm that **STATUS** is set to **ON**.
2. Under **TOOLS**, click **Restart provisioning** to kick-start the provisioning process.

Note Around ten minutes may elapse before the provisioning process will begin to send requests to the specified SCIM-based provisioning endpoint URL for the custom application. A summary of connection attempts is provided in DASHBOARD, and both a report of provisioning activity and any provisioning errors can be downloaded from REPORTS.

Note For more information, see the article [Using SCIM to enable automatic provisioning of users and groups from Azure Active Directory to applications](https://azure.microsoft.com/en-us/documentation/articles/active-directory-scim-provisioning/)[[186]](#footnote-186).

## Accessing your on-premises web applications on the Internet

With the ability of Azure AD to manage access to cloud based applications as covered in the previous sections, i.e. the ones the organization is developing and/or the ones the organization is subscribing to, the next question that inevitably comes in mind is "*How can I manage access to the organization’s on-premises web applications?*"

The Azure AD Application Proxy allows to extend the discussed Azure AD's pre-integrated SaaS and custom application management capabilities to your on-premises traditional applications, giving you the ability to manage conditional access to (Windows and on-Windows) web based applications. You can then make these apps available in a secure manner to authenticated users through a cloud proxy hosted in Azure.

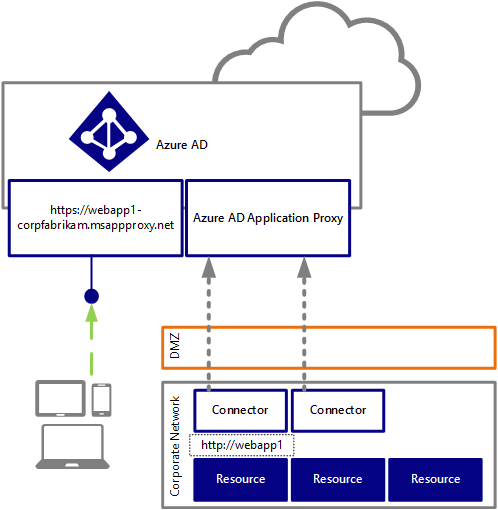
Important note This feature is only available when you enable the premium edition of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[187]](#footnote-187).

The Azure AD Application Proxy is a reverse-proxy as a service that builds on the Web Application Proxy (WAP) capability built for and available as a server role in Windows Server 2012 R2.

Note For additional information, see the Microsoft TechNet article [Web Application Proxy](http://technet.microsoft.com/en-us/library/dn584107.aspx)[[188]](#footnote-188).

It enables selective publishing of application endpoints on HTTP(S) that are hosted in Azure, so any type of device and browser can connect to them.

This implies the installation of a light weight software agent (a.k.a. a connector) on-premises typically at the backend application tier: the Azure AD Application Proxy connector is deployed usually on the organization’s corporate network next to resources.



The Azure AD Application Proxy connector calls out the proxy by issuing outgoing HTTP(S) requests to the cloud proxy service. Unlike a VPN connection, there is no direct inbound access to the corporate network. This greatly limits the attack surface area exposed.

Note The [Azure AD Application Proxy Connector Troubleshooter](http://aka.ms/aadapConnectorTroubleshoot)[[189]](#footnote-189) allows you to easily troubleshoot network issues on the connector machine like closed outbound ports. For additional information, see the blog post [Troubleshooting tool to validate connector networking prerequisites](http://blogs.technet.com/b/applicationproxyblog/archive/2015/09/03/troubleshooting-tool-to-validate-connector-networking-prerequisites.aspx)[[190]](#footnote-190).

Users connect to the cloud proxy service that performs a set of validation checks. The cloud proxy service can for instance challenge for step-up multi-factor authentication. Once that is completed, the proxy attempts to rout the traffic to the resources via the connector. In other words, the cloud proxy service sends back responses which contain a payload of incoming requests from a user which are routed from connector to the on-premises target resource.

Multiple connectors can be deployed for redundancy, scale, multiple sites and different resources for scalability and advanced topology scenarios. For example, thanks to connector groups, if you have multiple branch offices in different regions, or if you want to ensure redundancy in case of failure.

Note For additional information, see the blog post [Publishing apps on separate networks and locations using connector groups](http://blogs.technet.com/b/applicationproxyblog/archive/2015/10/14/publishing-apps-on-separate-networks-and-locations-using-connector-groups.aspx)[[191]](#footnote-191).

The benefit of this architecture is that there is no infrastructure for you to operate in the DMZ, and users can access your on-premises applications without gaining direct access to your network as illustrated hereafter.

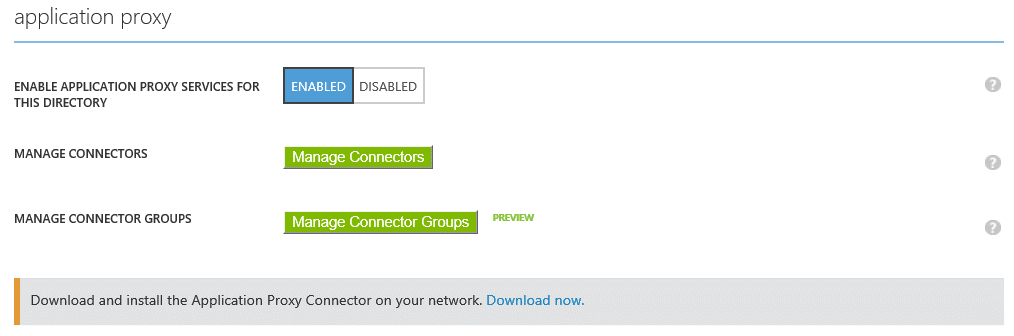
Note For additional information, see the Microsoft TechNet article [Using Application Proxy to publish applications for secure remote access](https://msdn.microsoft.com/en-us/library/azure/dn768219.aspx)[[192]](#footnote-192).

### Enabling the Azure AD Application Proxy

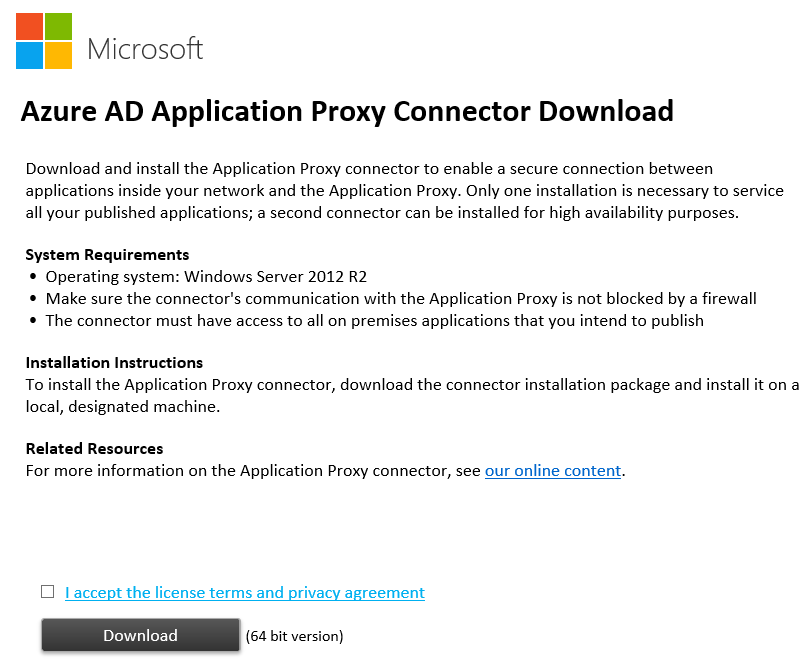
To enable the Azure AD Application Proxy service, proceed with the following steps:

Note For more information, see the Microsoft MSDN article [Enable Application Proxy services](http://msdn.microsoft.com/en-us/library/azure/dn768214.aspx)[[193]](#footnote-193).

1. Open a browsing session and sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which you want to turn on the proxy service.
3. Click **CONFIGURE** and scroll down to **application proxy**.
4. Click **ENABLED** to turn the proxy service on.
5. Click **SAVE** to save the configuration.



1. Click **Download now** to download the connector to your corporate network. A new page pops up in a new tab.



1. Check **I accept the license terms and privacy agreement**, and then click **Download**.



1. Click **Save** to save the Azure AD Application Proxy connector (*AADApplicationProxyConnectorInstaller.exe*) setup package.

### Deploying the Azure AD Application Proxy connector

You will then need to install the Azure AD Application Proxy connector inside the organization’s corporate network on at least one computer running Windows Server 2012 R2 and register it with your Azure AD tenant.

To deploy the Azure AD Application Proxy connector on an on-premises server, proceed with the following steps:

1. Install the connector (*AADApplicationProxyConnectorInstaller.exe*) setup package on the computer. A wizard dialog pops up. Follow the instructions in the wizard to install.
2. During installation you will be prompted to register the connector with your proxy service with your active Azure AD account.
3. Click **Finish** in the installation window to complete installation. When the installation completes, a new service named **Microsoft AAD Application Proxy Connector** is added to your computer.

At this stage, you can publish selected on-premises applications so that they can be made accessible to your users outside your private network.

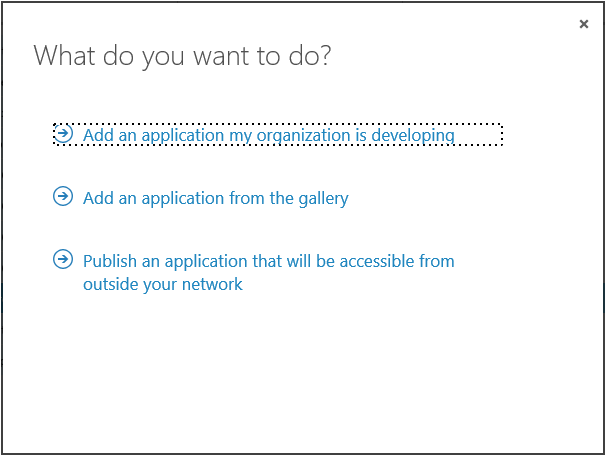
### Publishing an on-premises web application

Any web app over the HTTP 1.1 protocol can work, for example SharePoint web site, Outlook Web App (OWA), Lync Web App, ASP.NET web site, IIS applications, Windows Server 2012 R2 Work Folders, or any other homegrown or third parties’ applications.

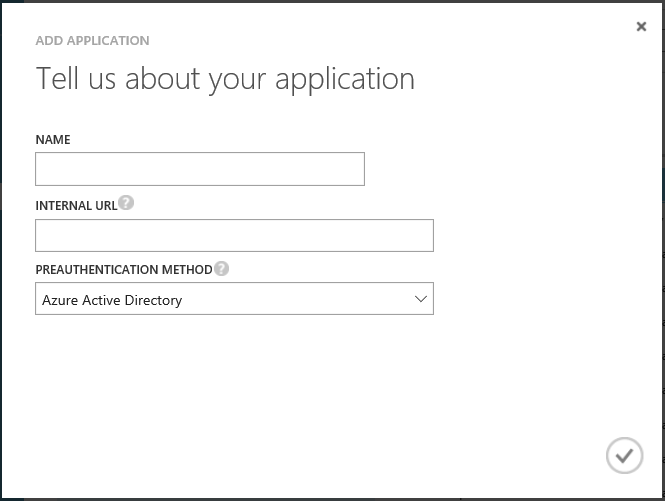
Note For more information, see the Microsoft TechNet article [Publish applications with Application Proxy](http://msdn.microsoft.com/en-us/library/azure/dn768220.aspx)[[194]](#footnote-194).

To publish an on-premises web application, proceed with the following steps:

1. Sign into the classic Azure management portal as the administrator of the directory to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which you want to add a pre-integrated SaaS application.
3. Click **APPLICATIONS** in the **active directory**.
4. Click **ADD** in the tray of the bottom. A **What do you want to do?** dialog brings up.



1. Click **Publish an application that will be accessible from outside your network**. An **ADD APPLICATION** dialog pops up.



1. Provide the following information about your application:
   1. In **NAME**, specify a descriptive name for the application you publish, for example “*webapp1*” in our illustration, and then click the arrow icon at the bottom right.
   2. In **INTERNAL URL**, specify the internal URL that the Application Proxy connector uses to access the application internally on the corporate network. This is the URL that is typically used to access the application on your premises.

The proxy service assigns a unique external URL for you that can be used to access the application from outside your private network. The URL is automatically generated based on the name you provided in the previous step, the related directory, and the suffix ***msappproxy.net*.**

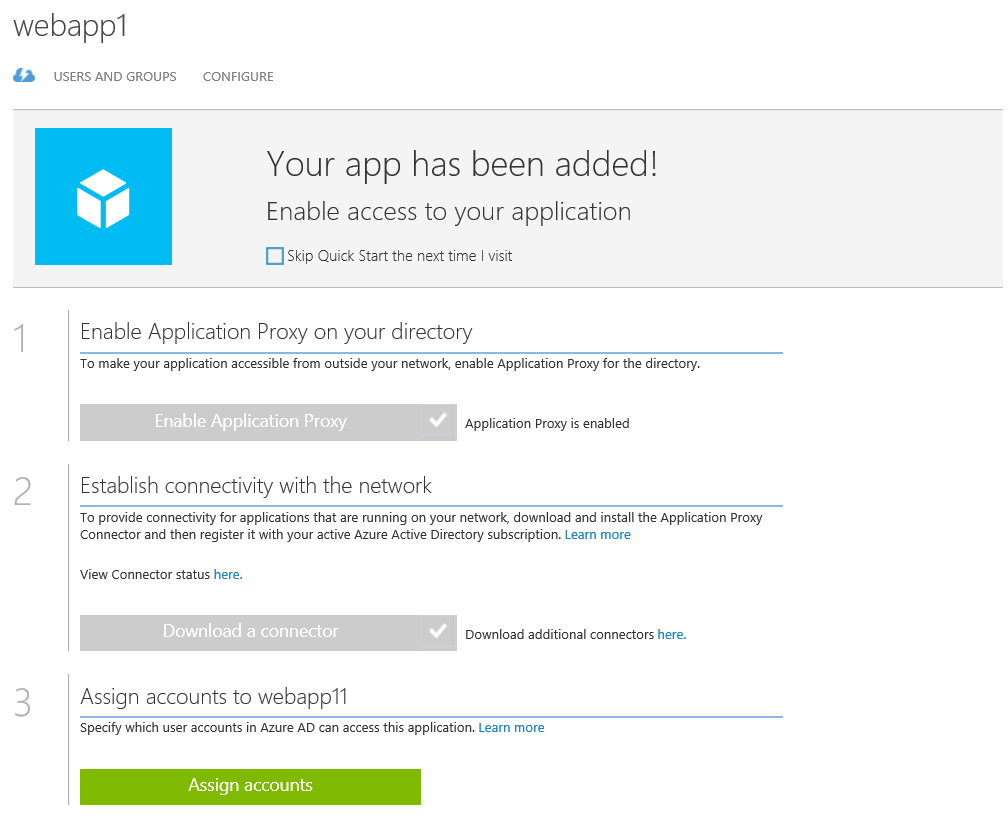
* 1. In **PREAUTHENTICATION METHOD**, set the type of pre-authentication method to use for the application:
     1. **Azure Active Directory**. Whenever a user tries to access the application, the proxy service will redirect the user to Azure AD for sign-in. Azure AD will then authenticate the user ensuring that the user has the necessary permissions for the directory and the application (see below).

This enables to benefit from the additional security capabilities such as Distributed Denial of Service (DDoS) protection, auditing and anomaly detection, etc.

- or -

* + 1. **Passthrough**. Pre-authentication is not performed.

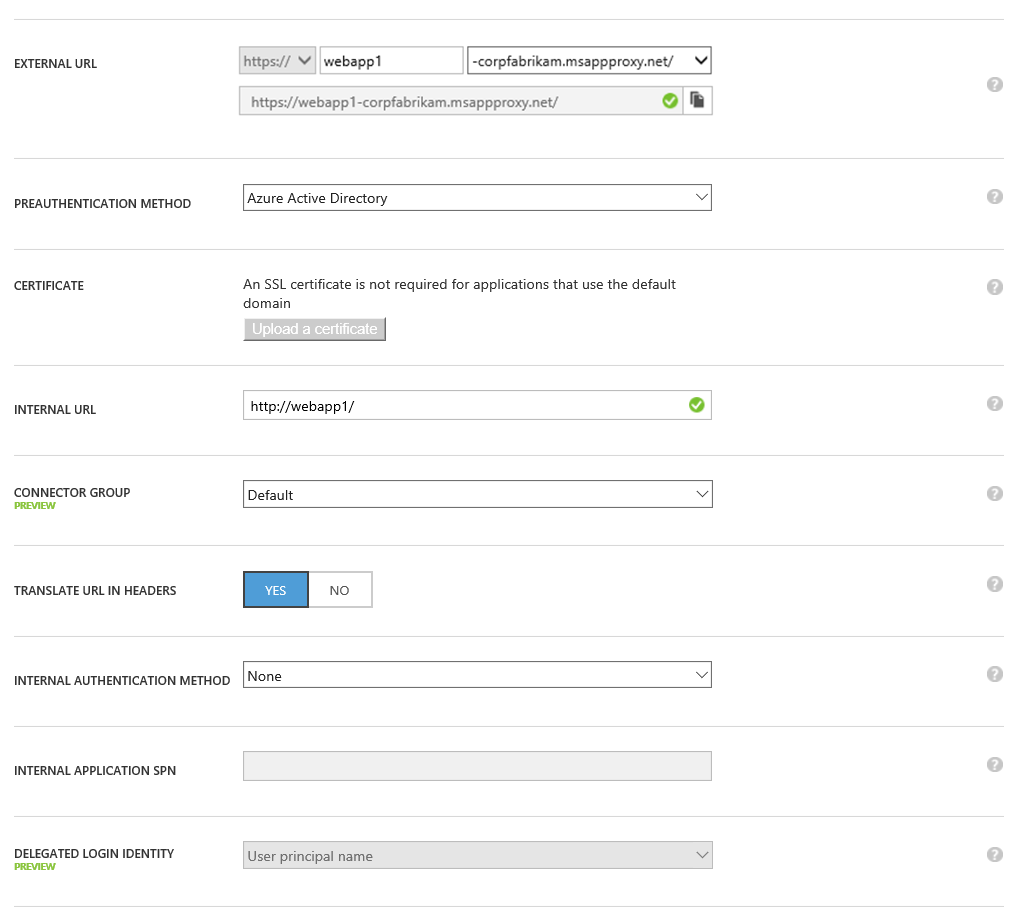
1. Click the check mark icon at the bottom of the screen.



Interestingly, the Azure AD Application Proxy supports the use of a custom verified domain name for the published on-premises application so that users can feel “at home” when access it.

To use a custom verified domain name, proceed with the following steps:

1. Click **CONFIGURE** and scroll down to **EXTERNAL URL**.



1. From the drop down box, select the custom verified domain name you want to use.
2. Click **SAVE** at the bottom of the tray.
3. Click **Upload a certificate** in **CERTIFICATE**. Upload a certificate that matches this domain name in PFX file format. The certificate must be a valid certificate that has a private key. Simple certificates, SAN or wildcard certificates can be used.
4. Add to the public DNS registrar that cover this domain name a CNAME record that would point to the msappproxy.net record of your application as instructed, and you’re done!

Note For more information, see the blog post [Azure AD Application Proxy now supports custom domain](http://blogs.technet.com/b/ad/archive/2015/04/22/azure-ad-application-proxy-now-support-custom-domain-names.aspx)[[195]](#footnote-195).

Like the pre-integrated SaaS and custom applications, Azure AD will not allow users to have an access into the application unless they have been granted access. Users may be granted access directly, or through a group that they are a member of. You can follow the directions outlined in section § Managing access to applications to quickly assign it to your employees.

## Providing identity and access management to (your) modern business applications

Modern business applications you’re developing can be easily integrated with your directory and granted access to that directory so that you can easily provide single sign-on capabilities (sign in and sign out), manage the user authorization, etc. without the additional cost, burden, and hassle of having to acquire and manage new user credentials. This comprises not only homegrown web applications, web APIs but also native applications.

Note A native application is an application that is installed on a device such as a phone or computer. The combined influence of growing presence of devices in business environments with the Consumerization of IT and the Bring Your Own Device (BYOD) trends, and success of the various marketplace (iTunes, Google Play, Windows (Phone) Store make this form factor one of the fastest growing ones.

The main areas of native application revolve around mobile workforce scenarios (sales people, pharmaceutical promoters, etc.), scenarios in which mobility and free hands are of essence (manufacturing, logistic, healthcare services) and the like.

Note For more information, see the Microsoft MSDN article [Integrating Applications in Azure Active Directory](http://msdn.microsoft.com/en-us/library/windowsazure/dn151122.aspx)[[196]](#footnote-196).

For the federated users, a seamless end-to-end single sign-on (federated) experience can be delivered for users logging on their Windows 10 Azure AD joined machines, Windows domain-joined machines and their Workplace joined devices on (exposed) on-premises applications and other applications integrated in your Azure AD directory. Such an experience requires to federate your directory with your on-premises STS, and may require to sync the devices objects between your Azure AD directory and your on-premises identity infrastructure depending on your configuration in place.

Furthermore, if you’re a developer or a cloud ISV, you can allow for external users a web application (or a web API) that you've previously registered in your Azure AD directory and consequently make it available with one click for use by any other Azure AD customer. With one click, those customers can in turn add your web application (or web API) to their own directory tenant giving it a clearly called out set of privileges. They get the benefit of using Azure AD to administer access to your application with one click, you get the benefit of offering world class enterprise directory capabilities that can be easily connected to your customers existing on-premises directory infrastructure.

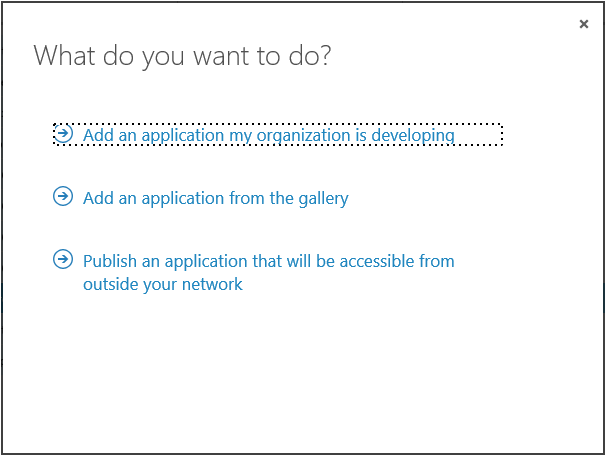
The aforementioned white paper [Leverage Azure AD for modern business applications](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[197]](#footnote-197) details the registration process in directory tenant(s) and how to (build and) configure such applications to provide sign up for multi-tenant applications, single sign-on for cloud and federated users, and more.

