Azure AD & Windows 10: Better Together for Work or School

Overview Technical Article

Microsoft France

Published: May 2015 (Updated: January 2016)

Version: 1.0a

Authors: Philippe Beraud, Pascal Sauliere (Microsoft France)

Reviewer: Jairo Cadena (Microsoft Corporation)

For the latest information on Azure Active Directory, please see

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

For the latest information on Windows 10, please see

http://www.microsoft.com/en-us/windows/features

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

Abstract: With the consumerization of IT (CoIT) along with the Bring Your Own Device (BYOD) trend, organizations of all sizes are facing growing needs to protect and control corporate sensitive information whilst being pressured to provide a seamless access to it from an end-user perspective. Thinking about CoIT indeed necessarily leads to some security and management challenges. It’s all the more so with the move the Cloud to save cost and bring agility as a result of the modernization of IT, the explosion of information with dispersed enterprise data, the Social Enterprise and its applications enabling new collaboration, etc.

Microsoft has enabled CoIT through many technologies for many years and now helps IT professionals face security, compliance and compatibility issues they might deal with and give users access to corporate intellectual property from ubiquitous devices, both managed and unmanaged.

With the availability of Windows 10, Microsoft continues the above investments to provide even more compelling experiences for end users whilst bringing additional and richer controls for IT professionals to master the company assets thanks to Azure AD.

The document demonstrates how Azure AD and Windows 10 can enable together the most frequent and relevant CoIT scenarios.

Table of Contents

[Introduction 3](#_Toc439843742)

[Objectives of this paper 5](#_Toc439843743)

[Non-objectives of this paper 5](#_Toc439843744)

[Organization of this paper 6](#_Toc439843745)

[About the audience 6](#_Toc439843746)

[Understanding the new capabilities enabled by Azure AD & Windows 10 7](#_Toc439843747)

[Capabilities for corporate owned computers and devices 7](#_Toc439843748)

[Capabilities for personal computers and devices 8](#_Toc439843749)

[Additional common capabilities 9](#_Toc439843750)

[Building a test lab environment 10](#_Toc439843751)

[Provisioning an Azure AD test tenant 10](#_Toc439843752)

[Building an on-premises test lab environment (Optional) 11](#_Toc439843753)

[Building a Windows 10 image 17](#_Toc439843754)

[Testing the new capabilities for corporate owned devices 23](#_Toc439843755)

[Configuring your Azure AD tenant 23](#_Toc439843756)

[Joining a device to Azure AD in a cloud-only environment 33](#_Toc439843757)

[Joining a device to a domain in a hybrid AD environment (Optional) 64](#_Toc439843758)

[Testing the new capabilities for personal devices 66](#_Toc439843759)

[Configuring your Azure AD tenant 66](#_Toc439843760)

[Adding an Azure AD account to a device 66](#_Toc439843761)

# Introduction

Devices have become cheaper and more affordable over the last few years and unsurprisingly proliferate: netbooks, laptops, smartphones, phablets, slates and tablets. Same is true for both cellular and wireless networks that have become ubiquities. Social networks (Facebook, Google+, Yammer, etc.) are changing how people get information and communicate. People want content and services to work seamlessly across these all these devices and environments. They are becoming connected all the time: at home, at work and everywhere in between… up to the point where personal and work communication can become indistinguishable.

As technology plays an increasingly important role in people’s personal lives, it is having a profound effect on their expectations for and use of technology in their work lives. People have access to powerful and affordable personal computers, laptops, and tablets, are using mobile devices more and more, expect “always on” connectivity and are connecting with each other in new ways using social networks. Ultimately, they have more choice, more options, and more flexibility in the technology they use every day, and as that technology spills over into their professional lives, the line between personal and professional time is blurring. People want to be able to choose what technology they use at work, and they increasingly want to use that same technology in all aspects of their lives. In fact, according to a study by Unisys (conducted by IDC), a full 95 percent of information workers use at least one self-purchased device at work.