### Adding a modern business application

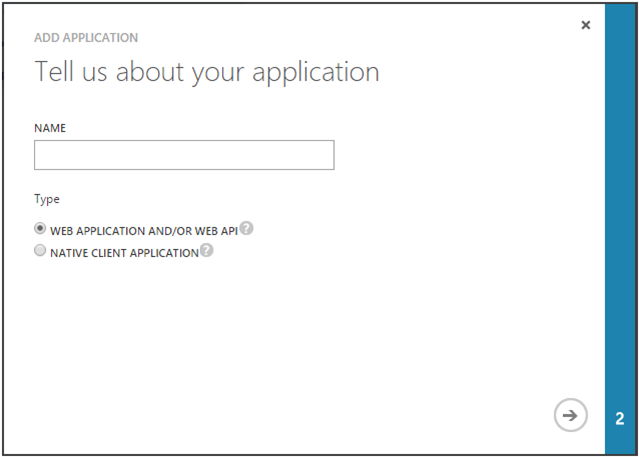
To simply illustrate the related operation, let’s consider a (fictitious) single-tenant web application you’re developing.

To add a single-tenant application, proceed with the following steps:

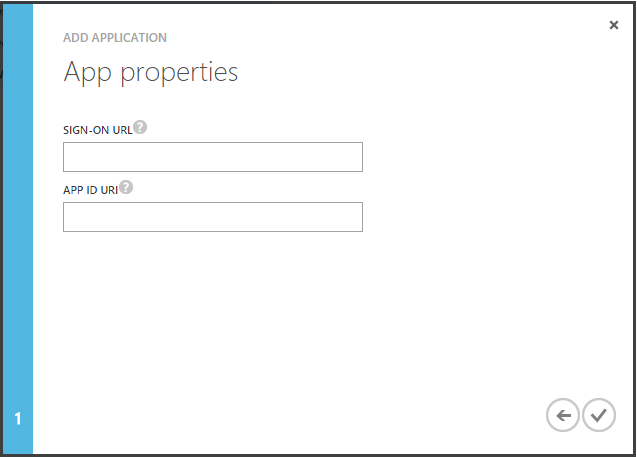
1. Sign into the classic Azure management portal as the administrator of the directory to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which you want to add the single-tenant web application you’re developing.
3. Click **APPLICATIONS** in the **active directory**.
4. Click **ADD** in the tray of the bottom. A **What do you want to do?** dialog brings up.



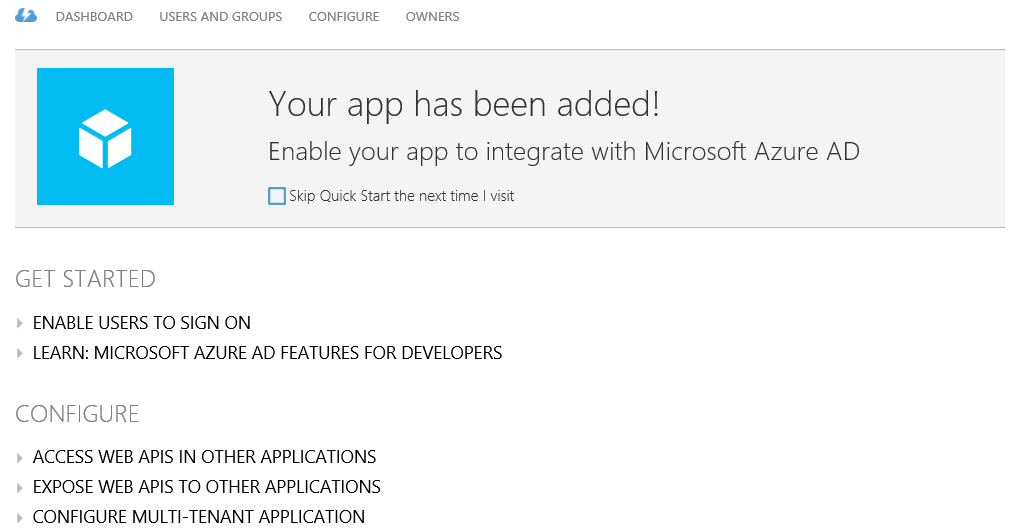
1. Click **Add an application for my organization is developing**.



1. On the **Tell us about your application** page, specify a name for your web application. This used as human-readable moniker to refer to the application. Select **WEB APPLICATION AND/OR WEB API**. Click the arrow icon on the bottom-right hand corner of the page.



1. On the **App properties** page, provide the URL of a web page where users can sign in and use the web application in **APP URL**, and the ID URI to use to logically identify the web application in **APP ID URI**, then click the check mark icon on the bottom-right hand corner of the page.
2. You are redirected to the **Quick Start** page for the web application.



Note For more information, see the MSDN article [Adding, Updating, and Removing an App](http://msdn.microsoft.com/en-us/library/dn132599.aspx) [[198]](#footnote-198).

Like the pre-integrated SaaS, custom, and published on-premises applications, Azure AD will not allow users to have an access into the application unless they have been granted access. Users may be granted access directly, or through a group that they are a member of. You can follow the directions outlined in next section § Managing access to applications to quickly assign it to your employees.

# Managing access to applications

You can assign access privileges to your applications to the users in your Azure AD directory tenant assuring that every employee has access to the applications they need. Interestingly enough, when a user leaves your organization or changes jobs within the company, you can just as easily remove their access privileges assuring data security and minimizing IP loss.

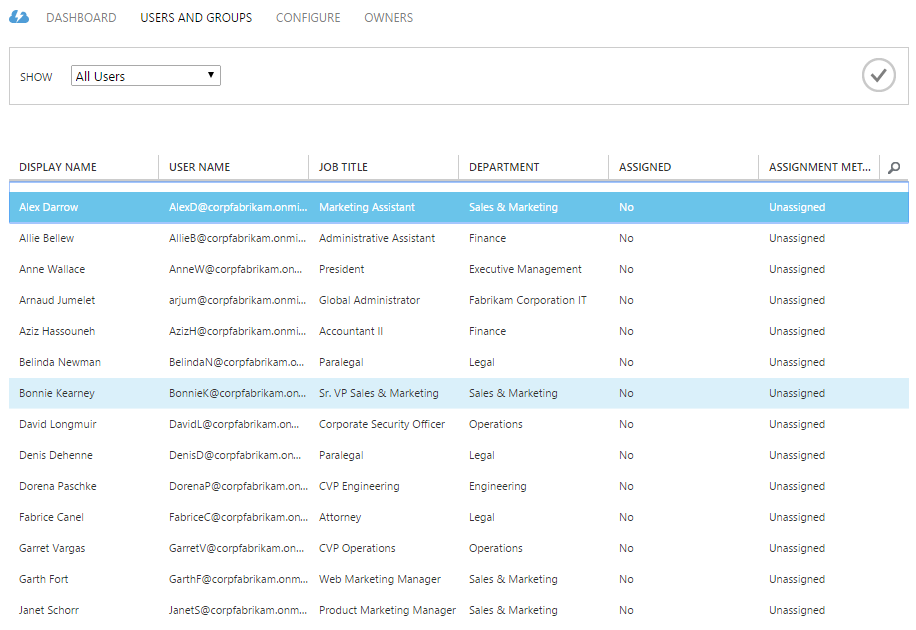
A single, unified administrative experience for all of your applications is provided, whether it is a pre-integrated SaaS application, a custom application, a published on-premises web application (provided that pre-authentication has been chosen for publishing), or a modern business application you’re developing. Let’s see how this works.

## Assigning/Removing users

To manage application access to users, proceed with the following steps:

1. Click **USERS** under the application in the Azure management portal.

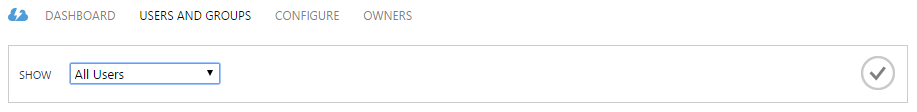
Important note If you have enabled the Basic or the Premium editions of Azure AD, click USERS AND GROUPS instead. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[199]](#footnote-199).



Users can be created directly on Azure AD or originated from the on-premises AD that is synced to Azure AD. (See section § Synchronizing your directory with Active Directory on-premises earlier in this document.)

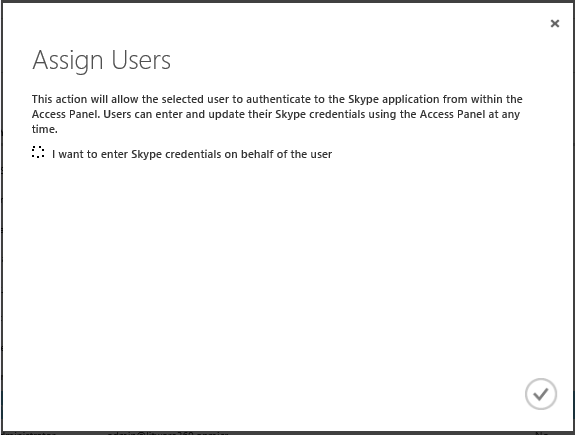
1. Select the right users and use the **ASSIGN** button at the bottom to grant access. (Conversely, use the **REMOVE ASSIGNMENT** button to remove access).

Important note If you have enabled the Azure Active Directory Premium, next to ****SHOW****, select All Users in the drop-down list.



Then click the check mark icon. You can then proceed as instructed is step 2.

Note With a pre-integrated SaaS application configured with password single sign-on, such as the Skype application hereafter, you can directly configure the user’s credentials (username and password) for this application. For that purpose, select I want to enter Skype credentials on behalf the user while enabling access (or through the EDIT ACCOUNT button after the access has been enabled).

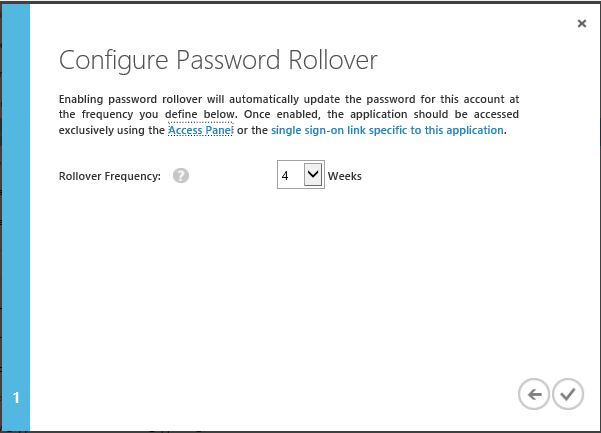


If you choose not to do this, the user will need (and be able) to enter their own credential through the Azure AD Access Panel. The users can only see in the Access Panel the applications the administrator has granted them access.

Note The above capability can be leveraged for shared organization’s accounts to be used with some pre-integrated SaaS applications. In such a context, and more specifically for the pre-integrated Facebook, Twitter, and LinkedIn applications, you will have the ability to enable an automatic password rollover. For that purpose, select in addition I want to enable an automatic password rollover.



After clicking the check mark icon, you will be then provided with the ability to configure the password rollover.



You can select the frequency at which Azure AD will sign into the application and rollover the password for the provided account. During each rollover, the password is updated using a randomly-generated 16-character strong password.

For more information, see the blog posts [Azure Active Directory's support for managing shared company accounts for Twitter, Facebook and more](http://blogs.technet.com/b/ad/archive/2014/10/31/azure-ad-now-supports-sharing-logins-for-twitter-facebook-and-more.aspx)[[200]](#footnote-200) and [Azure AD automated password roll-over for Facebook, Twitter and LinkedIn now in preview!](http://blogs.technet.com/b/ad/archive/2015/02/20/azure-ad-automated-password-roll-over-for-facebook-twitter-and-linkedin-now-in-preview.aspx)[[201]](#footnote-201).

A browser based end-user Azure AD Access Panel, My Apps mobile applications, or Azure AD single sign-on links **make** it easy for users to find and then launch with a single sign-on experience applications that are assigned to them (See section § Empowering users later in this document).

## Using groups to control access

A group is a collection of users and groups that can be managed as a single unit. Users and groups that belong to a particular group are referred to as group members.

As with Active Directory on-premises, using groups in Azure AD can simplify administration by assigning a common set of permissions and rights to many accounts at once, rather than assigning permissions and rights to each account individually. Groups can be created directly on Azure AD or originated from the on-premises AD that is synced to Azure AD. (See section § Synchronizing your directory with Active Directory on-premises earlier in this document.)

Note For more information, see the article [Managing access to resources with Azure Active Directory groups](file:///C:\Users\Public\Documents\Activités\DT&S\Sécurité\Livrables\FY16\AAD%20whitepapers\NEW%20Introduce%20AAD%20B2B\How%20to%20configure%20and%20assign%20groups%20in%20Windows%20Azure%20AD)[[202]](#footnote-202).

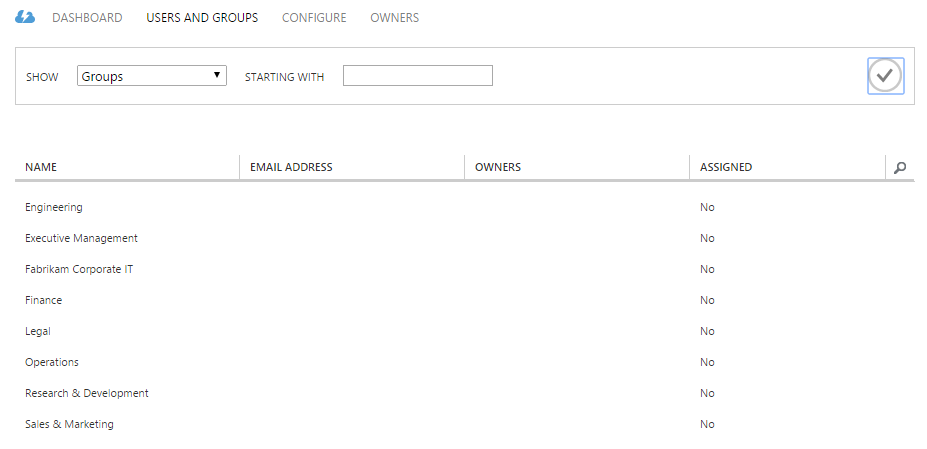
To use groups in lieu of users to control access to SaaS applications, proceed with the following steps:

1. Click **USERS AND GROUPS** under the application in the Azure management portal.

Important note This feature is only available when you enable Azure Active Directory Premium. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[203]](#footnote-203).



1. Next to **SHOW**, select **Groups** in the drop-down list. Next to **STARTING WITH**, optionally specify the first characters of the name of the group, and, then click the check mark icon.



1. Select the right groups and use the **ASSIGN** button at the bottom to grant access. (Conversely, use the **REMOVE ASSIGNMENT** button to remove access). A confirmation dialog brings up at the tray in the bottom.



1. Click **YES** to confirm the operation.

## Leveraging dynamic groups

The Dynamic membership for groups feature represents the first step in the efforts to support Role Based Access Management (RBAC) in Azure AD.

Important note This feature is only available when you enable the premium edition of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[204]](#footnote-204).

With this feature, you can now specify a rule on a security group that will automatically manage the membership of that group based on user's attribute values. Dynamic membership enables you to define a group using single attribute rules, such as "*All users where Department equals Sales*", or you can configure complex rules including logical operators to combine clauses, such as in "*All users where Department equals Sales or Marketing and Job title contains Manager*".

A typical scenario would then give this group access to some applications. (It can also serve to automatically assign to users Office 365 licenses.)

Note For additional information, see the blog post [Attribute based Dynamic Group Membership for Azure AD Premium is now in Preview](http://blogs.technet.com/b/ad/archive/2015/03/09/attribute-based-dynamic-group-membership-for-azure-ad-premium-is-now-in-preview.aspx)[[205]](#footnote-205). You can also watch the Channel 9 demo video [Azure AD: Introduction to Dynamic Memberships for Groups](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Azure-AD--Introduction-to-Dynamic-Memberships-for-Groups)[[206]](#footnote-206).

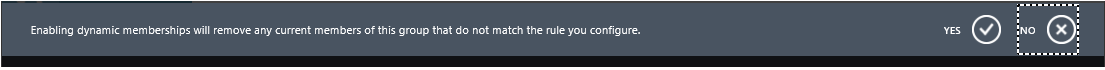
To configure a rule to manage memberships on a security group, proceed with the following steps:

1. From the Azure AD management portal, just create or select a new security group.
2. Click the group's **CONFIGURE** tab.

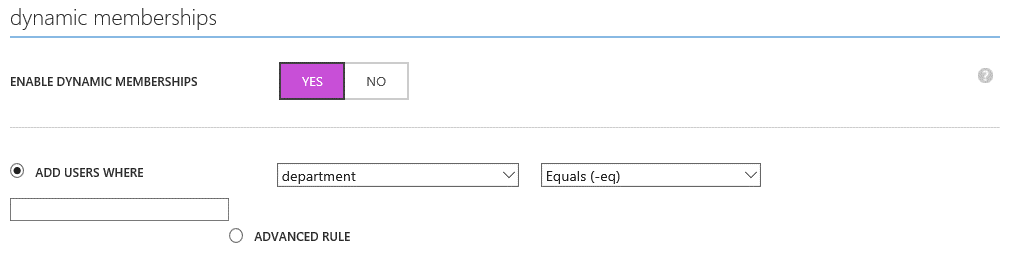


1. Click **YES** next to **ENABLE DYNAMICS MEMBERSHIPS**.

Important note To enable the dynamic rules evaluation, you need to enable delegated groups Management feature (see DELEGATED GROUP MANAGEMENT ENABLED under group management in the directory CONFIGURE page).



1. Click **YES**.



1. Configure a rule for the group.
2. Click **SAVE** at the bottom of the tray.
3. Configure a rule for the group.

When first configuring a rule for a group, all users in your Azure AD tenant are scanned to find which users satisfy the rule you provided, and all matching users are added as members to the group. Subsequent changes to user's attributes, such as when a user changes job titles or departments, or when a new user joins, will trigger a re-evaluation of the rule and the outcome of that evaluation will be reflected in the user's group memberships.

You can then use the dynamic group as per previous section.

## Registering the devices

As discussed in the [Active Directory from the on-premises to the Cloud](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[207]](#footnote-207) whitepaper, the rapid increase in the number of consumer devices and ubiquitous information access is changing the way that people perceive their technology. The constant use of information technology throughout the day, along with easy access of information from everywhere, is blurring traditional boundaries between work and home life. These shifting boundaries as a result of the consumerization of IT (CoIT) are accompanied by a belief that personal technology should extend into the workplace.

To accommodate the growing requirement of personal consumer devices to access the organization’s applications, Windows Server 2012 R2 has introduced the AD Workplace Join capability on-premises. This capability allows users to join their devices with the organization’s workplace and thus enables their devices to be provisioned with an identity. When a device is joined by Workplace Join, it becomes a known device, provides seamless second factor authentication to access to the organization’s applications, and attributes of the device can be retrieved from AD to drive conditional access for the purpose of authorizing issuance of security tokens for these applications.

Workplace Join is made possible on-premises by Device Registration Service (DRS) that is included with AD FS in Windows Server 2012.

**Note** For additional information, see the Microsoft TechNet 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)[[208]](#footnote-208).

The registered devices can then be used in the conditional access policies that are available in AD FS in Windows Server 2012 R2.

**Note** For more information, see the Microsoft TechNet article [Manage Risk with Conditional Access Control](http://technet.microsoft.com/en-us/library/dn280937.aspx)[[209]](#footnote-209) as well as the [Azure AD/Office 365 single sign-on (SSO) with AD FS in Windows Server 2012 R2 – Part 1](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[210]](#footnote-210) whitepaper.

Azure AD provides similar features and beyond.  Let’s consider them.

### Registering Android, iOS, and Windows devices

The Azure AD Device Registration (Azure AD DRS) enables Workplace Join and register devices in Azure AD in lieu of on-premises with DRS. Azure AD DRS enables employee's devices to be provisioned with an identity.

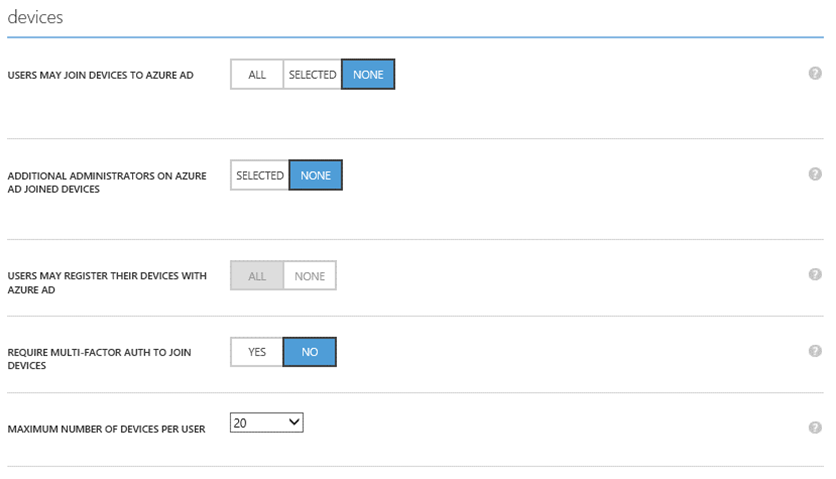
When a device is registered, Azure AD DRS provisions the device with an identity in the Azure AD tenant which is used to authenticate the device when the user signs in. The authenticated device, and the attributes of the device, can then be used to enforce conditional access policies for applications that are hosted in the cloud and on-premises.

Once a policy is set to require compliant devices to access Office 365, Azure AD authenticates the device and checks whether the device is complaint before allowing access to Office 365 services such as email and SharePoint.

**Note** The registered devices can also be used in the above AD FS similarly to what could previously be achieved through the deployment of DRS. This requires device objects write-back to AD from Azure AD as per synchronization between the two. (See section § Synchronizing your directory with Active Directory on-premises before in this document).

To enable Azure AD DRS, proceed with the following steps:

1. Open a browsing session and sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which device registration should be enabled.
3. Click **CONFIGURE** and scroll down to **devices**.



1. Set **USERS MAY REGISTER THEIR DEVICES WITH AZURE AD** to **ALL** in order to enable device registration.

Note Enrollment with [Microsoft Intune](http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/default.aspx)[[211]](#footnote-211) (or Mobile Device Management for Office 365) requires Workplace Join. If you have (already) configured either of these services, ****ALL**** will be already selected for USERS MAY REGISTER THEIR DEVICES WITH AZURE AD.

1. By default, once enabled, users can have 20 devices joined with Azure AD (**MAXIMUM NUMBER OF JOINED DEVICES PER USER**). If a user reaches this quota, they will not be able to join additional devices until one is deleted. You can change this value to accommodate your own needs and/or requirements.

Furthermore, and by default, multi-factor authentication is not enabled for the service. However, requiring multi-factor authentication is recommended for joining devices to Azure AD. Click **YES** next to **REQUIRE MULT-FACTOR AUTH TO JOIN DEVICES** if users that are connecting to the workplace from the Internet must use a second method of authentication before they can workplace join their device. This said, you MUST prior configure a MFA solution and configure your user accounts for Multi-Factor Authentication (See section § Using Azure Multi-Factor Authentication later in this document).

1. After configuring the device registration capability as desired for your tenant, click **SAVE** in the tray of the bottom.

**Once Azure AD DRS is enabled, you will then need to configure the service discovery if you have custom vanity domain(s) associated with your Azure AD tenant.**

You must indeed create a DNS CNAME record that points to the A record associated with your Azure AD DRS. The CNAME record must use the well-known prefix **enterpriseregistration** followed by the UPN suffix used by the user accounts at your organization. If your organization uses multiple UPN suffixes, multiple CNAME records must be created in DNS. For example, if you use two UPN suffixes at your organization named *@corpfabikam.com* and **@region.corpfabikam.com**, you will create the following DNS records.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Type | | Value | |
| enterpriseregistration.corpfabikam.com | | CNAME | | enterpriseregistration.windows.net |
| enterpriseregistration.region.corpfabikam.com | | CNAME | | enterpriseregistration.windows.net |

After adding the above records in your domain registrar, users in your organization who sign in on their device with an email address that uses the above suffixes can register to your Azure AD tenant.

Note For more information, see the blog post [Azure AD Device Registration is now Generally Available](http://blogs.technet.com/b/ad/archive/2015/03/30/azure-ad-device-registration-service-is-now-ga.aspx)[[212]](#footnote-212) and the Microsoft MSDN articles [Azure Active Directory Device Registration Overview](https://msdn.microsoft.com/en-us/library/azure/dn903763.aspx)[[213]](#footnote-213) and [Setting up On-premises Conditional Access using Azure Active Directory Device Registration](https://msdn.microsoft.com/en-us/library/azure/dn788908.aspx)[[214]](#footnote-214).

### Joining Azure AD with Windows 10 devices

Azure AD and Windows 10 together provide an evolution of the traditional WSAD **Domain Join**. Indeed, on domain joined computers, the connected Windows services (backup and restore, roaming of settings, live tiles and notifications, Windows store, etc.) will work natively with work or school accounts. There will be no longer the requirement to use a personal Microsoft Account (MSA).

Windows 10 will use Azure AD as a relay to power these experiences, which means that organizations must have a hybrid Active Directory environment in-place and thus have connected their on-premises WSAD to Azure AD to make this happen. Both synchronization and federation models will be supported in terms of identity model.

Auto-registration of these devices in Azure AD and auto-enrolment in an Azure AD supported Mobile Device Management (MDM) solution ([Microsoft Intune](http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/default.aspx)[[215]](#footnote-215), Mobile Device Management for Office 365, or 3rd party solution) will be all supported.

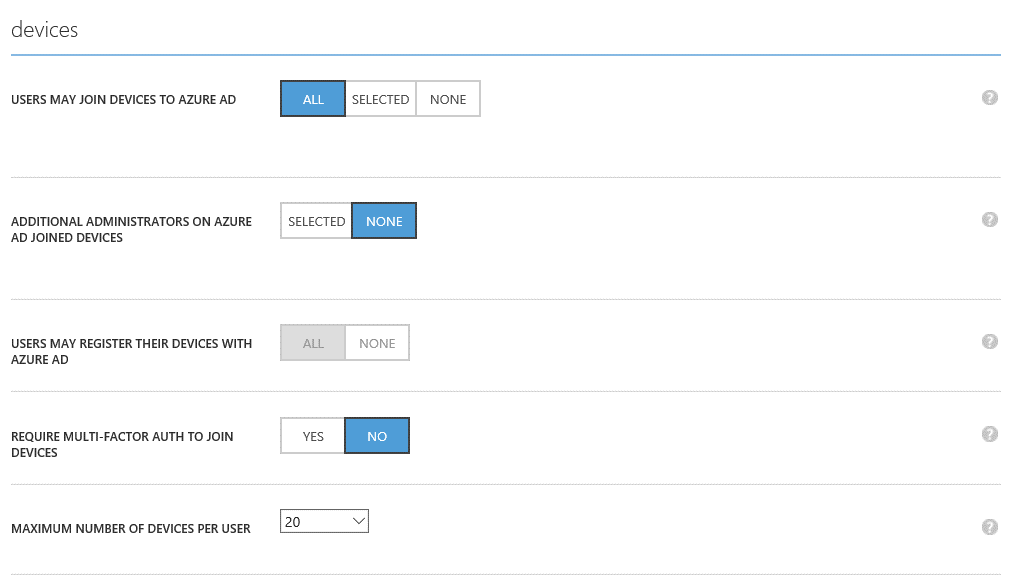
This new feature of Windows 10 Pro and Windows 10 Enterprise editions is called **Azure AD Join**.

With this new feature, Windows also will enable a device to join an Azure AD tenant without needing the traditional WSAD domains on-premises if you want to. In this cases, Windows will directlyauthenticate to Azure AD. You can then enjoy a cloud-only environment and this only requires that your organization provisions an Azure AD tenant.

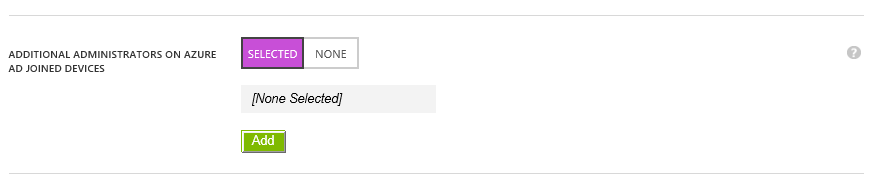
Note For more information, see the whitepaper [Azure AD & windows 10: Better Together for Work or School](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[216]](#footnote-216).

To enable Azure AD Join in addition of the Azure DRS, proceed with the following steps:

1. Click **CONFIGURE** for the organization’s directory for which Azure AD Join should be enabled and scroll down to **devices**.
2. Click **USERS MAY AZURE AD JOIN DEVICES**.
3. Click **SAVE** at the bottom of the tray. **USERS MAY AZURE AD JOIN DEVICES** supersedes **USERS MAY REGISTER THEIR DEVICES WITH AZURE AD** that is thus grayed.



When a Windows 10 device will join Azure AD, you are provided with the ability to configure additional administrators to later have administrative privileges on it.



Now that you now the various options to register a device, let’s deal with the conditional access control.

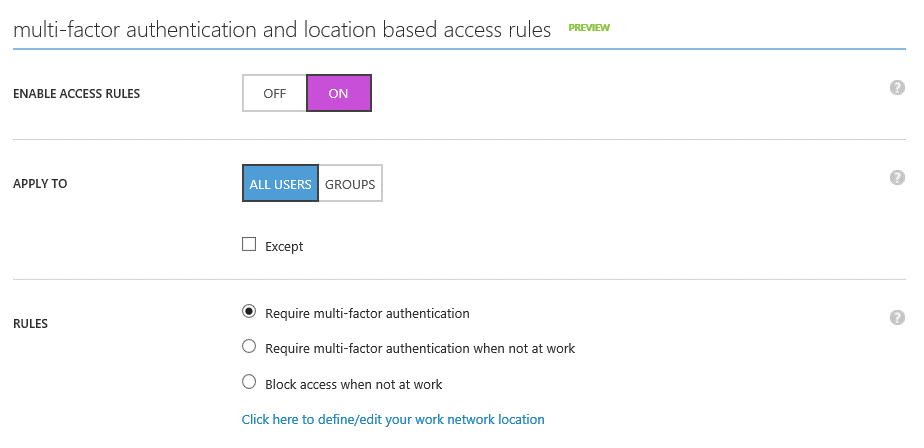
## Using Conditional Access Control

Conditional Access is the ability to define different access rules for applications based on the business needs, user location and the device that is used. This feature is available for all the federated pre-integrated SaaS applications, your on-premises applications that use Azure AD Application proxy, your Line of business (LOB) applications that your organization has specifically developed for and registered in Azure AD, as well as multi-tenanted applications developed by other organizations. Conditional access rules are independent of the supported protocol used by the application if any (WS-Fed, SAML 2.0, OpenID Connect 1.0 or OAuth 2.0).

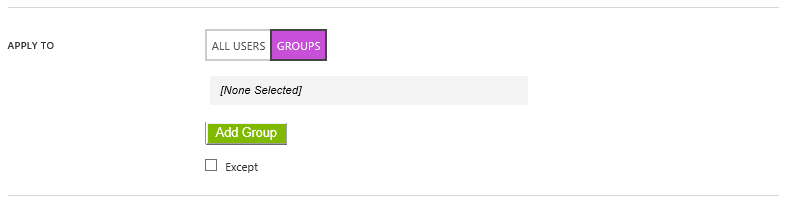
Important note This feature is only available when you enable the premium edition of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[217]](#footnote-217).

To define conditional access rules for an application, proceed with the following steps:

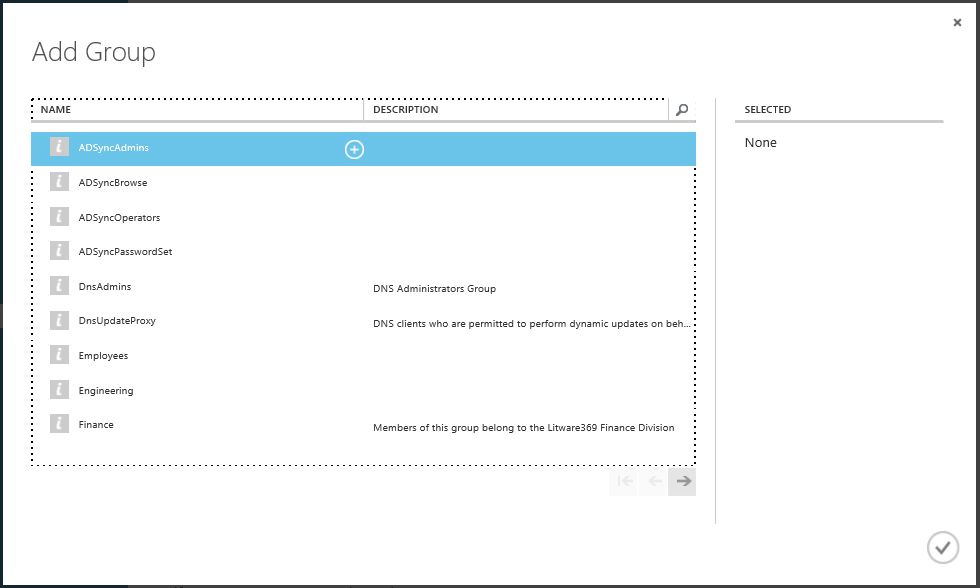
1. Click **CONFIGURE** under the application in the classic Azure management portal.
2. Scroll down to **multi-factor authentication and location based** **access rules**.
3. Set **ENABLE ACCESS RULES** to **ON**.



1. Define the scope for the rules. Rules can be applied to all users or to specific security groups. Click **GROUPS** for the latter case.



Click **Add Group** and then specify the groups in the eponym dialog.Click the check mark once done.



1. Define the rule itself: **Require multi-factor authentication**, **Require multi-factor authentication when not at work**, or **Block access when not at work**.

Thanks to the first two options, you can require just username and password or multi-factor authentication (MFA) to login into an application depending if the user is on the corporate network or off the network. The access rule work with Azure MFA. They also work on-premises if you have deployed AD FS in Windows Server 2012 R2 and set up it with an MFA adapter. Azure AD will perform the conditional access check, and then redirect the MFA request to AD FS.

Note To sustain the above capability of the access rules, the default MFA behavior for federated Azure AD/Office 365 tenants has been set to occur in the cloud where in the past it was set to occur on-premises. Operations has backfilled to ensure customers that were using multi-factor authentication on-premises will continue to use their on-premises infrastructure. You can affect this behavior by downloading latest version of the Azure Active Directory Module for Windows PowerShell (64-bit version) from [here](http://social.technet.microsoft.com/wiki/contents/articles/28552.microsoft-azure-active-directory-powershell-module-version-release-history.aspx)[[218]](#footnote-218) and running the below commands.

To perform multi-factor authentication on-premises, you will have to run the following command:

Set-MsolDomainFederationSettings -DomainName <yourfederateddomain> -SupportsMFA $true

Where *SupportsMFA* as *true* means that Azure AD will redirected the user to AD FS for multi-factor authentication if multi-factor authentication is required and the MFA claim, is missing

To perform multi-factor authentication in the cloud for your federated domain, you will have to run the following command if you’ve previously set SupportsMFA to *true*:

Set-MsolDomainFederationSettings -DomainName <yourfederateddomain> -SupportsMFA $false

Where *SupportsMFA* as *false* means that Azure AD does multi-factor authentication natively (again assuming multi-factor authentication is required and MFA claim is missing). If flag is not set, it is assumed to be false. Users won't be double MFA'd. If multi-factor authentication was already done at AD FS as part of login, the MFA claim will be present and Azure AD won't ask for multi-factor authentication again.

1. Click **SAVE** at the bottom of the tray.

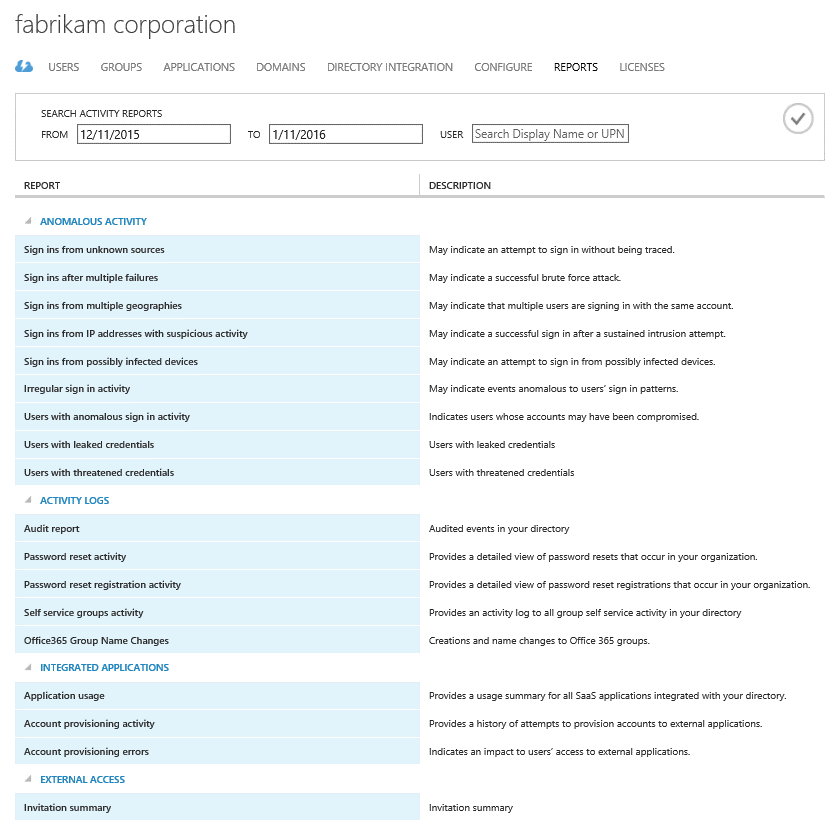
Note For additional information, see the blog posts [Azure AD Conditional Access and Azure AD Connect Health - Now in Preview](http://blogs.technet.com/b/ad/archive/2015/01/29/azure-ad-conditional-access-and-azure-ad-connect-health-now-in-preview.aspx)[[219]](#footnote-219), [Azure AD Conditional Access preview updated: Now supports On-Premises and Custom LOB apps](http://blogs.technet.com/b/ad/archive/2015/03/11/azure-ad-conditional-access-preview-updated-now-supports-on-premises-and-custom-lob-apps.aspx)[[220]](#footnote-220), and the Microsoft MSDN article [Azure Conditional Access Preview for SaaS Apps](https://msdn.microsoft.com/en-us/library/azure/dn906877.aspx)[[221]](#footnote-221).

# Monitoring and protecting access to applications and beyond

## Monitoring security reports and blocking users

The Applications Access Enhancements for Azure AD enable you to review security reports associated with the sign-ons by your organization’s end-users.

With the free version of the Application Access Enhancements for Azure AD, you get access to a standard set of access reports giving you visibility into which users are using which applications, when they were using and where they are using them from. In addition, we'll alert you to un-usual usage patterns for instance when a user logs in from multiple locations at the same time.



The following anomaly reports are available for free in Azure for monitoring tenant-wide user sign-ins to Azure AD:

* **Sign ins from unknown sources**. You can use this report when you want to determine if any users have successfully signed in to your tenant while assigned a client IP address that has been recognized by Microsoft as an anonymous proxy IP address.
* **Sign ins after multiple failures**. You can use this report when you want to determine if any users have successfully signed in after multiple failed sign in attempts. This may indicate that a hacker has been trying to guess the password of a user and finally succeeded in doing so.
* **Sign ins from multiple geographies**. You can use this report when you want to view all successful sign in activities from a user where two sign ins appeared to originate from different countries and the time between the sign ins makes it impossible for the user to have travelled between those countries. This may indicate that a hacker has signed in to the account of a user from a different country.
* **Users with threatened credentials**. You can use when you want to view all the user accounts we've found and when we discovered the threatened credentials.

The Premium offering adds following machine learning-based anomaly reports:

Important note The reports below are only available when you enable the basic or the premium editions of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[222]](#footnote-222).

* **Sign ins from IP addresses with suspicious activity**. You can use this report when you want to see sign in attempts that have been executed from IP addresses where suspicious activity has been noted.
* **Irregular sign in activity**. You can use this report when you want to see sign in attempts that have been marked as “irregular”. Reasons for marking a sign in attempt as irregular include unexpected sign in locations, time of day and locations or a combination of these. This may indicate that a hacker has been trying to sign in using this account.
* **Sign ins from possibly infected devices**. You can use this report when you want to see sign ins from devices on which some malware (malicious software) may be running.
* **Users with anomalous sign in activity**. You can use this report when you want to view all user accounts for which anomalous sign in activity has been identified. This report includes data from all other anomalous activity reports.
* **Users with leaked credentials**. You can use when you want to view all the user accounts we've found and when we discovered the leaked credentials. To mitigate the security risk, we recommend you to enable Multi-Factor Authentication or reset the password for the accounts listed.

Note For more information, see the blog post [Azure Active Directory Premium reporting now detects leaked credentials](http://blogs.technet.com/b/ad/archive/2015/06/15/azure-active-directory-premium-reporting-now-detects-leaked-credentials.aspx)[[223]](#footnote-223).

The following usage, error, and activity reports are free for monitoring user provisioning to external SaaS applications:

* **Application usage**. You can use this report to when you want to see usage for all the SaaS applications in your directory.
* **Account provisioning activity**. You can use this report to view a history of attempts to provision accounts to external applications.
* **Account provisioning errors**. You can use this report to monitor errors that occur during the synchronization of accounts.

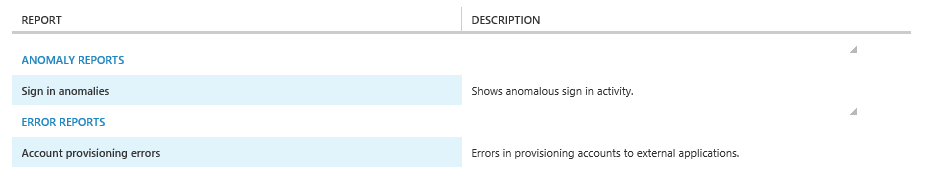
In addition to the above reports, the following new activity log reports are now available for free to give you very detailed views of user activity:

* **Audit**. You can use this report when you want to view and audit all the key changes in the directory: role membership changes, credential updates, and domain, user, license, and application management.
* **Password reset activity**. You can use this report when you want to view the history of resets done.
* **Password reset registration activity**. You can use this report when you want to view which users have registered their methods for password reset, and which methods they have selected.
* **Group activity**. You can use this report when you want to view the history of changes to the groups that were initiated in the Access Panel. (See next section.)

Note For more information, see the Microsoft MSDN article [View your access and usage reports](http://msdn.microsoft.com/en-us/library/dn283934.aspx)[[224]](#footnote-224).

To view or download a report, proceed with the following steps:

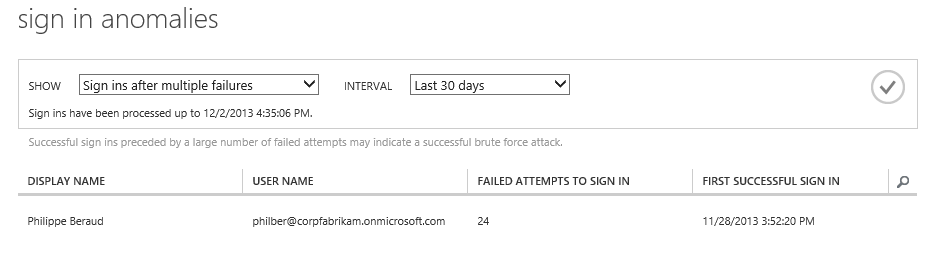
1. Sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which you want to view or download a report.
3. Click **REPORTS**.



1. Click **Sign in anomalies** to view or download an anomaly report as illustrated below. Likewise, click **Account provisioning errors** to view or download an error report for the provisioning of SaaS applications.



1. Click the drop-down menu next to **SHOW**, and then select one of the reports in the list that you want to view.
2. Click the drop-down menu next to **INTERVAL**, and then select one of the following time ranges that should be used when generating this report: **Last 24 hours**, **Last 7 days**, or **Last 30 days**.
3. Click the check mark icon to run the report.



1. If applicable, click **DOWNLOAD** at the tray in the bottom to download the report to a compressed file in Comma Separated Values (CSV) format for offline viewing or archiving purposes.