“Consumerization of IT” (CoIT) is the current phenomenon whereby consumer technologies and consumer behavior are in various ways driving innovation for information technology within the organization. As people become more comfortable with technology innovation in their personal lives, they expect it in their professional lives.

Without any doubt, employees as well as contractors will demand access with anything anywhere:

* From any location: at work, at home, or mobile.
* From any device (laptops, tablets, smartphones, etc.) regardless of the fact they’re managed/unmanaged, corporate owned/personal.
* With UI that meets the high standard set in the consumer world.

While CoIT has remarkable potential for improving collaboration and productivity, many organizations are grappling with the potential security, privacy and compliance risks of introducing consumer technologies into their environment. However, there are also many benefits to the CoIT trend that organizations can capitalize on with the right approach. Managing the CoIT challenge requires striking a balance between users’ expectations and an organization’s requirements. People love their consumer technology because it makes it easier for them to connect with each other, access and share information, and collaborate. Those same benefits are there for the taking for businesses.

**Microsoft believes there is power in saying “Yes” to users and their technology requests in a responsible way – responsible meaning here that you embrace these trends but also ensure the environment remains secure and well managed.**

**Azure Active Directory (Azure AD) plays a central role in such a context to provide relevant technological answers for both corporate owned devices and personal devices in order to adequately and thus to smoothly accompany both corporate owned, personally enabled (COPE) and Bring Your Own Device (BYOD) initiates for organization of any size.**

Azure AD is Microsoft’s vehicle for providing Identity Management as-a-Service (IDaaS) capabilities in a cloud or hybrid environment. Microsoft’s approach to IdMaaS for organizations of all sizes 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. Microsoft has earned widespread adoption of its on-premises identity technology, a suite of capabilities packaged and branded as Windows Server Active Directory (WSAD).

In the on-premises world, AD provides a set of identity capabilities. AD is used extensively by organizations world-wide. AD is widely deployed in the Fortune 1000 and the Global 5000 today as their authoritative identity and access management system as well as in small and medium organizations and we will not describe it further here.

Azure AD has been designed to easily extend AD (in whole or in part) into the public Azure cloud[[1]](#footnote-1) as a directory whose content is owned and controlled by the organization providing the information.

**Azure AD is NOT a monolithic directory of information belonging to Microsoft, but rather, at the time of writing, more than three 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.**

**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**.

Note For additional information on Azure AD, see the white paper [Active Directory from on-premises to the cloud](http://www.microsoft.com/en-us/download/details.aspx?id=36391).)[[2]](#footnote-2).

Azure AD lets you achieve all your Identity and Access Management needs in an easy to configure environment. With your Azure AD tenant, you can create a private identity directory in the cloud, similar to the look and feel of a traditional Active Directory from the user's perspective.

Like WSAD, your Azure AD tenant allows you centrally control access to applications and resources. You can easily add existing resources (cloud services and/or on-premises applications with the [Azure AD Application Proxy](https://msdn.microsoft.com/en-us/library/azure/dn768219.aspx)[[3]](#footnote-3), a feature of Premium edition of Azure AD) as well as integrate applications and APIs you are developing.

Note Azure AD is available in three different editions you can choose from: Azure Active Directory (free), Azure Active Directory Basic, and Azure Active Directory Premium. 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)[[4]](#footnote-4). 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/)[[5]](#footnote-5). 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)[[6]](#footnote-6).

Your Azure AD tenant can be used as a standalone cloud directory or can be an extension of your on-premises identity and access management solutions to the cloud. In such cases, you can continue benefiting from your existing investments and on-premises capabilities while leveraging Azure AD to gain identity and access management in the cloud. You may hear these defined as cloud-only or hybrid Active Directory. This is the terminology we will use later in this document.

**Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Education editions enable a device to join an Azure AD tenant without needing the traditional WSAD domains on-premises if you want to. (Windows 10 mobile doesn’t support this capacity as of this writing.) Both aforementioned cloud-only and hybrid Active Directory environments will be supported.**

This provides a series of benefits for the end-users like a seamless Single Sign-On (SSO) experience to all the resources protected by your Azure AD tenant.