Note For more information, see the Microsoft TechNet article [View your access and usage reports](http://technet.microsoft.com/en-us/library/dn283934.aspx)[[225]](#footnote-225). you can watch the Channel 9 demo video [Azure Active Directory Reports](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Azure-Active-Directory-Reports)[[226]](#footnote-226).

Note Activity and Events Reporting data is now also available (in preview) to developers through the Azure AD Graph API.  For more details, see the guide [Azure Active Directory Reporting Guide](https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-guide/)[[227]](#footnote-227) as well as the blog post [Announcing the preview of Graph Reports and Events API](http://blogs.msdn.com/b/aadgraphteam/archive/2015/05/15/announcing-the-preview-version-of-graph-reports-and-events-api.aspx)[[228]](#footnote-228) and the Microsoft MSDN article [Azure AD Reports and Events (Preview)](https://msdn.microsoft.com/en-us/library/azure/mt126081.aspx)[[229]](#footnote-229).

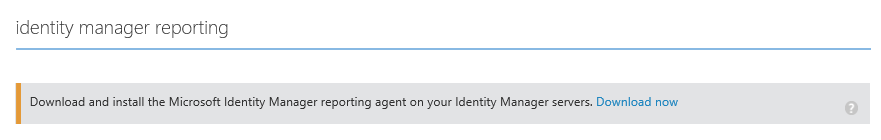
Beyond the above available reports for your Azure AD tenant, a first set of hybrid reports is now available in Azure AD. These reports give customers a unified visibility into both Azure AD in the cloud and MIM 2016 on-premises activity in the following two areas:

* Self-service password registration and reset.
* Self-service group management (a.k.a. delegated group management).

To start using the above hybrid reports, you need to download and install a connector (a.k.a. reporting agent) to hook up MIM with Azure AD reports. This connector uploads data from service requests in MIM to your Azure AD tenant's reports. With this connector, you do not need to install the traditional on-premises Identity Manager reporting component infrastructure.

To download the connector package, proceed with the following steps:

1. Sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which you want to view or download a report.
3. Click **CONFIGURE**, and then scroll down to **identity manager reporting**.



1. Click **Download now**. The ZIP file (*HybridReportingInstaller.zip*) to download contains the MSI file of the connector (*MIMHybridReportingAgent.msi*) and a certificate used to authenticate to your Azure AD tenant in the cloud.
2. Copy the downloaded ZIP file to the server running MIM, install the connector by running it, accepting the license agreement, and restart MIM.

Et voilà! You can now start viewing the reporting data from **REPORTS**. As of this writing, you should toggle between the data sources (Azure AD or Identity Manager) using a drop-down list box.



Going forward, we plan to eliminate the drop-down box, and merge the data onto a single report.

Note If you want to turn off the uploading of reporting data from MIM, you can do this in the configuration file, located in your MIM installation folder, for example: *C:\Program Files\Microsoft Forefront Identity Manager\2010\Service\Microsoft.ResourceManagement.Service.exe.config*.

Note For more information, see the blog post [Azure AD and Microsoft Identity Manager reporting – we’ve gone hybrid!](http://blogs.technet.com/b/ad/archive/2015/05/22/azure-ad-and-microsoft-identity-manager-reporting-we-ve-gone-hybrid.aspx)[[230]](#footnote-230).

## Using Azure Multi-Factor Authentication

Global administrators of the Azure AD tenant can optionally choose to enable the [Azure Multi-Factor Authentication](http://azure.microsoft.com/en-us/services/multi-factor-authentication/)[[231]](#footnote-231) support in Azure AD to require employees to use a second-form of authentication when logging into the Cloud based and SaaS applications declared in the directory tenant (e.g. a mobile phone app, an automated phone call, or text message challenge) to enable even more secure identity access, and to protect the organization’s identity data in the cloud.

Interestingly enough, the Multi-Factor Authentication service composes really nice with the SaaS support you can literally set up secure support for any pre-integrated SaaS application (complete with multi-factor authentication support) to your entire enterprise within minutes.

Azure Multi-Factor Authentication service is a paid offering available as a stand-alone service with per user and per authentication billing options, or bundled with Azure AD Premium and Enterprise Mobility Suite (EMS).

Note For additional information, see [Multi-Factor Authentication Pricing Details](http://azure.microsoft.com/en-us/pricing/details/multi-factor-authentication/)[[232]](#footnote-232).

To leverage this service with:

* Cloud identities, follow the instructions outlined in the whitepaper [Leveraging Multi-Factor Authentication with Azure AD](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[233]](#footnote-233).

Note For more information, see Microsoft TechNet article [Using Multi-Factor Authentication with Azure AD](http://technet.microsoft.com/en-us/library/jj713614.aspx)[[234]](#footnote-234). You can also watch the Channel 9 demo video [Getting started with Azure Multi-Factor Authentication](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Getting-started-with-Azure-Multi-Factor-Authentication)[[235]](#footnote-235).

* Federated identities with AD FS in Windows Server 2012 R2, follow the instructions outlined in the whitepaper [Leveraging Multi-Factor Authentication Server on-premises](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[236]](#footnote-236).

## Leveraging the Privileged Identity Management service

The Privileged Identity Management (Azure AD PIM) feature improves your organization's cloud security posture by reducing risk from users who have access to highly-privileged roles, such as administrator roles in Azure AD and other services such as Office 365, Intune, and SaaS applications whose access is managed by Azure AD.

This service (currently in public preview as of this writing) is available in the new Azure portal at <https://portal.azure.com/>. The portal allows you to add the Privileged Identity Management tile to your Startboard.

Important note This service is only available when you enable the premium edition of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[237]](#footnote-237).

Today, most IT professionals enjoy permanent and unmonitored permissions to high-value resources. While this could be convenient, it poses major security concerns and makes their accounts high-value targets for security attacks. In many of the recent high-profile security breaches that made the headlines in the newspapers, an attacker simply found a way to compromise a user account that was permanently assigned to privileged roles.

The attacker was then able to use that account to access resources across the organization's network, in many cases going undetected for months. These network attacks are referred as to Advanced Persistent Threats (APT): “*a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time.*”[[238]](#footnote-238)

The Azure AD PIM service reduces this risk around access to these privileged roles by enabling you to:

* **Discover and monitor privileged roles**. The Azure AD PIM Dashboard gives you visibility into and tracking of users with privileged roles.
* **Automatically restrict the time** that users have these privileged permissions through on-demand "just in time (JIT)" activation of permissions for pre-configured time windows.
* **Monitor and track privileged operations** for audit purposes or security incident forensics.

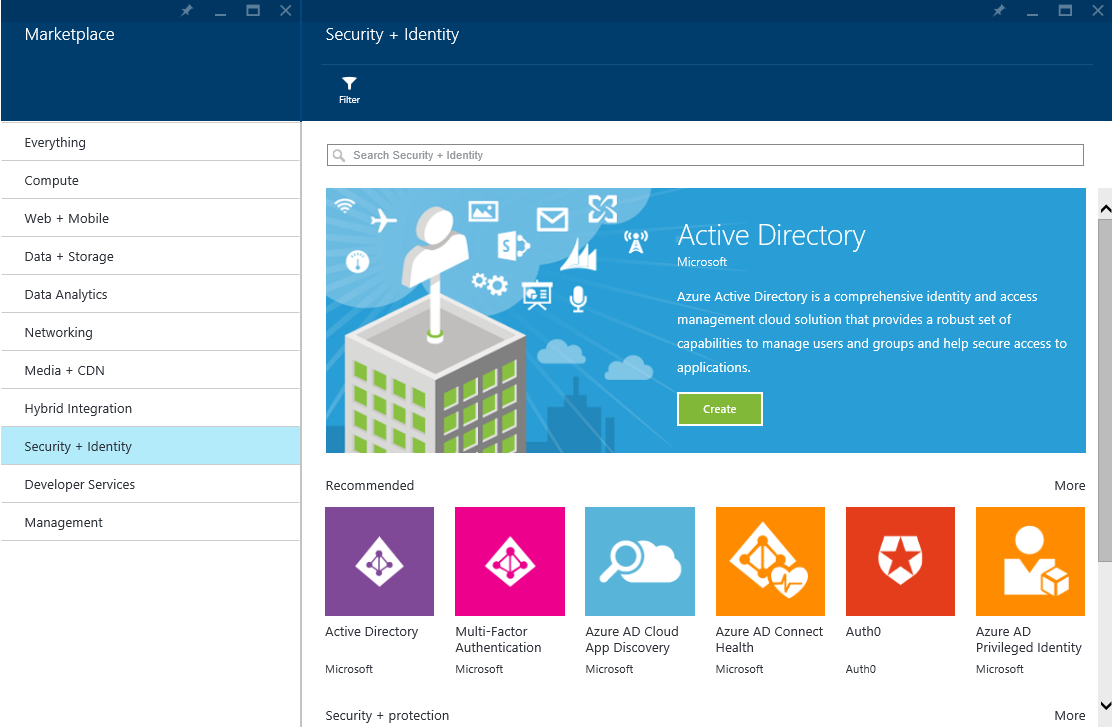
For the public preview, the Azure AD PIM service currently manages only the **built-in Azure AD privileged roles**, and their access to directory resources: Global administrator, Billing administrator, Service administrator, User administrator, Password administrator.

In upcoming releases, a bunch of new capabilities is going to be added, such as:

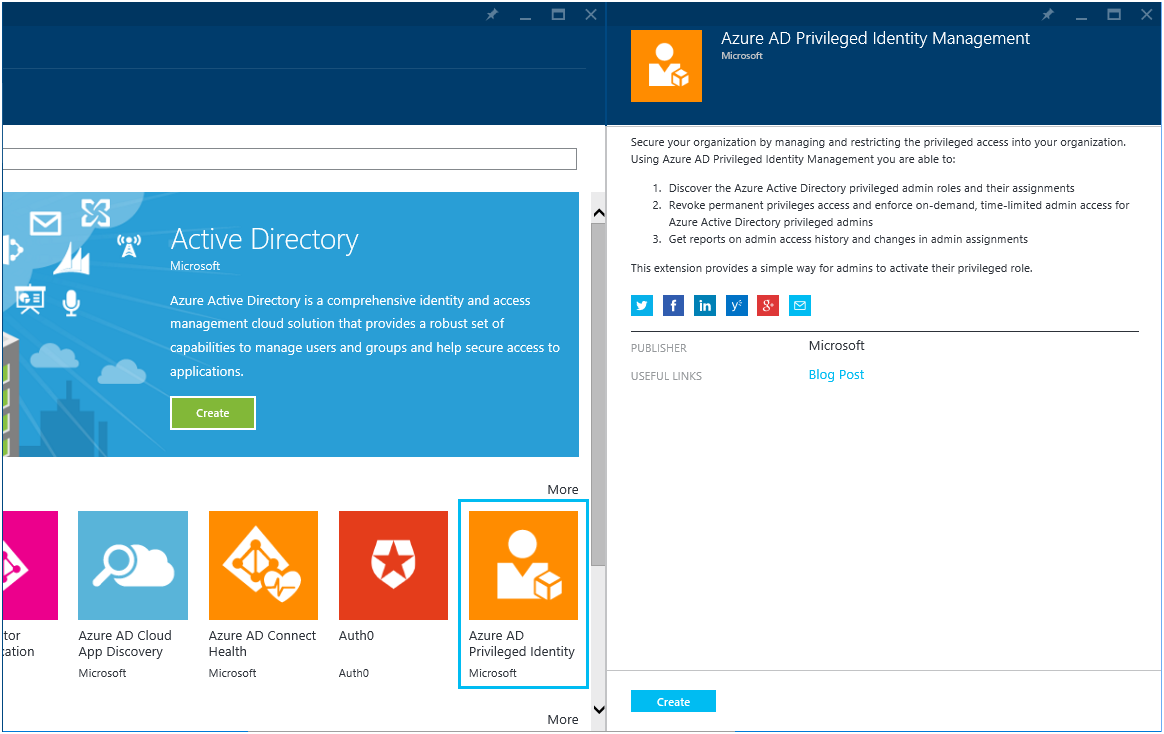
* Add **stronger workflow gates for activation**: Multi-Factor Authentication, human approval, and integration with ticketing systems
* Expanded management **coverage for additional privileged roles** and resources such as Office 365, Azure, and SaaS applications managed by Azure AD
* **Expose APIs** so you can to integrate your own workflow experiences.

To start using the Azure AD PIM, proceed with the following steps:

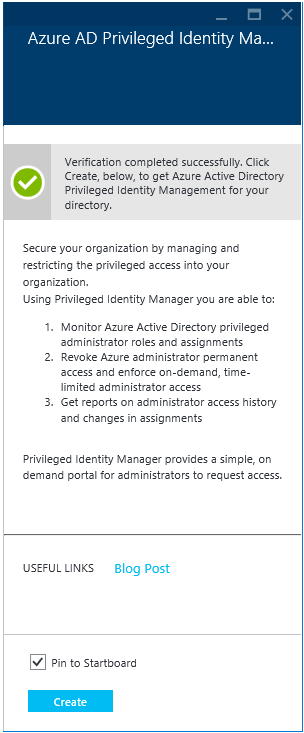
1. **Open** a browsing session and navigate to the new Azure Portal at <https://portal.azure.com/>.
2. **Click** **Sign in** and enter the credentials for a global administrator account of your organization that has a trial or paid subscription to Azure AD Premium.
3. Select **Marketplace**, and then select **Security + Identity**, or search for it by typing “*Identity*”.



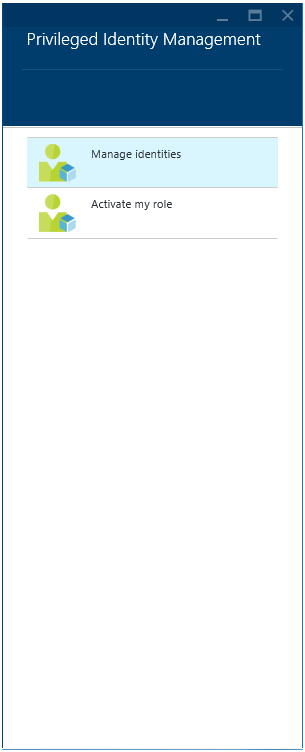
1. Click **Azure AD Privileged Identity**. An introductory blade opens up.



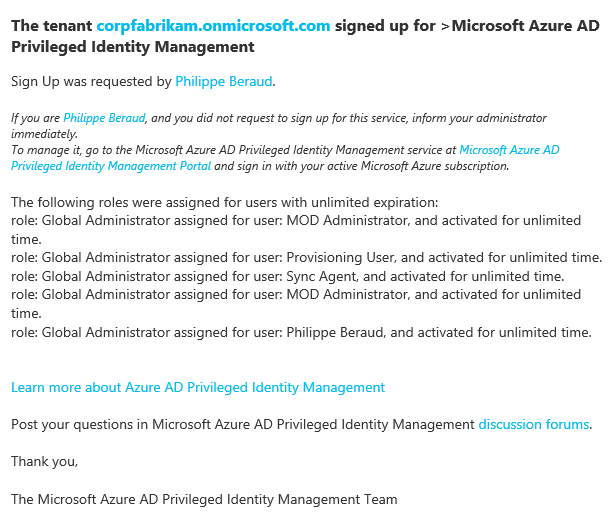
1. Click **Create**. This will open another blade.



1. Once verification is completed, click **Create** once again.



1. Once provisioned, you will receive in parallel a signup notification mail.

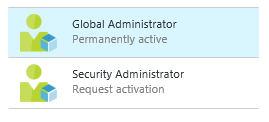


Note As the first global administrator who initiates access to this preview, you’re automatically assigned to the security administrator role, which is a new role used to manage privileged identities. You can add other users to the security administrator role.

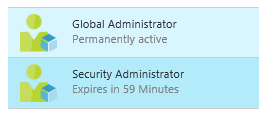
1. At this stage, you are ready to begin managing privileged identities. Click **Activate my role** to activate your membership.

Note The basic model is that that a privileged role is assigned to candidate members, who in turn activate their membership in the role on-demand and for a limited pre-configured time. Since the security administrator role is a privileged role, and in order to begin managing privileged identities.

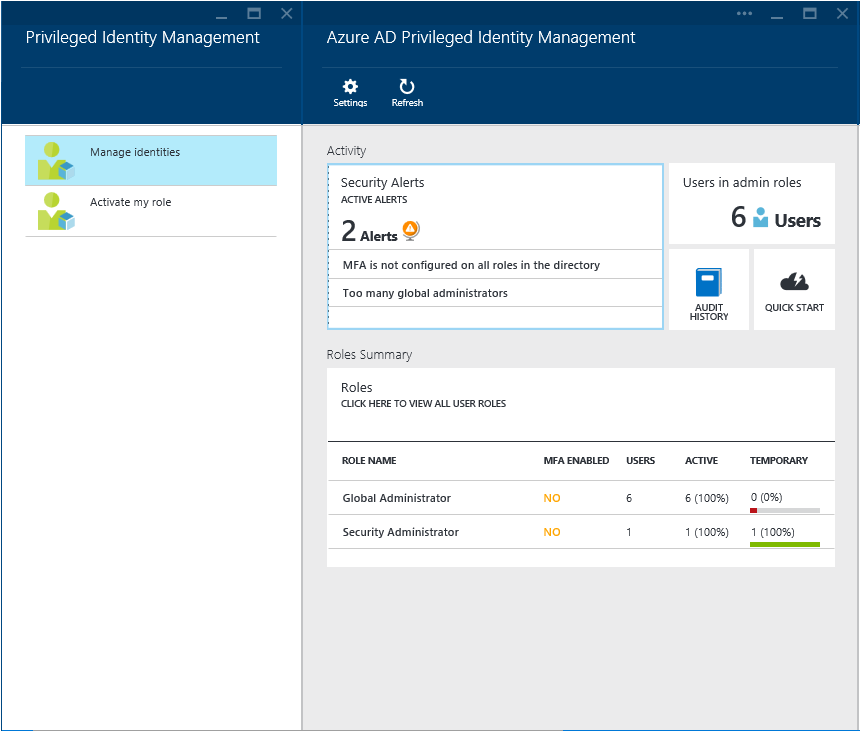
A list of roles assigned to you: the global administrator role with "permanent activation" and the new security administrator for which you need to "request activation". The security administrator manages the other privileged identities.



1. Click **Security Administrator**, and the **Make active…** Finish the wizard to request activation for the security administrator role.



1. Click **Manage identities** in the **Privileged Identity Management** blade. A new blade opens up.



For each privileged role, you can see how many users are assigned to that role, how many of these assignments are currently **active** and how many are **permanently** active. The blade also shows a summary of the security alerts. For instance, if there are too many permanent assignments, it shows an alert as illustrated above for the global administrators.

Azure AD PIM provides a self-service experience for administrators.

The privileged identities managed by the service are regular users until they’re activated into their assigned privileged role. Users must activate the privileged role to which they’ve been assigned. After activation, they can complete privileged operations until their access to the privileged role expires.

In today's preview, when a user submits an activation request, the request is logged in the system. The request is immediately auto-approved, and the role is activated for the time period that is pre-configured for the role (this time period for the role can be configured by the security administrator).

Capabilities will be added so that you can secure the activation for a role even further by using security gates such as Azure Multi-Factor Authentication (MFA), human approval, or validation of an incident ticket assigned to the requesting user.

Note For more information, see the blog post [Azure Cloud App Discovery GA and our new Privileged Identity Management service](http://blogs.technet.com/b/ad/archive/2015/05/04/azure-cloud-app-discovery-ga-and-our-new-privileged-identity-management-service.aspx)[[239]](#footnote-239). You can also watch the Channel 9 demo video [Azure AD Privileged Identity Management](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Azure-AD-Privileged-Identity-Management)[[240]](#footnote-240).

# Empowering users

In terms of end-users’ experience that Azure AD provides single sign-on to thousands of application hosted in any cloud and on-premises, self-service capabilities that can boost productivity from a customizable user friendly environment accessible from every device. This is notably accomplished through the Azure AD Access Panel.

Note As an introduction, you can watch the Channel 9 demo video [First day at work with Azure Active Directory](http://channel9.msdn.com/Blogs/Windows-Azure/How-to-configure-self-service-password-reset-for-users-in-Windows-Azure-AD)[[241]](#footnote-241).

## Using the Azure AD Access Panel

The Azure AD Access Panel allows an end user with an organizational account in Azure AD to view and launch applications that have been assigned to them by their administrator of their tenant (plus any applications that they have consented to).

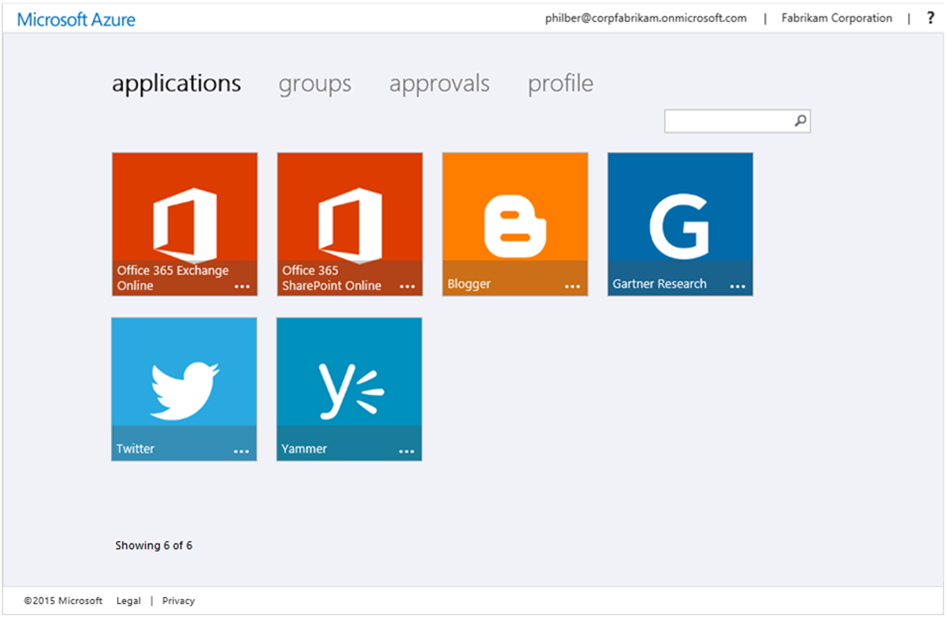
In other words, this is a single screen with assigned SaaS applications for every user, and where they can discover which applications they have, single sign-on to those applications, and in some cases manage their application credentials.

The Azure AD Access Panel is a web-based portal available at <http://myapps.microsoft.com>[[242]](#footnote-242).

Note The Access Panel is separate from the Azure Management Portal and does not require users to have an Azure subscription.

To use the Azure AD Access Panel with your organizational account, proceed with the following steps:

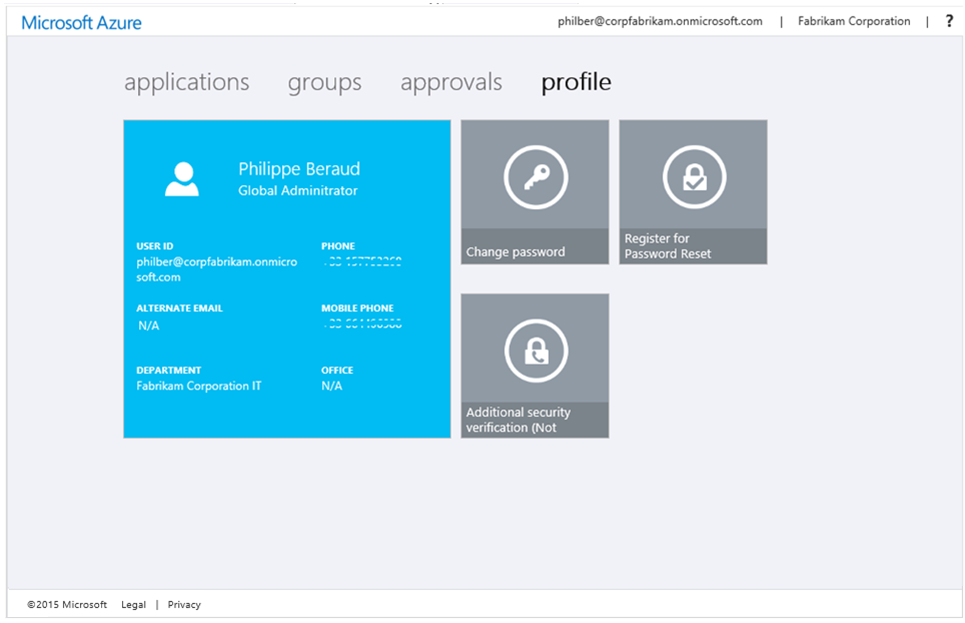
1. Open a browsing session and navigate to the Azure AD Access Panel.
2. In the sign in page, enter the credential for your organizational account in your directory. Once authenticated, you’re redirected to the Azure AD Access Panel.



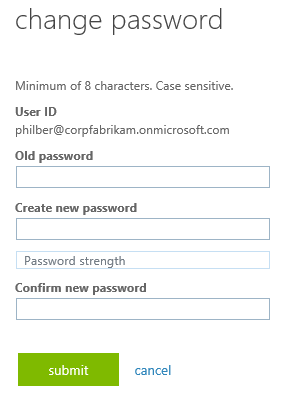
## Editing the profile settings for the users

The Azure AD Access Panel allows users to edit some of their profile settings, including the ability to:

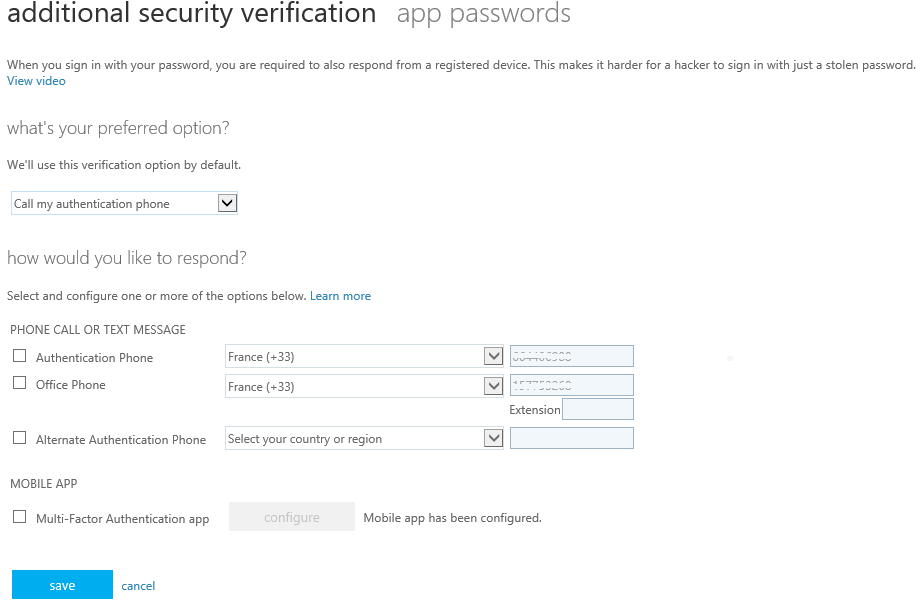
* **View the details about their account**, such as their User ID, alternate email, mobile and office phone numbers.



* **Change their password** associated with their organizational account via **Change password**.



* **Edit multi-factor authentication (MFA) related contact and preference settings** - for those accounts that have been required to use it by an administrator – via **Additional security verification** (See section § Using Azure Multi-Factor Authentication earlier in this document). This requires the Premium editions of Azure AD).



And with Basic and Premium editions of Azure AD:

* **Self-register for password reset**. See next section.
* **Self-manage the groups**. See section § Self-service group management for users later in this document.
* **Self-service for application access**. See section § Self-service for application access later in this document.

## Self-service password reset for cloud users

Self-service password reset for users allows end users in your organization to reset their passwords automatically without calling an administrator or helpdesk for support.

Important note This feature is only available when you enable the Basic or the Premium editions of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[243]](#footnote-243).

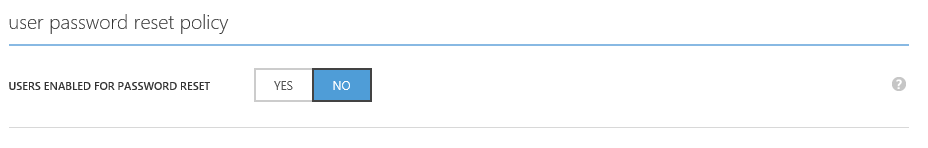
This feature is comprised of the following components:

* **Password reset policy configuration portal**. Administrators can control different facets of user password reset policy in the classic Azure management portal in the **CONFIGURE** page of the directory (see below).
* **User registration portal**. Users can self-register for password reset with the administrator-controlled password reset policy through the Azure AD Access Panel at <https://account.activedirectory.windowsazure.com/PasswordReset/Register.aspx>. This requires an office phone and/or a mobile phone as contact data.
* **User password reset portal**. Users can reset their own passwords - using a number of different challenges in accordance with the administrator-controlled password reset policy - via a **Can’t access your account?** link available from any web page, which uses an organizational account for sign in. Clicking the link will launch a launch a self-service password reset wizard.

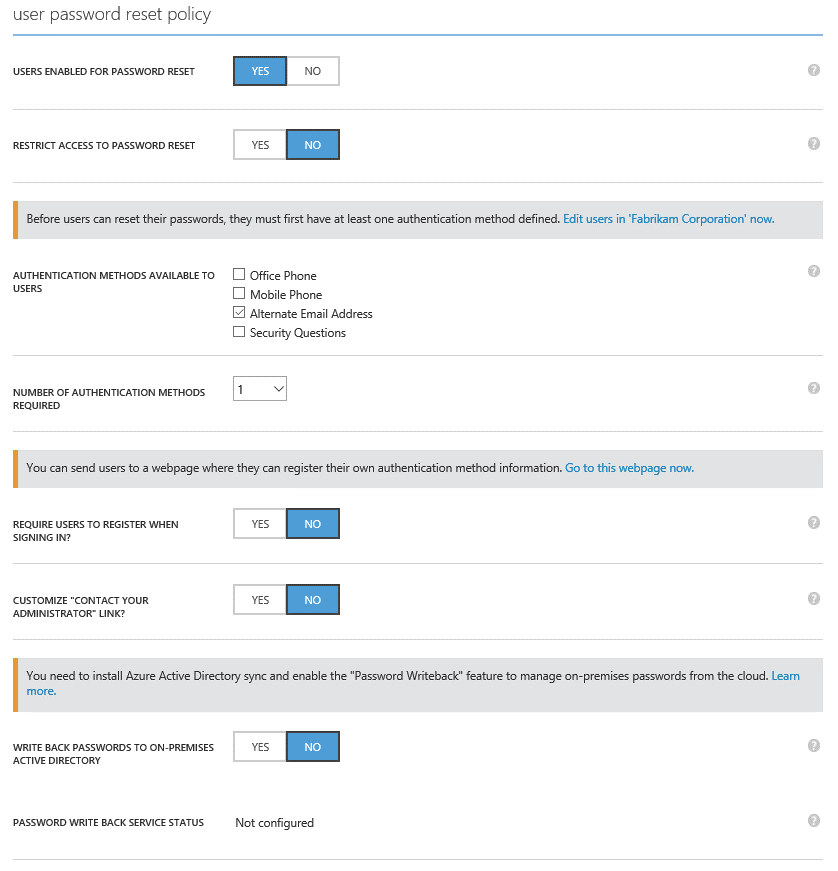
### Activating the password reset policy

To activate the password reset policy for cloud users, proceed with the following steps:

1. Sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which a user password reset policy should be defined.
3. Click **CONFIGURE** and scroll down to **user password reset policy**.



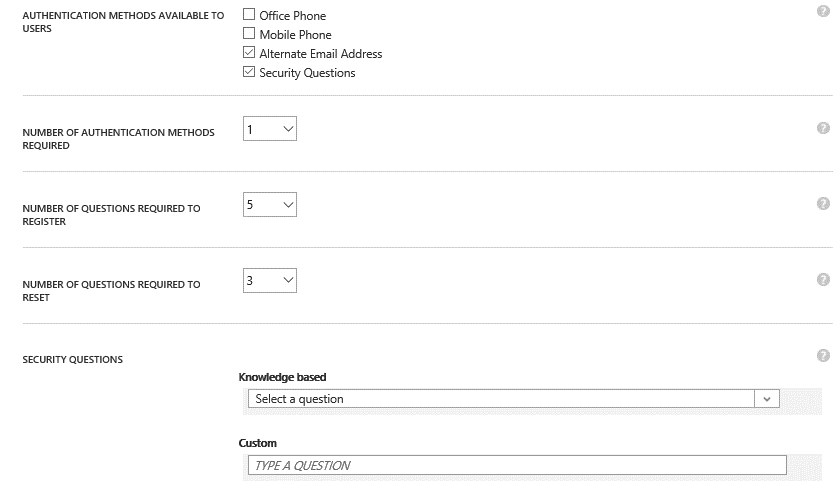
1. Set **USERS ENABLED FOR PASSWORD RESET** to **YES**. This setting reveals several more controls which enable you to configure how this feature works in your directory. As indicated, this setting requires that the user accounts have been configured with Office and/or Mobile phones for verification.



1. Review the available settings such as **AUTHENTICATION METHODS AVAILABLE TO USERS** that enables you to require the addition of an Office and/or Mobile phone number and/or security questions the first time a user signs in to Azure AD.

Enabling security questions provides the ability for IT professionals to require users to provide answers to a specified amount of questions to register for the password reset feature. Once registered the user will need to answer the questions for verification in order to reset their password:

* + **NUMBER OF QUESTIONS REQUIRED TO REGISTER** defines the minimum number of security questions a user must select and answer when registering for password reset.
  + **NUMBER OF QUESTIONS REQUIRED TO RESET** defines the number of randomly-selected security questions a user must answer when resetting a password.

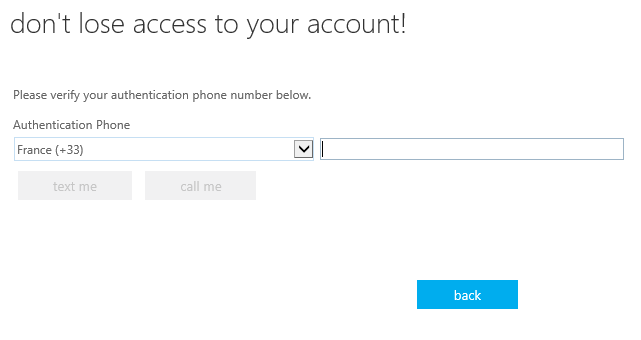


1. After configuring user password reset policy as desired for your tenant, click **SAVE** in the tray of the bottom.

### Adding user contact

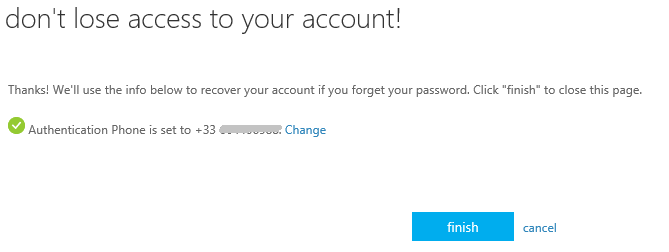
To add user contact via the user registration portal, proceed with the following steps:

1. Navigate to the user registration page in the Azure AD Access Panel at <https://account.activedirectory.windowsazure.com/PasswordReset/Register.aspx> and sign in with your organizational account.



1. Under **Mobile Phone**, specify a country code and phone number and click **text me** respectively **call me** to receive a verification text message respectively a verification phone call.

After verifying a phone number, the user’s profile will be updated with the number provided.

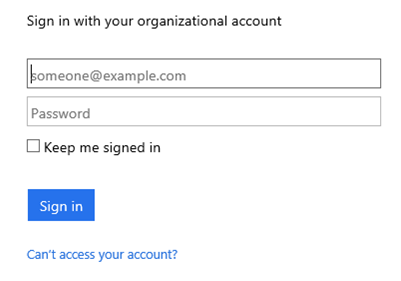


1. Click **all done!**

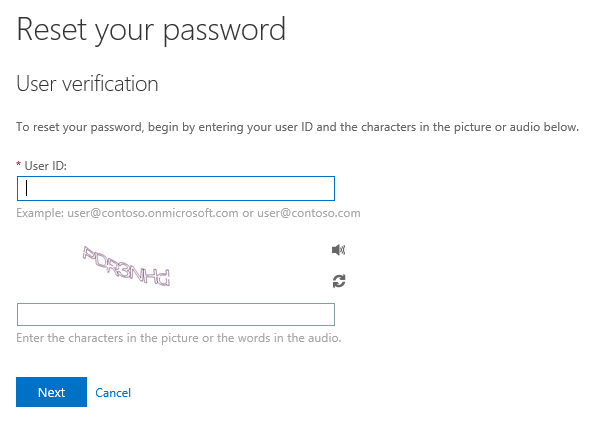
### Performing a self-service password reset

To perform a self-service password reset, proceed with the following steps:

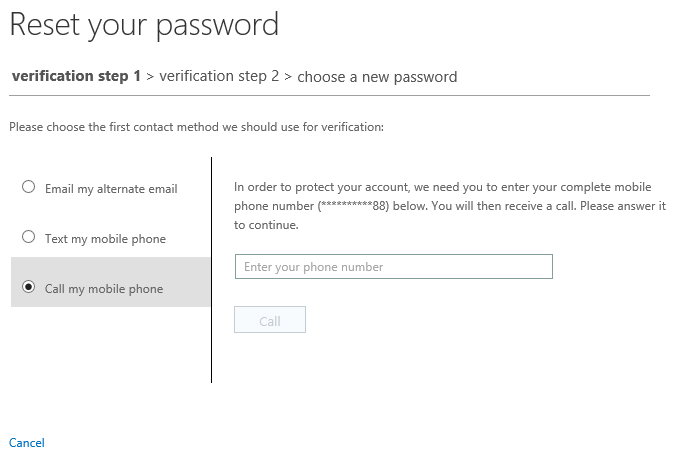
1. Navigate to a page that uses an organizational account.



1. Click **Can’t access your account link?**. You’re redirected to a **Reset your password** page at <https://passwordreset.microsoftonline.com> with you context as a query string.



1. Specify your user ID, for example “*philber@corpfabrikam.onmicrosoft.com*” as illustrated hereafter, pass the captcha, and then click **Next**.



1. You can view and read the password reset instructions page. Click **Next** to proceed with the verification step(s). Once you’ve met the requirements of the organizational policy, you are allowed to choose a new password. The password is validated based on the password policy of the tenant, and a strength validator appears to indicate to the user whether the password entered meets that policy.
2. Once you provide matching passwords that meet the organizational policy, your password is reset and you can log in with your new password immediately.

Note For more information, see the Microsoft TechNet article [Enable self-service password reset for users](http://technet.microsoft.com/en-us/library/dn510386.aspx)[[244]](#footnote-244). You can also watch the Channel 9 demo video [Azure Active Directory Premium Self-Service Password Reset w/write-back](http://channel9.msdn.com/Blogs/Windows-Azure/How-to-configure-self-service-password-reset-for-users-in-Windows-Azure-AD)[[245]](#footnote-245).

## Self-service group management for users

Self-service group management, a.k.a. delegated group management, enables users to create and manage security groups in Azure AD and offers users the possibility to request security group memberships, which can subsequently be approved or denied by the owner of the group. By using self-service group management features, the day-to-day control of group membership can be delegated to people who understand the business context for that membership.

Important note This feature is only available when you enable the Basic or the Premium editions of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[246]](#footnote-246).

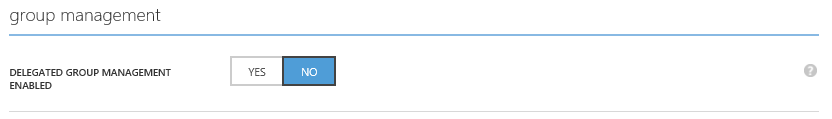
**This capability can notably serve to delegate the access management of an application to a business owner**. For that purpose, an IT professional can assign access for the application to a new group that the business owner has created. The business owner can then manage the group membership.

Note For more information, see the Microsoft TechNet article [Self-service group management for users](http://technet.microsoft.com/en-us/library/dn510386.aspx)[[247]](#footnote-247). You can also watch the Channel 9 demo video [Delegated Group Management on Azure Active Directory Premium](https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Delegated-Group-Management-on-Azure-Active-Directrory-Premium)[[248]](#footnote-248).

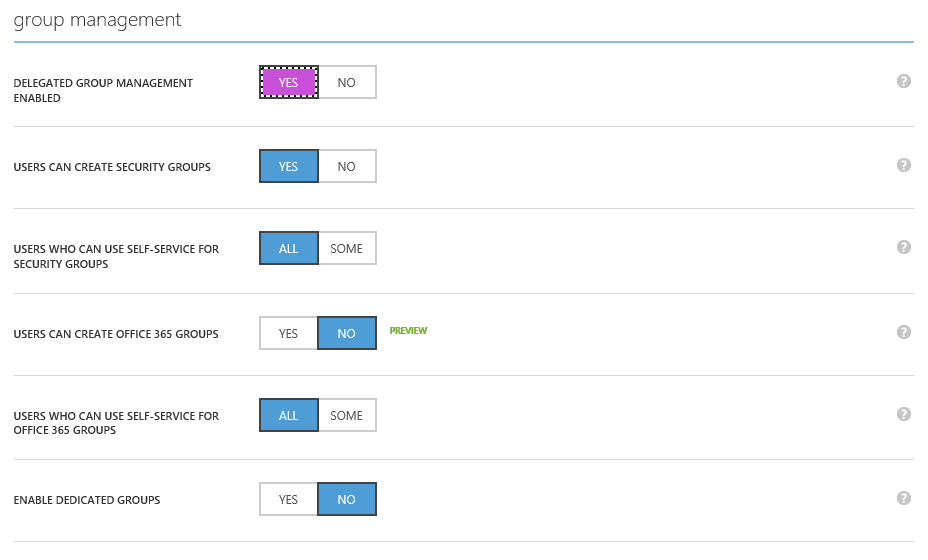
### Enabling the capability

To activate the self-service group management for users, proceed with the following steps:

1. Sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which self-service group management should be enabled.
3. Click **CONFIGURE** and scroll down to **group management**.



1. Click **YES** to enable the delegated group management through the Azure AD Access Panel. This setting reveals additional controls which enable you to configure how this feature works in your directory, for example:
   * **Users who can use self-service for security groups** allows to restrict security group management to a limited group of users
   * **Users who can use self-service for Office 365 groups** allows to restrict Office365 group management to a limited group of users



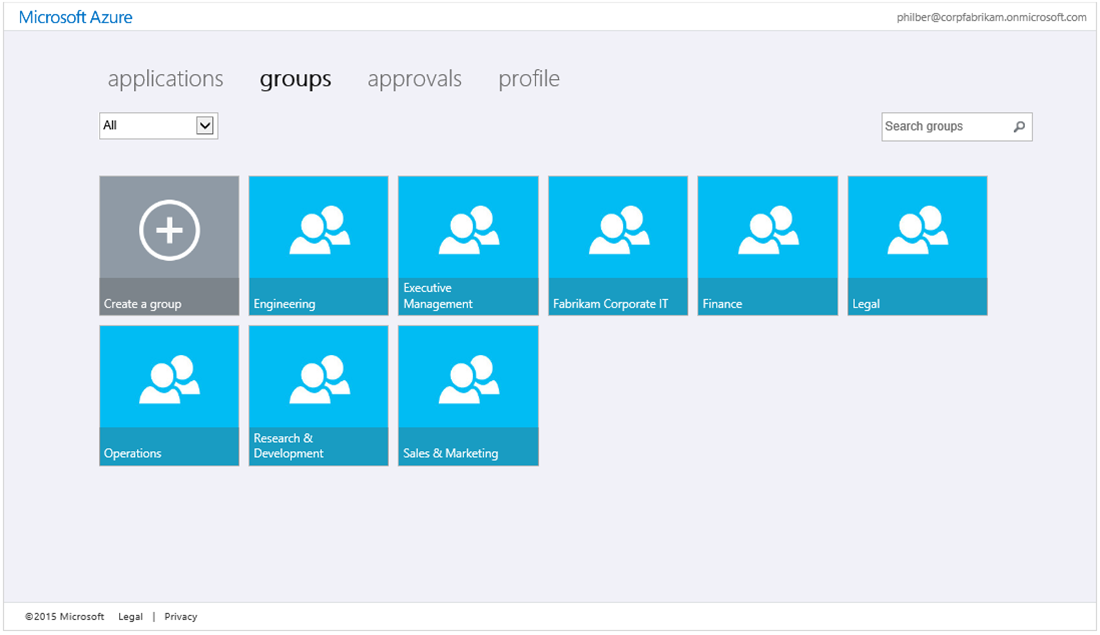
1. By default, and once activated, users can create new groups through the Azure AD Access Panel. Click **NO** if you don’t want to offer this ability. Likewise, no restriction applies to the security group management. Click **YES** if you want to restrict it to a limited group of users.
2. After configuring the self-service group management capability as desired for your tenant, click **SAVE** in the tray of the bottom.