In addition, from an IT professional perspective, this allows to set rules and policies that control who has access and under what conditions. For example, you can require [Azure Multi-Factor Authentication (MFA)](https://azure.microsoft.com/en-us/services/multi-factor-authentication/)[[7]](#footnote-7), and manage access based on the device.

Beyond those capabilities more devoted to corporate owned devices, personal devices will allow to add an Azure AD account in a BYOD context.

## Objectives of this paper

This document is intended as an overview document for discovering and understanding the benefits of using Azure AD and Windows 10 together for work and school accounts. As the introduction suggests, such an overview is given from both a corporate owned device perspective and a personal one in a BYOD context.

Built on existing Microsoft’s documentation, knowledge base articles, and blog posts, this document provides a complete walkthrough to build a suitable test lab environment in Azure, test, and evaluate the above scenarios. It provides additional guidance if any.

## Non-objectives of this paper

This document is not intended as an overview document for the Azure AD offerings.

Note For additional information, see the Microsoft MSDN article [Getting started with Azure AD](http://msdn.microsoft.com/en-us/library/dn655157.aspx)[[8]](#footnote-8). As well as the white paper An overview of Azure AD[[9]](#footnote-9) as part of the same series of documents.

Likewise, it doesn’t provide either 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.

Note Please make sure you periodically check the [Azure AD community forum](http://social.msdn.microsoft.com/Forums/en-US/WindowsAzureAD/threads)[[10]](#footnote-10) as well as the MSDN [Azure blog](http://blogs.msdn.com/b/windowsazure/)[[11]](#footnote-11) for notification of upcoming enhancement and changes that relate to Azure AD.

The same consideration applies to Windows 10 as well.

## Organization of this paper

To cover the aforementioned objectives, this document is organized in the following four sections:

* Understanding the new capabilities enabled by Azure AD & Windows 10.
* Building a test lab environment.
* Testing the new capabilities for corporate owned devices.
* Testing the new capabilities for personal devices.

These sections provide the information details necessary to (hopefully) successfully build a working environment for the new capabilities enabled by combining Azure AD and Windows 10. They must be followed in order.

## About the audience

This document is designed for system architects and IT professionals interested in trying out the next version of Windows on behalf of their organizations. Some features and functionalities covered in this document may require additional hardware or software.

# Understanding the new capabilities enabled by Azure AD & Windows 10

As already shortly introduced, Azure AD and Windows 10 bring new capabilities for corporate owned and personal computers and devices. The next sections will give you an overview of these new capabilities for both corporate owned devices and personal devices.

Note For additional information, see the webcast [Microsoft Azure Active Directory and Windows 10: Better Together for Work or School](http://channel9.msdn.com/Events/Ignite/2015/BRK3332)[[12]](#footnote-12).

## Capabilities for corporate owned computers and devices

First of all, 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.) work natively with work or school accounts. There will be no longer the requirement to use a personal Microsoft Account (MSA).

Windows 10 uses 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 are supported in terms of identity model.

For organizations that do not have on-premises AD or do not use it for all their users (e.g. EDUs, seasonal workers, and temps): users are able to log on to Windows with their work account powered by Azure AD to enjoy single sign-on (SSO) from the desktop to Azure AD-backed applications and resources such as Office 365 and other organizational apps, websites and resources.

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)[[13]](#footnote-13), Mobile Device Management for Office 365, or 3rd party solution) are all supported. This is called **Azure AD Join**. With this new feature of Windows 10, Windows authenticates directly to Azure AD, and no WSAD domain controllers (DC) are needed. You can enjoy a cloud-only environment and this only requires that your organization provisions an Azure AD tenant.

This also works on mobile devices that do not have Domain Joined capabilities, and it works for managed and federated Azure AD accounts. This makes it easy for information workers to use their existing work credentials to log in to phones, tablets, and phablets that are owned by their organization and rehydrate their personalized work environment on these secondary devices.

Users are also allowed to set up shrink-wrapped Windows devices with their work or school account (managed or federated in Azure AD) and configure them as corporate-owned assets right in the Windows first run experience, a.k.a. out-of-box experience (OOBE), without the need for IT to spend time and money on device imaging. IT have the choice between imaging and allowing the corporate users to configure corporate owned devices by themselves during OOBE.