Once Self-service group management has been enabled for the directory, it is made available to users through the Azure AD Access Panel via the **groups** and **approvals** tabs.

### Performing self-service group management

To manage your groups in the Azure AD Access Panel, proceed with the following steps:

1. Open a browsing session and navigate to the Azure AD Access Panel at <https://myapps.microsoft.com>.
2. Sign-in with your user’s credentials. The Azure AD Access Panel shows up.
3. Click **Groups**.

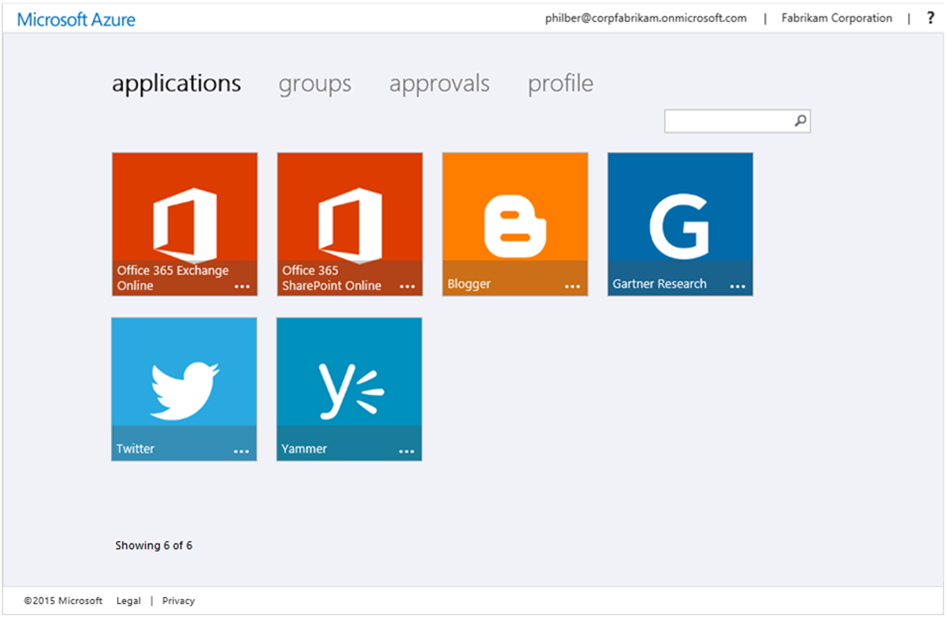


1. You can then self-manage the groups: create, edit, leave, or delete a group, manage group members, request group membership, and manage group membership requests.

Note For more information, see the Microsoft TechNet article [Manage your groups](http://msdn.microsoft.com/en-us/library/azure/dn641268.aspx)[[249]](#footnote-249).

## Accessing applications from the Azure AD Access Panel

All the applications assigned to a user or (dynamic) groups they belong to appear as a tile on the Azure AD Access Panel.

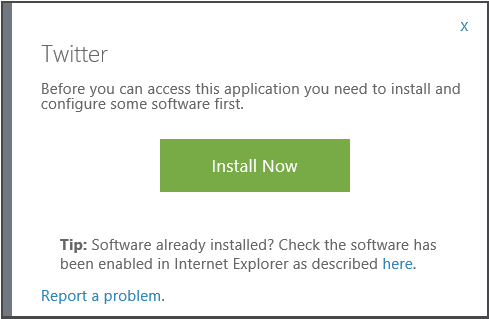


#### Accessing applications configured with federation-based single sign-on

When a user clicks on an application tile that has been configured for federation-based single sign-on for one of these applications, they are redirected to that application and automatically signed in. The **user account information from Azure AD is being used in this context.**

#### Accessing applications configured with password-based single sign-on

The first time a user clicks on an application that has been configured for password-based single sign-on, and if not already done for another similar application, they will be prompted to install an Azure AD Access Panel Extension plugin for Internet Explorer, Chrome or Firefox. This extension is needed to support the password-based single sign-on functionality.

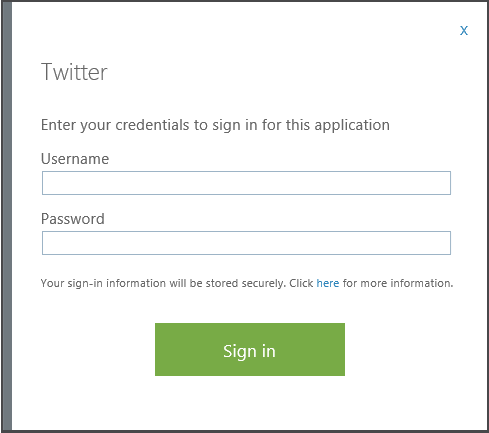


They will have to follow the browser specific instructions. The setup of the Azure AD Access Panel Extension (*Access Panel Extension.msi*) plugin may require restarting of their web browser.



When they are returned to the Azure AD Access Panel and click on the application tile again, they will be prompted for a username and password for the application.

Note If you have assigned credentials for this user, they will not need to perform this step and instead will be redirected and signed to the application.



Once the username and password are entered, these credentials will be securely stored in Azure AD and linked to their account in Azure AD, and the Access Panel will automate signing the user in to the application using those credentials.

The next time a user clicks on the application tile, they will be automatically signed into the application without needing to enter the credentials again and without needing to install the Password single sign-on plugin again.

If a user’s credentials have changed in the target third-party application, then the user must also update their credentials which are stored in Azure AD. To update credentials, a user must select the icon in the lower-right of the application tile, and select **update credentials** to re-enter the username and password for that application.

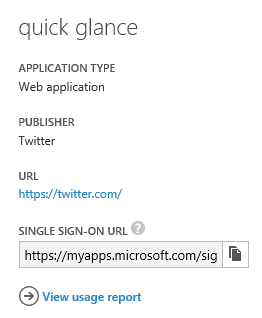
### Accessing applications from direct single sign-on links

Many applications that support federation-based single sign-on with Azure AD already support the ability for users to sign in directly at the application without first loading the Azure AD Access Panel. (In the federation terminology, this is known as service provider initiated federation).

However, applications that are configured to use an alternate sign-in method, such as password-based single sign-on, required to be launched from the Azure AD Access Panel.

Direct single sign-on links to individual applications are available. Technically speaking, such links are specifically-crafted URLs that send a user through the Azure AD sign in process for a specific application without requiring the user to load the Azure AD Access Panel.

These specific direct single sign-on URLs are specified in **SINGLE SIGN-ON URL** under the **DASHBOARD** tab of any pre-integrated application in the **ACTIVE DIRECTORY** section of the classic Azure management portal as illustrated hereafter.



These links can be copied and pasted anywhere you want to provide a sign-in link to the considered application. Here's an example of such an URL for Twitter:

*https://myapps.microsoft.com/signin/Twitter/230848d52c8745d4b05a60d29a40fced*

These links use the same access control mechanisms as the Azure AD Access Panel, and only those users or groups who have been assigned to the application in the Azure management portal will be able to successfully authenticate. However, any user who is unauthorized will see a message explaining that they have not been granted access, and are given a link to load the Access Panel to view available applications for which they do have access.

Note For more information, see the blog post [Customize Your App SSO Experience with Azure AD](http://blogs.technet.com/b/ad/archive/2014/10/30/customize-your-app-sso-experience-with-azure-ad.aspx)[[250]](#footnote-250).

## Self-service for application access

With an ever growing list of applications added to your Azure AD tenant, you may become over whelmed with requests from their employees to get access to a specific application.

Self-Service for Application Access allows users to request access to an application using a **Get more applications** tile in the Azure AD access panel. This capability is supported for all application that support federated or password-based single sign-on.

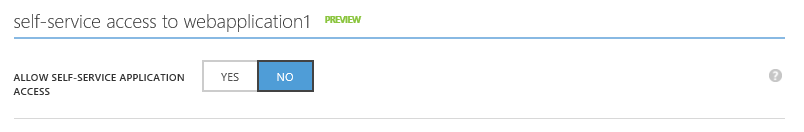
Enabling the feature allows you to:

* Set which applications users can request access to.
* Create an approval policy if needed.
* Specify who should approve requests for specific applications: an approver can be any user in the organization with an Azure AD account.

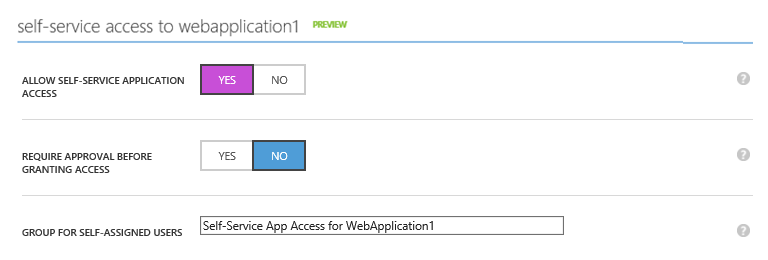
Note For more information and instructions on how to enable the feature, see the blog post [Employee Self-Service App Access for Azure AD now in preview!](http://blogs.technet.com/b/ad/archive/2015/04/23/employee-self-service-app-access-for-azure-ad-now-in-preview.aspx)[[251]](#footnote-251).

To enable users to request access to an application, proceed with the following steps:

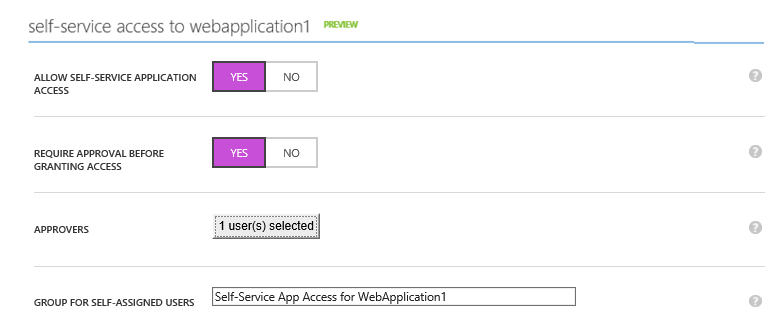
1. Sign into the classic Azure management portal as the administrator of the directory you wish to configure.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which self-service group management should be enabled.
3. Click **APPLICATIONS,** and then click the name of the application.
4. Click CONFIGURE and scroll down to **self-service access**.



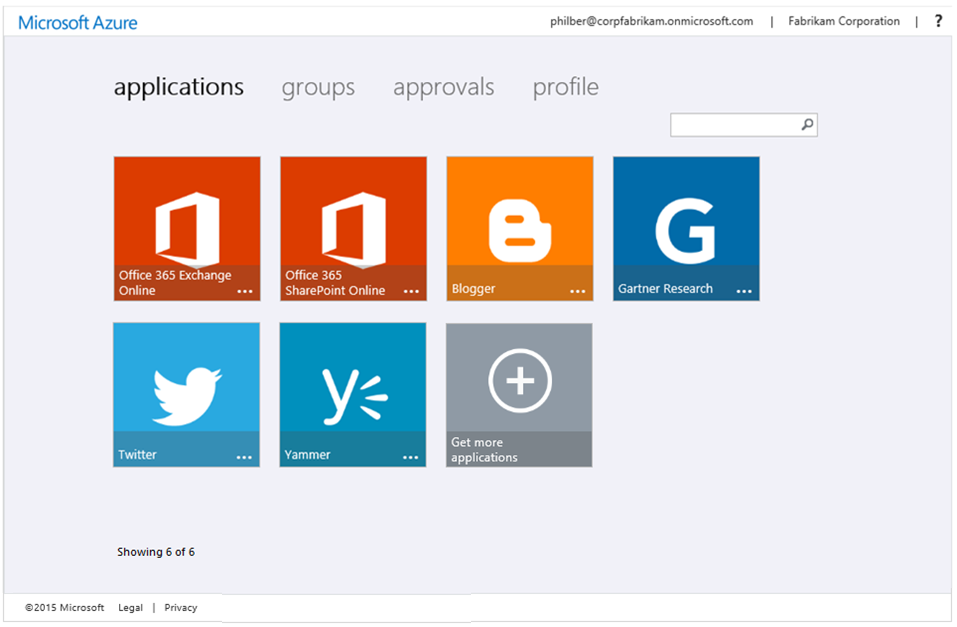
1. Set **ALLOW SELF-SERVICE APPLICATION ACCESS** to **YES**.



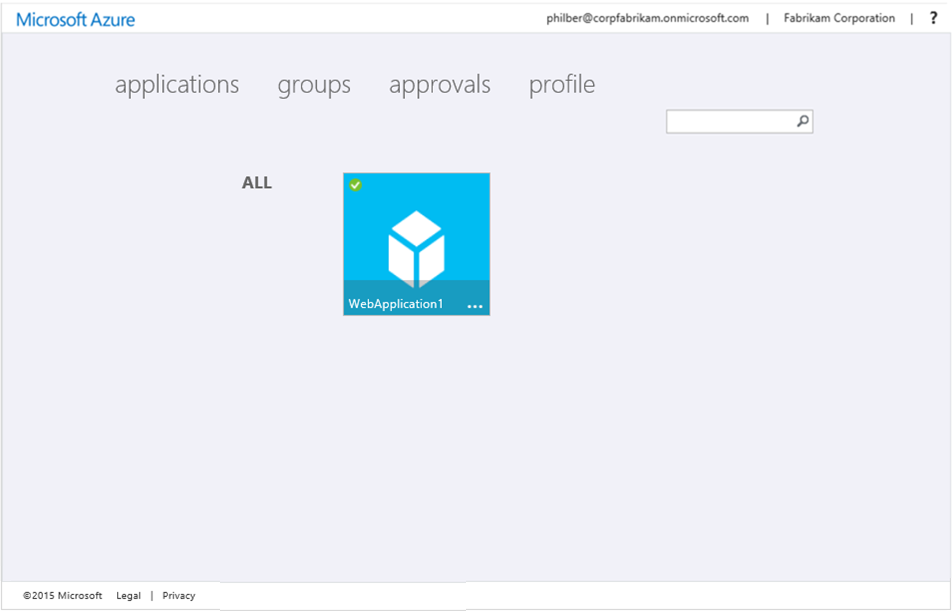
1. To optionally configure an approval workflow for access requests, set **REQUIRE APPROVAL BEFORE GRANTING REQUEST** to **YES**. Then one or more approvers can be selected using the **APPROVERS** button.



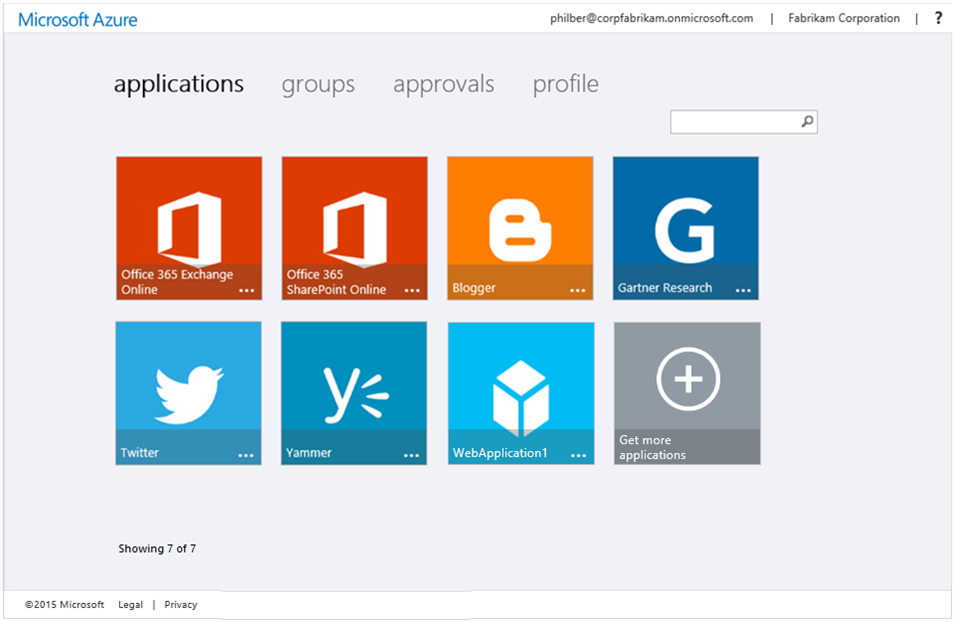
1. Click **SAVE** at the bottom of the tray. Users will be allowed to self-assign access to this application in the Azure AD Access Panel
2. Back to the Azure AD Access Panel, an additional tile **Get More applications** is now displayed.



1. Click **Get More applications**.



1. Click **WebApplication1** that has been enabled for self-service.
2. Et voilà!



## Customizing the Azure AD Access Panel (and the Sign-in page)

Administrators can customize how the Azure AD Access Panel and the sign-in page will appear to users within an organization. More specifically, administrators can brand these pages to include their company’s logo and customize other on-screen elements.

Important note This feature is only available when you enable the Basic or the Premium edition of Azure AD. For more information, see the Microsoft TechNet article [Azure Active Directory Editions](http://technet.microsoft.com/en-us/library/dn532272.aspx)[[252]](#footnote-252).

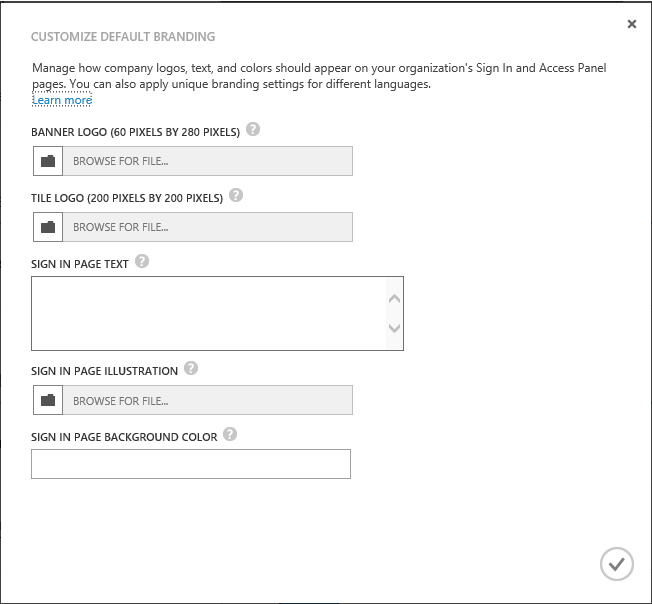
To customize the Azure AD Access Panel, proceed with the following steps:

1. Sign into the classic Azure management portal as the administrator of the directory you wish to customize.
2. Click **ACTIVE DIRECTORY**, and then click the name of the organization’s directory for which the Access Panel should be customized.
3. Click **CONFIGURE**.

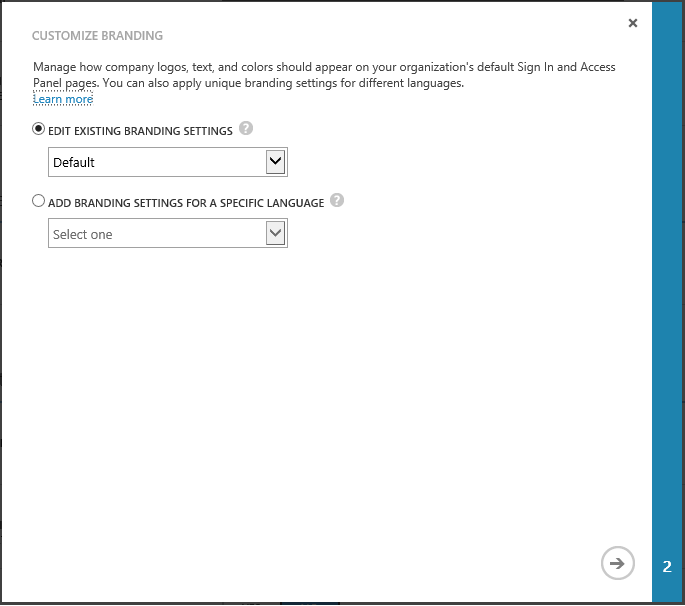


Important note You have to assign a Basic or a Premium license to the administrator of the directory to see the above Customize Branding button.

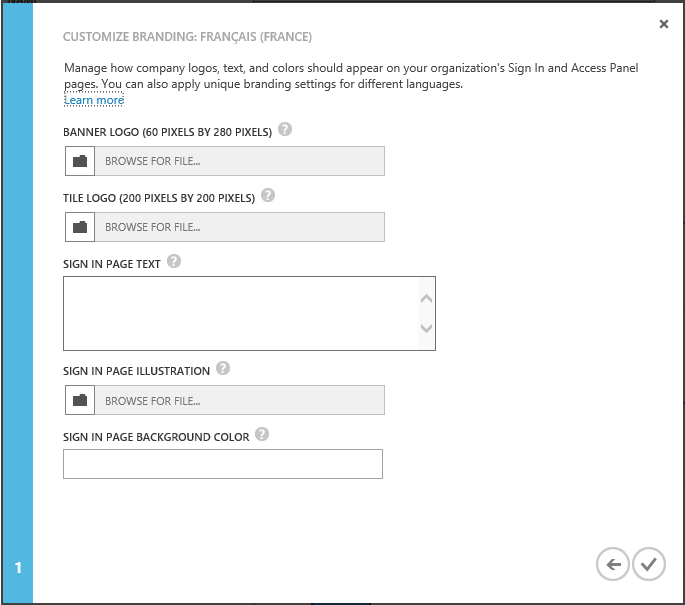
1. On the **CONFIGURE** page, under **directory properties**, next to **SIGN IN AND ACCESS PANEL PAGE APPEARANCE**, click **Customize Branding**. A **CUSTOMIZED DEFAULT BRANDING** dialog brings up for the directory.



1. Review the options that can be customized, set your branding settings accordingly, and then click the check mark icon to commit your changes.
2. As indicated, you can apply your unique branding settings for different languages once default branding settings have been defined. Click **Customize Branding** again.



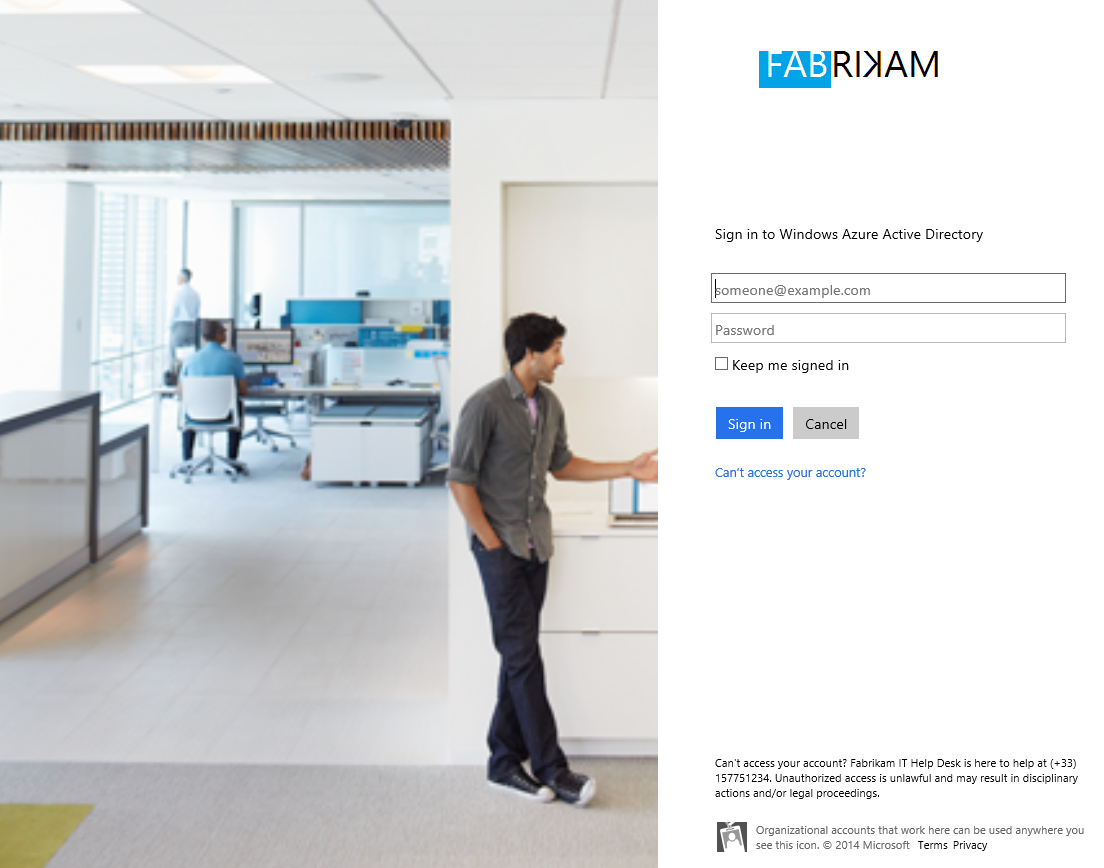
1. Select **ADD BRANDING SETTINGS FOR A SPECIFIC LANGUAGE**, specify the language in the drop-down list, for example **Français (France)** as illustrated hereafter, and then click the arrow.



1. Set your branding settings for the specific language, and then click the check mark icon to commit your changes.

Note For more information, see the Microsoft TechNet article [Add company branding to your Sign In and Access Panel pages](http://technet.microsoft.com/en-us/library/dn532270.aspx)[[253]](#footnote-253).

1. Open a private browsing session, navigate to the Azure AD Access Panel at <https://myapps.microsoft.com> by appending one of the active or verified domain names configured for your directory to the end of the URL, for example <http://myapps.microsoft.com/corpfabrikam.onmicrosoft.com>. Your branding settings should be reflected in the user interface.



Similar to the above organization-specific URL for the Azure AD Access Panel, you can also customize the direct single sign-on links (see section § Accessing applications from direct single sign-on links) by adding one of the active or verified domain names configured for your directory after the *myapps.microsoft.com* domain. This ensures any organizational branding is loaded immediately on the sign-in page without the user needing to enter their user ID first:

*https://myapps.microsoft.com/corpfabrikam.onmicrosoft.com/signin/Twitter/230848d52c8745d4b05a60d29a40f*

When an authorized user clicks one of these application-specific links, they first see their organizational sign-in page (as shown above assuming they are not already signed in), and after sign-in, they are redirected to their application without stopping at the Azure AD Access Panel first. If the user is missing pre-requisites to access the application, such as the password-based single sign-on browser plugin, then the link will prompt the user to install the missing extension.

## Using the “My Apps” mobile applications

Since the major mobile platforms don't support the browser plugins as notably used by the Azure AD Access Panel (e.g. the password-based single sign-on browser plugins), a "My Apps" mobile application is also available to help users access their apps on their mobile devices.

The "My Apps" application is optimized for your mobile device and supports all of the features of the Azure AD Access Panel.

"My Apps" is available as of today for both the iOS and Android platforms:

* My Apps for Android works on any device running Android version 4.1 or higher, and is available in the [Google Play store](https://play.google.com/store/apps/details?id=com.microsoft.myapps)[[254]](#footnote-254).
* My Apps for iOS is supported on any iPhone or iPad running iOS version 7 and up, and is available in the [Apple App Store](https://itunes.apple.com/us/app/my-apps-windows-azure-active/id824048653?mt=8)[[255]](#footnote-255).

To use “My Apps” with your organizational account, proceed with the following steps:

1. Download, install and launch the app.
2. Sign in using your organizational account in your directory.
3. Like the Azure AD Access Panel, select the app you want to sign into. Your app launches immediately inside the "My Apps" web browser, no other sign in required.

You can also change your organizational password, or edit your multi-factor authentication settings (if configured) from inside the “My Apps” app.

Note For more information, see the blog post [Accessing Azure AD connected apps on Android phones, iPhones, and iPads](http://technet.microsoft.com/en-us/library/dn532270.aspx)[[256]](#footnote-256).

**This concludes this paper. We hope that you now have a better overview of what is Azure AD and the various benefits it can provide as an IdMaaS solution in the cloud.**