Note For additional information, see the blog posts [Azure Active Directory and Windows 10: Bringing the cloud to enterprise desktops!](http://blogs.technet.com/b/ad/archive/2015/05/13/azure-active-directory-and-windows-10-making-the-enterprise-cloud-a-reality.aspx)[[14]](#footnote-14), [Azure AD joint on Windows 10 devices](http://blogs.technet.com/b/ad/archive/2015/05/21/azure-ad-on-windows-10-personal-devices.aspx)[[15]](#footnote-15), [Managing Azure Active Directory joined devices with Microsoft Intune](http://blogs.technet.com/b/in_the_cloud/archive/2015/05/28/managing-azure-active-directory-joined-devices-with-microsoft-intune.aspx)[[16]](#footnote-16), [Azure AD, Microsoft Intune and Windows 10 – Using the cloud to modernize enterprise mobility](http://blogs.technet.com/b/ad/archive/2015/06/12/azure-ad-microsoft-intune-and-windows-10-using-the-cloud-to-modernize-enterprise-mobility.aspx)[[17]](#footnote-17), and [Windows 10, Azure AD and Microsoft Intune: Automatic MDM enrollment powered by the cloud](http://blogs.technet.com/b/ad/archive/2015/08/14/windows-10-azure-ad-and-microsoft-intune-automatic-mdm-enrollment-powered-by-the-cloud.aspx)[[18]](#footnote-18).

## Capabilities for personal computers and devices

Azure AD Join described in the previous section is for computers and devices owned by your organization and is NOT a replacement of **Workplace Join**. In Windows 10, the Workplace Join world of Windows 7 and Windows 8.x is now replaced by the ability to **add a work account to Windows**.

For personal computers and devices, this new provided feature will be making Bring-Your-Own-Device (BYOD) simpler and more powerful. Users are able to add their work or school account to an application, and make this account available to other applications and web sites. Moreover, adding a work or a school account to a Windows 10 device also both registers and enrolls the device in MDM (if configured), all in one step. Think of this as "Workplace Join on steroids".

Compared to the previous section, both “Azure AD Join” and “add a work account to Windows” register the device in the directory but devices are respectively marked as “Azure AD joined” or “Workplace joined” (*deviceTrustType* attribute in the device object), which can be then used in turn for conditional access. In the former case, this helps providing guidance to IT that the device is corporate-owned and they can apply full management on the device. This is as opposed to the latter case, where IT makes the assumption that the device is a personal device and may apply lighter management in recognition of personal ownership.

With the above, user of a personal device enjoys SSO to work resources, via apps and on the web. This enables to build apps that cater to both enterprise and personal contexts with shared programing stack.

Note For additional information, see the blog post [Azure AD on Windows 10 Personal Devices](http://blogs.technet.com/b/ad/archive/2015/05/21/azure-ad-on-windows-10-personal-devices.as)[[19]](#footnote-19).

## Additional common capabilities

In both corporate owned and personal device cases, it’s easy to configure additional accounts, both work or school and personal, on a Windows 10 device. This includes adding a personal MSA on a work device or a work or school account on a personal device.

This is enabled in a way that makes compliance much easier and reduce user confusion about which data is work vs. play. For example, users may be able to add their personal MSA to a domain joined computer to enable SSO to their personal resources (e.g. personal OneDrive) while connected Windows services continue to be backed by the user’s work account in WSAD/Azure AD.

# Building a test lab environment

As its title suggests, this section guides you through a set of instructions required to build a representative test lab environment that will be used in the next section to configure, test, and evaluate the new capabilities introduced by Azure AD and Windows 10 in various situations.

As we keep mentioning Azure AD from the beginning of this document, you won’t be surprised by the need to have an Azure AD tenant provisioned. Let’s start with that.

## Provisioning an Azure AD test tenant

An Azure AD test tenant can be created through a Microsoft Azure Subscription.

Note 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.