|  |
| --- |
| 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.  © 2016 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. Modern business applications: http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx [↑](#footnote-ref-1)
2. 2013 Planning Guide: Identity and Privacy: http://www.gartner.com/id=2221415 [↑](#footnote-ref-2)
3. Identity Management as a Service: http://www.identityblog.com/?p=1205 [↑](#footnote-ref-3)
4. Active Directory from on-premises to the cloud – Azure AD whitepapers: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-4)
5. Getting started with app access enhancements for Azure AD: http://blogs.technet.com/b/ad/archive/2013/08/14/getting-started-with-app-access-enhancements-for-windows-azure-ad.aspx [↑](#footnote-ref-5)
6. Getting started with Azure AD: http://msdn.microsoft.com/en-us/library/dn655157.aspx [↑](#footnote-ref-6)
7. Azure Active Directory community forum: http://social.msdn.microsoft.com/Forums/en-US/WindowsAzureAD/ [↑](#footnote-ref-7)
8. Azure blog: http://blogs.msdn.com/b/windowsazure/ [↑](#footnote-ref-8)
9. Reimaging Active Directory for the Social Enterprise (Part 1): http://blogs.msdn.com/b/windowsazure/archive/2012/05/23/reimagining-active-directory-for-the-social-enterprise-part-1.aspx [↑](#footnote-ref-9)
10. Reimaging Active Directory for the Social Enterprise (Part 2): http://blogs.msdn.com/b/windowsazure/archive/2012/06/20/reimagining-active-directory-for-the-social-enterprise-part-2.aspx [↑](#footnote-ref-10)
11. Modern business applications: http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx [↑](#footnote-ref-11)
12. Microsoft by the Numbers: The Enterprise Cloud (October 2014): http://news.microsoft.com/cloud/ms\_numbers.pdf [↑](#footnote-ref-12)
13. Jason Zander and Joe Belfiore: TechEd Europe 2014: http://news.microsoft.com/speeches/jason-zander-and-joe-belfiore-teched-europe-2014/ [↑](#footnote-ref-13)
14. Azure AD is live in Hong Kong!: http://blogs.technet.com/b/ad/archive/2014/10/06/azure-ad-now-live-in-hong-kong.aspx [↑](#footnote-ref-14)
15. Azure AD: Under the hood of our geo-redundant, highly available, distributed cloud directory: http://blogs.technet.com/b/ad/archive/2014/09/02/azure-ad-under-the-hood-of-our-geo-redundant-highly-available-geo-distributed-cloud-directory.aspx [↑](#footnote-ref-15)
16. KuppingerCole Leadership Compass Cloud User and Access Management: http://news.microsoft.com/itanalyst/docs/06-20-14CompassCloudUser.pdf [↑](#footnote-ref-16)
17. Microsoft recognized in Leader Quadrant of Gartner’s Magic Quadrant for Identity and Access Management as a Service, Worldwide: https://info.microsoft.com/EMS-IDaaS-MQ-2016.html [↑](#footnote-ref-17)
18. #AzureAD a leader in the 2016 Gartner IDaaS MQ!: https://blogs.technet.microsoft.com/enterprisemobility/2016/06/07/azuread-a-leader-in-the-2016-gartner-idaas-mq/ [↑](#footnote-ref-18)
19. Ibid [↑](#footnote-ref-19)
20. Azure Active Directory Applications: http://azure.microsoft.com/en-us/marketplace/active-directory/ [↑](#footnote-ref-20)
21. Application access enhancements for Windows Azure AD: http://technet.microsoft.com/en-us/library/dn308588.aspx [↑](#footnote-ref-21)
22. Azure management portal: http://manage.windowsazure.com [↑](#footnote-ref-22)
23. Using your Office 365 Azure AD tenant with application access enhancements for Windows Azure AD: http://blogs.technet.com/b/ad/archive/2013/09/10/empower-your-office-365-subscription-identity-management-with-application-access-enhancements-for-windows-azure-ad.aspx [↑](#footnote-ref-23)
24. Azure Active Directory Basic is now GA!: http://blogs.technet.com/b/ad/archive/2014/09/15/azure-active-directory-basic-is-now-ga.aspx [↑](#footnote-ref-24)
25. Enterprise Mobility Suite (EMS): http://www.microsoft.com/en-us/server-cloud/products/enterprise-mobility-suite/ [↑](#footnote-ref-25)
26. Microsoft Enterprise Agreement: http://www.microsoft.com/en-us/Licensing/licensing-programs/enterprise.aspx [↑](#footnote-ref-26)
27. Microsoft Cloud Solution Provider program: https://mspartner.microsoft.com/en/us/pages/solutions/cloud-reseller-overview.aspx [↑](#footnote-ref-27)
28. Microsoft Open Programs: http://www.microsoft.com/licensing/licensing-options/open-license.aspx [↑](#footnote-ref-28)
29. Azure AD and Enterprise Mobility Suite now available without an Enterprise Agreement: http://blogs.technet.com/b/ad/archive/2015/03/12/azure-ad-and-enterprise-mobility-suite-now-broadly-available-outside-of-an-enterprise-agreement.aspx [↑](#footnote-ref-29)
30. Azure Active Directory editions: http://msdn.microsoft.com/en-us/library/azure/dn532272.aspx [↑](#footnote-ref-30)
31. Azure Active Directory Pricing: http://azure.microsoft.com/en-us/pricing/details/active-directory/ [↑](#footnote-ref-31)
32. Azure AD service limits and restrictions: http://msdn.microsoft.com/en-us/library/azure/dn764971.aspx [↑](#footnote-ref-32)
33. Getting started with Azure AD Premium: http://msdn.microsoft.com/en-us/library/azure/dn499825.aspx [↑](#footnote-ref-33)
34. Enabling Azure Active Directory Premium trial: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Enabling-Azure-Active-Directory-Premium-trial [↑](#footnote-ref-34)
35. How to Purchase Azure Active Directory Premium - New Customers: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/How-to-Purchase-Azure-Active-Directory-Premium-New-Customers [↑](#footnote-ref-35)
36. How to Purchase Azure Active Directory Premium - Existing Customers: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/How-to-Purchase-Azure-Active-Directory-Premium-Existing-Customer [↑](#footnote-ref-36)
37. Simplified License Assignment with Azure AD and EMS: http://blogs.technet.com/b/ad/archive/2014/09/18/simplified-license-assignment-with-azure-ad-and-ems.aspx [↑](#footnote-ref-37)
38. How to assign EMS/Azure AD Premium licenses to user accounts: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/How-to-assign-Azure-AD-Premium-Licenses-to-user-accounts [↑](#footnote-ref-38)
39. Assign EMS/Azure AD Premium licenses with PowerShell: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Assign-EMS-Azure-AD-Premium-lics-with-PowerShell [↑](#footnote-ref-39)
40. Azure AD Premium Dashboard is in preview!: <http://blogs.technet.com/b/ad/archive/2015/09/15/azure-ad-premium-dashboard-is-in-preview.aspx> [↑](#footnote-ref-40)
41. Reimaging Active Directory for the Social Enterprise (Part 2): http://blogs.msdn.com/b/windowsazure/archive/2012/06/20/reimagining-active-directory-for-the-social-enterprise-part-2.aspx [↑](#footnote-ref-41)
42. Entity Reference: http://msdn.microsoft.com/en-us/library/azure/dn151470.aspx [↑](#footnote-ref-42)
43. Leverage Azure AD for modern business applications: http://www.microsoft.com/en-gb/download/details.aspx?id=36391 [↑](#footnote-ref-43)
44. Azure AD Graph API: http://msdn.microsoft.com/en-us/library/windowsazure/hh974476.aspx [↑](#footnote-ref-44)
45. Extend Azure Active Directory Schema using Graph API (preview): http://blogs.msdn.com/b/aadgraphteam/archive/2014/03/06/extend-azure-active-directory-schema-using-graph-api-preview.aspx [↑](#footnote-ref-45)
46. Extending the Azure Graph Using the Azure Graph Store: http://msdn.microsoft.com/en-us/library/azure/dn720459.aspx [↑](#footnote-ref-46)
47. Wrapping up the year with a boat load of Azure AD news!: http://blogs.technet.com/b/ad/archive/2014/12/11/wrapping-up-the-year-with-a-boat-load-of-azure-ad-news.aspx [↑](#footnote-ref-47)
48. Administrative units management in Azure AD - Public Preview: https://msdn.microsoft.com/en-us/library/azure/dn832057.aspx [↑](#footnote-ref-48)
49. Manage Azure AD using Windows PowerShell: http://msdn.microsoft.com/en-us/library/jj151815.aspx [↑](#footnote-ref-49)
50. Supported Token and Claim Types: https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/ [↑](#footnote-ref-50)
51. Azure Active Directory Authentication Protocols: http://msdn.microsoft.com/library/azure/dn151124.aspx [↑](#footnote-ref-51)
52. Web Services Federation Language (WS-Federation) Version 1.2: http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf [↑](#footnote-ref-52)
53. WS-Trust Version 1.3: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf [↑](#footnote-ref-53)
54. Security Assertion Markup Language (SAML) 2.0: http://go.microsoft.com/fwlink/?LinkId=193996 [↑](#footnote-ref-54)
55. Supported Token and Claim Types: https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/ [↑](#footnote-ref-55)
56. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf [↑](#footnote-ref-56)
57. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf [↑](#footnote-ref-57)
58. Single Sign-on (SAML Protocol): http://msdn.microsoft.com/en-us/library/windowsazure/dn195589.aspx [↑](#footnote-ref-58)
59. RFC 6749 The OAuth 2.0 Authorization Framework: http://tools.ietf.org/html/rfc6749 [↑](#footnote-ref-59)
60. RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage: http://tools.ietf.org/html/rfc6750 [↑](#footnote-ref-60)
61. OAuth 2.0 in Azure AD: https://msdn.microsoft.com/en-us/library/azure/dn645545.aspx [↑](#footnote-ref-61)
62. JSON Web Token (JWT): http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-13 [↑](#footnote-ref-62)
63. Supported Token and Claim Types: https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/ [↑](#footnote-ref-63)
64. Open ID Connect Core 1.0 incorporating errata set 1: http://openid.net/specs/openid-connect-core-1\_0.html [↑](#footnote-ref-64)
65. OpenID Connect 1.0: https://msdn.microsoft.com/en-us/library/azure/dn645541.aspx [↑](#footnote-ref-65)
66. The OpenID Foundation Launches OpenID Connect Certification Program: http://openid.net/2015/04/17/openid-connect-certification-program/ [↑](#footnote-ref-66)
67. OpenID Certification: http://openid.net/certification/ [↑](#footnote-ref-67)
68. Azure Multi-Factor Authentication: http://azure.microsoft.com/en-us/services/multi-factor-authentication/ [↑](#footnote-ref-68)
69. Simplifying our Azure AD Authentication Flows: http://blogs.technet.com/b/ad/archive/2015/03/06/simplifying-our-azure-ad-authentication-flows.aspx [↑](#footnote-ref-69)
70. Creating and Managing Multiple Azure Active Directories: http://blogs.technet.com/b/ad/archive/2013/11/08/creating-and-managing-multiple-windows-azure-active-directories.aspx [↑](#footnote-ref-70)
71. Azure AD service limits and restrictions: http://msdn.microsoft.com/en-us/library/azure/dn764971.aspx [↑](#footnote-ref-71)
72. What is an Azure AD directory?: http://msdn.microsoft.com/library/azure/jj573650.aspx#BKMK\_DeleteDirectory [↑](#footnote-ref-72)
73. Implement Password Synchronization: http://technet.microsoft.com/en-us/library/dn246918.aspx [↑](#footnote-ref-73)
74. DirSync: Password Sync Frequently Asked Questions: http://social.technet.microsoft.com/wiki/contents/articles/18096.dirsync-password-sync-frequently-asked-questions.aspx [↑](#footnote-ref-74)
75. Azure Active Directory Hybrid Identity Design Considerations: https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-overview/ [↑](#footnote-ref-75)
76. Office 2013 modern authentication public preview announced: http://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/ [↑](#footnote-ref-76)
77. Deploy AD DS or AD FS and Office 365 with single sign-on and Azure Virtual Machines: http://technet.microsoft.com/en-us/library/dn509513.aspx [↑](#footnote-ref-77)
78. Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines: http://msdn.microsoft.com/library/azure/jj156090.aspx [↑](#footnote-ref-78)
79. Office 2013 modern authentication public preview announced: http://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/ [↑](#footnote-ref-79)
80. Azure Active Directory Authentication Libraries: http://msdn.microsoft.com/en-us/library/azure/dn151135.aspx [↑](#footnote-ref-80)
81. Determine which directory integration scenario to use: http://technet.microsoft.com/en-us/library/jj573649.aspx [↑](#footnote-ref-81)
82. Administering your Azure AD tenant: http://technet.microsoft.com/en-us/library/hh967611.aspx [↑](#footnote-ref-82)
83. Add your domain: http://technet.microsoft.com/en-us/library/hh969247.aspx [↑](#footnote-ref-83)
84. Verify a domain at any domain name registrar: http://technet.microsoft.com/en-us/library/jj151803.aspx [↑](#footnote-ref-84)
85. Azure Active Directory Connect: https://msdn.microsoft.com/en-us/library/azure/dn757582.aspx [↑](#footnote-ref-85)
86. Azure Active Directory Connect: http://www.microsoft.com/en-us/download/details.aspx?id=47594 [↑](#footnote-ref-86)
87. Azure AD Connect & Connect Health is now GA!: http://blogs.technet.com/b/ad/archive/2015/06/24/azure-ad-connect-amp-connect-health-is-now-ga.aspx [↑](#footnote-ref-87)
88. Azure Active Directory Connect: https://msdn.microsoft.com/en-us/library/azure/dn832695.aspx [↑](#footnote-ref-88)
89. Azure Active Directory Sync tool – 64 bits: http://go.microsoft.com/fwlink/?LinkID=278924 [↑](#footnote-ref-89)
90. Azure Active Directory Synchronization Tool (DirSync): https://msdn.microsoft.com/en-us/library/azure/dn790211.aspx [↑](#footnote-ref-90)
91. DirSync: List of Attributes that are Synced by the Windows Azure Active Directory Sync Tool: http://social.technet.microsoft.com/wiki/contents/articles/19901.dirsync-list-of-attributes-that-are-synced-by-the-windows-azure-active-directory-sync-tool.aspx [↑](#footnote-ref-91)
92. Making it simple to connect Windows Server AD to Windows Azure AD with password hash sync: http://blogs.technet.com/b/ad/archive/2013/06/03/making-it-simple-to-connect-windows-server-ad-to-windows-azure-ad-with-password-hash-sync.aspx [↑](#footnote-ref-92)
93. Azure Active Directory Sync tool - Version Release History: http://social.technet.microsoft.com/wiki/contents/articles/18429.windows-azure-active-directory-sync-tool-version-release-history.aspx [↑](#footnote-ref-93)
94. DirSync: How To Switch From Single Sign-On To Password Sync: http://social.technet.microsoft.com/wiki/contents/articles/17857.aad-sync-how-to-switch-from-single-sign-on-to-password-sync.aspx [↑](#footnote-ref-94)
95. Directory synchronization roadmap: http://technet.microsoft.com/en-us/library/hh967642.aspx [↑](#footnote-ref-95)
96. Manage directory synchronization: http://technet.microsoft.com/en-us/library/jj151821.aspx [↑](#footnote-ref-96)
97. HowTo: Install the Azure Active Directory Sync Tool (now with Pictures!): http://social.technet.microsoft.com/wiki/contents/articles/19098.howto-install-the-windows-azure-active-directory-sync-tool-now-with-pictures.aspx [↑](#footnote-ref-97)
98. Best Practices for Deploying and Managing the Azure Active Directory Sync Tool: http://social.technet.microsoft.com/wiki/contents/articles/17370.best-practices-for-deploying-and-managing-the-windows-azure-active-directory-sync-tool.aspx [↑](#footnote-ref-98)
99. Azure Active Directory Sync is now GA!: http://blogs.technet.com/b/ad/archive/2014/09/16/azure-active-directory-sync-is-now-ga.aspx [↑](#footnote-ref-99)
100. Azure Active Directory Sync: https://msdn.microsoft.com/en-us/library/azure/dn790204.aspx [↑](#footnote-ref-100)
101. Forefront Identity Manager Connector for Windows Azure Active Directory: http://www.microsoft.com/en-us/download/details.aspx?id=41166 [↑](#footnote-ref-101)
102. Azure AD & Windows 10: better Together for Work and School: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-102)
103. Azure AD Connect: Version Release History: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-version-history/ [↑](#footnote-ref-103)
104. Topologies for Azure AD Connect: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-topologies/ [↑](#footnote-ref-104)
105. Integrating your on-premises identities with Azure Active Directory: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/ [↑](#footnote-ref-105)
106. Prepare for directory synchronization: http://technet.microsoft.com/library/jj151831.aspx [↑](#footnote-ref-106)
107. Microsoft Azure Active Directory Connect: http://www.microsoft.com/en-us/download/details.aspx?id=47594 [↑](#footnote-ref-107)
108. Considerations for Deploying Forest Trust: http://technet.microsoft.com/en-us/library/dd560680%28v=WS.10%29.aspx [↑](#footnote-ref-108)
109. Additional Configuration for Functionality Across Forests (Multiple Forest Considerations in Windows 2000 and Windows Server 2003): http://technet.microsoft.com/en-us/library/cc779566%28v=WS.10%29.aspx [↑](#footnote-ref-109)
110. Azure Active Directory Connect Health: https://msdn.microsoft.com/en-us/library/azure/dn906722.aspx [↑](#footnote-ref-110)
111. New Azure Portal: https://portal.azure.com/ [↑](#footnote-ref-111)
112. Azure AD Connect Health for sync is now in Public Preview!: http://blogs.technet.com/b/ad/archive/2015/11/05/azure-ad-connect-health-for-sync-is-now-in-public-preview.aspx [↑](#footnote-ref-112)
113. Monitor your on-premises identity infrastructure in the cloud: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-health/ [↑](#footnote-ref-113)
114. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-114)
115. Forefront Identity Manager Connector for Azure Active Directory: http://www.microsoft.com/en-us/download/details.aspx?id=41166 [↑](#footnote-ref-115)
116. Azure Active Directory Connector for FIM 2010 R2 Technical Reference: http://technet.microsoft.com/en-us/library/dn511001(v=ws.10).aspx [↑](#footnote-ref-116)
117. Azure AD Graph Entities Reference: http://msdn.microsoft.com/library/azure/hh974478.aspx [↑](#footnote-ref-117)
118. Connect Windows PowerShell to the Service: http://help.outlook.com/en-us/140/cc952755.aspx [↑](#footnote-ref-118)
119. Using Exchange Management Shell to manage your Exchange Online and Exchange On Premises Environment: http://blogs.technet.com/b/ilvancri/archive/2012/03/17/3487056.aspx [↑](#footnote-ref-119)
120. Reference to Available PowerShell Cmdlets in Exchange Online: http://help.outlook.com/en-us/140/dd575549.aspx [↑](#footnote-ref-120)
121. Announcing the new version of the Graph API: api-version=2013-11-08: http://blogs.msdn.com/b/aadgraphteam/archive/2013/11/14/announcing-the-new-version-of-the-graph-api-api-version-2013-11-08.aspx [↑](#footnote-ref-121)
122. Management Agents in FIM 2010 R2: http://technet.microsoft.com/en-us/library/jj863241(v=ws.10).aspx [↑](#footnote-ref-122)
123. Forefront Identity Manager Connector for Generic LDAP: http://www.microsoft.com/en-us/download/details.aspx?id=41163 [↑](#footnote-ref-123)
124. Microsoft Identity Manager 2016: http://www.microsoft.com/en-gb/server-cloud/products/microsoft-identity-manager/default.aspx [↑](#footnote-ref-124)
125. OpenLDAP Extensible Management Agent (XMA): http://sourceforge.net/projects/openldap-xma/ [↑](#footnote-ref-125)
126. Optimal IdM: http://www.optimalidm.com/ [↑](#footnote-ref-126)
127. Identity federation definition from Wikipedia: http://en.wikipedia.org/wiki/Federated\_identity [↑](#footnote-ref-127)
128. OASIS Web Services Federation Language (WS-Federation) Version 1.2: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf [↑](#footnote-ref-128)
129. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf [↑](#footnote-ref-129)
130. Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on: http://technet.microsoft.com/en-us/library/jj679342.aspx [↑](#footnote-ref-130)
131. 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-131)
132. Connectivity Analyzer: http://go.microsoft.com/?linkid=9841876 [↑](#footnote-ref-132)
133. STS Integration Paper using WS-\* Protocols: http://www.microsoft.com/en-us/download/details.aspx?id=41185 [↑](#footnote-ref-133)
134. Office 365 SAML 2.0 Federation Implementer’s Guide v1.0: http://go.microsoft.com/?linkid=9844221 [↑](#footnote-ref-134)
135. Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on: http://technet.microsoft.com/en-us/library/jj679342.aspx [↑](#footnote-ref-135)
136. Active Directory Federation Services 2.0 RTW: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=10909 [↑](#footnote-ref-136)
137. Description of Update Rollup 3 for Active Directory Federation Services (AD FS) 2.0: http://support.microsoft.com/kb/2790338 [↑](#footnote-ref-137)
138. Checklist: Use AD FS to implement and manage single sign-on: http://technet.microsoft.com/en-us/library/jj205462.aspx [↑](#footnote-ref-138)
139. Azure AD/Office 365 Single Sign-On (SSO) with AD FS in Windows Server 2012 R2: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-139)
140. Microsoft Office 365 Single Sign-On (SSO) with AD FS 2.0: http://www.microsoft.com/en-us/download/details.aspx?id=28971 [↑](#footnote-ref-140)
141. Web Application Proxy Overview: http://technet.microsoft.com/en-us/library/dn280944.aspx [↑](#footnote-ref-141)
142. Internet2/MACE (Middleware Architecture Committee for Education): http://middleware.internet2.edu/MACE [↑](#footnote-ref-142)
143. Shibboleth Consortium: http://shibboleth.net [↑](#footnote-ref-143)
144. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf [↑](#footnote-ref-144)
145. Single Sign-on (SAML Protocol): http://msdn.microsoft.com/en-us/library/windowsazure/dn195589.aspx [↑](#footnote-ref-145)
146. Single Sign-out (SAML Protocol): http://msdn.microsoft.com/en-us/library/windowsazure/dn195588.aspx [↑](#footnote-ref-146)
147. Azure AD/Office 365 Single Sign-on (SSO) with Shibboleth 2.0: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-147)
148. Shibboleth Installation: https://wiki.shibboleth.net/confluence/display/SHIB2/Installation [↑](#footnote-ref-148)
149. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-149)
150. Azure Cloud App Discovery is now GA: https://appdiscovery.azure.com/ [↑](#footnote-ref-150)
151. Azure Cloud App Discovery GA and our new Privileged Identity Management service: http://blogs.technet.com/b/ad/archive/2015/05/04/azure-cloud-app-discovery-ga-and-our-new-privileged-identity-management-service.aspx [↑](#footnote-ref-151)
152. Cloud App Discovery - Frequently Asked Questions: http://social.technet.microsoft.com/wiki/contents/articles/24037.cloud-app-discovery-frequently-asked-questions.aspx [↑](#footnote-ref-152)
153. Cloud App Discovery: https://msdn.microsoft.com/en-us/library/azure/mt143581.aspx [↑](#footnote-ref-153)
154. Power BI: http://www.microsoft.com/en-us/powerbi/default.aspx [↑](#footnote-ref-154)
155. Cloud App Discovery: Now with Excel and Power BI Support: http://blogs.technet.com/b/ad/archive/2014/10/01/more-news-on-cloud-app-discovery.aspx [↑](#footnote-ref-155)
156. Azure AD app gallery: http://azure.microsoft.com/en-us/marketplace/active-directory/all/ [↑](#footnote-ref-156)
157. Pre-Integrated Apps and our App Gallery: http://blogs.technet.com/b/ad/archive/2013/11/20/pre-integrated-apps-and-our-app-gallery.aspx [↑](#footnote-ref-157)
158. Azure Active Directory Applications: http://azure.microsoft.com/en-us/marketplace/active-directory/ [↑](#footnote-ref-158)
159. Integrating Salesforce with Azure AD: How to enable Single Sign-On (1/2): https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Integrating-Salesforce-with-Azure-AD-How-to-enable-Single-Sign-On-12 [↑](#footnote-ref-159)
160. Integrating Salesforce with Azure AD: How to automate User Provisioning (2/2): https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Integrating-Salesforce-with-Azure-AD-How-to-automate-User-Provisioning-22 [↑](#footnote-ref-160)
161. Application access capabilities for Azure Active Directory: https://msdn.microsoft.com/library/azure/dn308588.aspx [↑](#footnote-ref-161)
162. Azure Active Directory Integration Tutorials: https://msdn.microsoft.com/en-us/library/azure/dn893637.aspx [↑](#footnote-ref-162)
163. Tutorial: Azure AD integration with Salesforce: http://msdn.microsoft.com/en-us/library/azure/dn308593.aspx [↑](#footnote-ref-163)
164. Tutorial: Azure AD integration with Salesforce Sandbox: http://msdn.microsoft.com/en-us/library/azure/dn798671.aspx [↑](#footnote-ref-164)
165. Tutorial: Azure AD integration with Box: http://msdn.microsoft.com/en-us/library/azure/dn308589.aspx [↑](#footnote-ref-165)
166. Tutorial: Azure AD integration with Google Apps: http://msdn.microsoft.com/en-us/library/azure/dn308591.aspx [↑](#footnote-ref-166)
167. Tutorial: Azure AD integration with Citrix GoToMeeting: http://msdn.microsoft.com/en-us/library/azure/dn440168.aspx [↑](#footnote-ref-167)
168. Tutorial: Azure AD integration with Concur: http://msdn.microsoft.com/en-us/library/azure/dn308592.aspx [↑](#footnote-ref-168)
169. Tutorial: Azure AD integration with Workday: http://technet.microsoft.com/en-us/library/dn510972.aspx [↑](#footnote-ref-169)
170. Tutorial: Azure AD integration with Jive: http://technet.microsoft.com/en-us/library/dn510977.aspx [↑](#footnote-ref-170)
171. Tutorial: Azure AD integration with DocuSign: http://technet.microsoft.com/en-us/library/dn510973.aspx [↑](#footnote-ref-171)
172. Tutorial: Azure AD integration with Servicenow: http://technet.microsoft.com/en-us/library/dn510971.aspx [↑](#footnote-ref-172)
173. Tutorial: Azure AD integration with Dropbox for Business: http://technet.microsoft.com/en-us/library/dn510978.aspx [↑](#footnote-ref-173)
174. Best Practices for Managing the Application access enhancements for Azure Active Directory: http://social.technet.microsoft.com/wiki/contents/articles/18409.best-practices-for-managing-the-application-access-enhancements-for-windows-azure-active-directory.aspx [↑](#footnote-ref-174)
175. Azure AD Custom Attribute Mapping for SaaS App User Provisioning: http://blogs.technet.com/b/ad/archive/2015/01/07/azure-ad-custom-attribute-mapping-for-saas-app-user-provisioning.aspx [↑](#footnote-ref-175)
176. Customizing Attribute Mappings: https://msdn.microsoft.com/en-us/library/azure/dn872469.aspx [↑](#footnote-ref-176)
177. Writing Expressions for Attribute Mappings in Azure Active Directory: https://msdn.microsoft.com/en-us/library/azure/dn891618.aspx [↑](#footnote-ref-177)
178. Wrapping up the year with a boat load of Azure AD news!: http://blogs.technet.com/b/ad/archive/2014/12/11/wrapping-up-the-year-with-a-boat-load-of-azure-ad-news.aspx [↑](#footnote-ref-178)
179. “Bring your own app” with Azure AD Self-Service SAML configuration -> now in preview: http://blogs.technet.com/b/ad/archive/2015/06/17/bring-your-own-app-with-azure-ad-self-service-saml-configuration-gt-now-in-preview.aspx [↑](#footnote-ref-179)
180. Leverage Azure AD for modern business applications: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-180)
181. System for Cross-domain Identity Management (SCIM) 2.0: http://www.simplecloud.info/ [↑](#footnote-ref-181)
182. Azure AD Premium now supports SCIM 2.0!: http://blogs.technet.com/b/ad/archive/2015/11/17/azure-ad-premium-now-supports-scim-2-0.aspx [↑](#footnote-ref-182)
183. Azure AD: Helping you adding SCIM support to your applications: http://blogs.technet.com/b/ad/archive/2015/11/23/azure-ad-helping-you-adding-scim-support-to-your-applications.aspx [↑](#footnote-ref-183)
184. Microsoft.SystemForCrossDomainIdentityManagement: https://www.nuget.org/packages/Microsoft.SystemForCrossDomainIdentityManagement/ [↑](#footnote-ref-184)
185. AzureAD-BYOA-Provisioning-Samples: https://github.com/Azure/AzureAD-BYOA-Provisioning-Samples/tree/master [↑](#footnote-ref-185)
186. Using SCIM to enable automatic provisioning of users and groups from Azure Active Directory to applications: https://azure.microsoft.com/en-us/documentation/articles/active-directory-scim-provisioning/ [↑](#footnote-ref-186)
187. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-187)
188. Web Application Proxy: http://technet.microsoft.com/en-us/library/dn584107.aspx [↑](#footnote-ref-188)
189. Azure AD Application Proxy Connector Troubleshooter: http://aka.ms/aadapConnectorTroubleshoot [↑](#footnote-ref-189)
190. Troubleshooting tool to validate connector networking prerequisites: http://blogs.technet.com/b/applicationproxyblog/archive/2015/09/03/troubleshooting-tool-to-validate-connector-networking-prerequisites.aspx [↑](#footnote-ref-190)
191. Publishing apps on separate networks and locations using connector groups: http://blogs.technet.com/b/applicationproxyblog/archive/2015/10/14/publishing-apps-on-separate-networks-and-locations-using-connector-groups.aspx [↑](#footnote-ref-191)
192. Using Application Proxy to publish applications for secure remote access: https://msdn.microsoft.com/en-us/library/azure/dn768219.aspx [↑](#footnote-ref-192)
193. Enable Application Proxy services: http://msdn.microsoft.com/en-us/library/azure/dn768214.aspx [↑](#footnote-ref-193)
194. Publish applications with Application Proxy: http://msdn.microsoft.com/en-us/library/azure/dn768220.aspx [↑](#footnote-ref-194)
195. Azure AD Application Proxy now supports custom domain names!: http://blogs.technet.com/b/ad/archive/2015/04/22/azure-ad-application-proxy-now-support-custom-domain-names.aspx [↑](#footnote-ref-195)
196. Integrating Applications in Azure Active Directory: http://msdn.microsoft.com/en-us/library/windowsazure/dn151122.aspx [↑](#footnote-ref-196)
197. Leverage Azure AD for modern business applications: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-197)
198. Adding, Updating, and Removing an App: http://msdn.microsoft.com/en-us/library/dn132599.aspx [↑](#footnote-ref-198)
199. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-199)
200. Azure Active Directory's support for managing shared company accounts for Twitter, Facebook and more: http://blogs.technet.com/b/ad/archive/2014/10/31/azure-ad-now-supports-sharing-logins-for-twitter-facebook-and-more.aspx [↑](#footnote-ref-200)
201. Azure AD automated password roll-over for Facebook, Twitter and LinkedIn now in preview!: http://blogs.technet.com/b/ad/archive/2015/02/20/azure-ad-automated-password-roll-over-for-facebook-twitter-and-linkedin-now-in-preview.aspx [↑](#footnote-ref-201)
202. Managing access to resources with Azure Active Directory groups: <https://azure.microsoft.com/en-us/documentation/articles/active-directory-manage-groups/> [↑](#footnote-ref-202)
203. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-203)
204. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-204)
205. Attribute based Dynamic Group Membership for Azure AD Premium is now in Preview: http://blogs.technet.com/b/ad/archive/2015/03/09/attribute-based-dynamic-group-membership-for-azure-ad-premium-is-now-in-preview.aspx [↑](#footnote-ref-205)
206. Azure AD: Introduction to Dynamic Memberships for Groups: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Azure-AD--Introduction-to-Dynamic-Memberships-for-Groups [↑](#footnote-ref-206)
207. Active Directory from the on-premises to the Cloud: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-207)
208. 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-208)
209. Manage Risk with Conditional Access Control: http://technet.microsoft.com/en-us/library/dn280937.aspx [↑](#footnote-ref-209)
210. Azure AD/Office 365 single sign-on (SSO) with AD FS in Windows Server 2012 R2 – Part 1: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-210)
211. Microsoft Intune: http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/default.aspx [↑](#footnote-ref-211)
212. Azure AD Device Registration is now Generally Available: http://blogs.technet.com/b/ad/archive/2015/03/30/azure-ad-device-registration-service-is-now-ga.aspx [↑](#footnote-ref-212)
213. Azure Active Directory Device Registration Overview: https://msdn.microsoft.com/en-us/library/azure/dn903763.aspx [↑](#footnote-ref-213)
214. Setting up On-premises Conditional Access using Azure Active Directory Device Registration: https://msdn.microsoft.com/en-us/library/azure/dn788908.aspx [↑](#footnote-ref-214)
215. Microsoft Intune: http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/default.aspx [↑](#footnote-ref-215)
216. Azure AD & windows 10: Better Together for Work or School: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-216)
217. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-217)
218. Azure Active Directory Module for Windows PowerShell (64-bit version): http://go.microsoft.com/fwlink/p/?linkid=236297 [↑](#footnote-ref-218)
219. Azure AD Conditional Access and Azure AD Connect Health - Now in Preview: http://blogs.technet.com/b/ad/archive/2015/01/29/azure-ad-conditional-access-and-azure-ad-connect-health-now-in-preview.aspx [↑](#footnote-ref-219)
220. Azure AD Conditional Access preview updated: Now supports On-Premises and Custom LOB apps: http://blogs.technet.com/b/ad/archive/2015/03/11/azure-ad-conditional-access-preview-updated-now-supports-on-premises-and-custom-lob-apps.aspx [↑](#footnote-ref-220)
221. Azure Conditional Access Preview for SaaS Apps: https://msdn.microsoft.com/en-us/library/azure/dn906877.aspx [↑](#footnote-ref-221)
222. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-222)
223. Azure Active Directory Premium reporting now detects leaked credentials: http://blogs.technet.com/b/ad/archive/2015/06/15/azure-active-directory-premium-reporting-now-detects-leaked-credentials.aspx [↑](#footnote-ref-223)
224. View your access and usage reports: http://msdn.microsoft.com/en-us/library/dn283934.aspx [↑](#footnote-ref-224)
225. View your access and usage reports: http://technet.microsoft.com/en-us/library/dn283934.aspx [↑](#footnote-ref-225)
226. Azure Active Directory Reports: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Azure-Active-Directory-Reports [↑](#footnote-ref-226)
227. Azure Active Directory Reporting Guide: https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-guide/ [↑](#footnote-ref-227)
228. Announcing the preview of Graph Reports and Events API: http://blogs.msdn.com/b/aadgraphteam/archive/2015/05/15/announcing-the-preview-version-of-graph-reports-and-events-api.aspx [↑](#footnote-ref-228)
229. Azure AD Reports and Events (Preview): https://msdn.microsoft.com/en-us/library/azure/mt126081.aspx [↑](#footnote-ref-229)
230. Azure AD and Microsoft Identity Manager Reporting – we’ve gone hybrid!: http://blogs.technet.com/b/ad/archive/2015/05/22/azure-ad-and-microsoft-identity-manager-reporting-we-ve-gone-hybrid.aspx [↑](#footnote-ref-230)
231. Azure Multi-Factor Authentication: http://azure.microsoft.com/en-us/services/multi-factor-authentication/ [↑](#footnote-ref-231)
232. Multi-Factor Authentication Pricing Details: http://azure.microsoft.com/en-us/pricing/details/multi-factor-authentication/ [↑](#footnote-ref-232)
233. Leveraging Multi-Factor Authentication with Azure AD: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-233)
234. Using Multi-Factor Authentication with Azure AD: http://technet.microsoft.com/en-us/library/jj713614.aspx [↑](#footnote-ref-234)
235. Getting started with Azure Multi-Factor Authentication: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Getting-started-with-Azure-Multi-Factor-Authentication [↑](#footnote-ref-235)
236. LEVERAGING MULTI-FACTOR AUTHENTICATION SERVER ON-PREMISES: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-236)
237. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-237)
238. Advanced persistent threat: https://en.wikipedia.org/wiki/Advanced\_persistent\_threat [↑](#footnote-ref-238)
239. Azure Cloud App Discovery GA and our new Privileged Identity Management service: http://blogs.technet.com/b/ad/archive/2015/05/04/azure-cloud-app-discovery-ga-and-our-new-privileged-identity-management-service.aspx [↑](#footnote-ref-239)
240. Azure AD Privileged Identity Management: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Azure-AD-Privileged-Identity-Management [↑](#footnote-ref-240)
241. First day at work with Azure Active Directory: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/First-day-at-work-with-Azure-Active-Directory [↑](#footnote-ref-241)
242. Access Panel portal: https://account.activedirectory.windowsazure.com/applications (shortened URL: http://myapps.microsoft.com) [↑](#footnote-ref-242)
243. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-243)
244. Self-service password reset for users: http://technet.microsoft.com/en-us/library/dn510386.aspx [↑](#footnote-ref-244)
245. How to configure self-service password reset for users in Azure AD: http://channel9.msdn.com/Blogs/Windows-Azure/How-to-configure-self-service-password-reset-for-users-in-Windows-Azure-AD [↑](#footnote-ref-245)
246. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-246)
247. Self-service group management for users: http://msdn.microsoft.com/en-us/library/dn641267.aspx [↑](#footnote-ref-247)
248. Delegated Group Management on Azure Active Directory Premium: https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Delegated-Group-Management-on-Azure-Active-Directrory-Premium [↑](#footnote-ref-248)
249. Manage your groups: http://msdn.microsoft.com/en-us/library/azure/dn641268.aspx [↑](#footnote-ref-249)
250. Customize Your App SSO Experience with Azure AD: http://blogs.technet.com/b/ad/archive/2014/10/30/customize-your-app-sso-experience-with-azure-ad.aspx [↑](#footnote-ref-250)
251. Employee Self-Service App Access for Azure AD now in preview!: http://blogs.technet.com/b/ad/archive/2015/04/23/employee-self-service-app-access-for-azure-ad-now-in-preview.aspx [↑](#footnote-ref-251)
252. Azure Active Directory Editions: http://technet.microsoft.com/en-us/library/dn532272.aspx [↑](#footnote-ref-252)
253. Add company branding to your Sign In and Access Panel pages: <https://technet.microsoft.com/en-us/library/dn532270.aspx> [↑](#footnote-ref-253)
254. My Apps for Android: https://play.google.com/store/apps/details?id=com.microsoft.myapps [↑](#footnote-ref-254)
255. Apple App Store: https://itunes.apple.com/us/app/my-apps-windows-azure-active/id824048653?mt=8 [↑](#footnote-ref-255)
256. Accessing Azure AD connected apps on Android phones, iPhones, and iPads: http://blogs.technet.com/b/ad/archive/2014/11/19/accessing-azure-ad-connected-apps-on-android-phones-iphones-and-ipads.aspx [↑](#footnote-ref-256)