However, the easiest way to provision both an Azure AD tenant and a Mobile Device Management (MDM) environment for the purpose of the test lab certainly consists in signing up to a [Microsoft Office 365 Enterprise](http://office.microsoft.com/en-us/business/office-365-enterprise-e3-business-software-FX103030346.aspx)[[20]](#footnote-20) tenant.

Indeed, such an approach enables to leverage the MDM features built in to Office 365. Thanks to these MDM features, you can view an inventory of all enrolled devices that connect to your organization, create and manage device security policies, remotely wipe a device, and view detailed device reports. These MDM capabilities built in to Office 365 are powered by Microsoft Intune, the Microsoft comprehensive device and app management solution for devices.

Note For more information on Mobile Device Management for Office 365, see the Microsoft TechNet article [Overview built-in Mobile Device Management for Office 365](https://technet.microsoft.com/en-us/library/ms.o365.cc.devicepolicy.aspx)[[21]](#footnote-21) as well as the blog posts [Introducing built-in mobile device management for Office 365](http://blogs.office.com/2014/10/28/introducing-built-mobile-device-management-office-365/)[[22]](#footnote-22) and [Built-in mobile device management now generally available for Office 365 commercial plans](http://blogs.office.com/2015/03/30/announcing-general-availability-of-built-in-mobile-device-management-for-office-365/)[[23]](#footnote-23).

Important note Organizations that need protection beyond what’s included in Office 365 can subscribe to Microsoft Intune and get additional device and app management capabilities. The built-in MDM for Office 365 service, the advanced protection available with Microsoft Intune, or a combination of the two may be right for your organization depending on your needs.

To sign up to a free 30-day Microsoft Office 365 Enterprise E3 trial, follow the instructions at <http://office.microsoft.com/en-us/business/redir/XT104175934.aspx>.

Note For more information, see the article [Sign in to Office 365](http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff637600.aspx)[[24]](#footnote-24).

**For the course of this walkthrough, we’ve provisioned an Office 365 Enterprise (E3) tenant: *litware369.onmicrosoft.com*.** **You will have to choose in lieu of it a tenant domain name of your choice whose name is currently not in use.** **Whenever a reference to *litware369.onmicrosoft.com* is made in a procedure, it has been replaced by the tenant domain name of your choice to reflect accordingly the change in naming.**

## Building an on-premises test lab environment (Optional)

The on-premises test lab environment allows to test scenarios that pertains to a hybrid Active Directory environment such as:

1. Using a federated identity for the Azure AD Join.
2. Testing Windows 10 domain joined devices in a hybrid Active Directory environment.

**If you are not interested in the above listed scenarios, you can skip this section.**

**Every walkthrough that may require this optional on-premises test lab environment later in this document will have an explicit mention for this dependency and in addition will be explicitly identified as “Optional”.**

A hybrid Active Directory environment implies as its name suggest a cross-premises configuration between WSAD and Azure AD.

Considering the involved services, products, and technologies that encompass such a cross-premises configuration, the test configuration should feature:

* In the cloud, an Azure AD tenant that you’ve already provisioned as per previous section,
* In the on-premises, Windows Server Active Directory (WS AD), Active Directory Certificate Services (AD CS), Active Directory Federation Services (AD FS), and Internet Information Services (IIS), to name a few - and the related required configuration.

The following diagram provides an overview of the overall test lab environment with the software and service components that need to be deployed / configured.



A challenge in creating a useful on-premises test lab environment is to enable their reusability and extensibility. Because creating a test lab can represent a significant investment of time and resources, your ability to reuse and extend the work required to create the test lab is important. An ideal test lab environment would enable you to create a basic lab configuration, save that configuration, and then build out multiple test lab scenarios in the future by starting with the base configuration.

Moreover, another challenge people is usually facing with relates to the hardware configuration needed to run such a base configuration that involves several (virtual) machines.

For these reasons and considering the above objectives, we have tried to streamline and to ease as much as possible the way to build a suitable test lab environment, to consequently reduce the number of instructions that tell you what servers to create, how to configure the operating systems and core platform services, and how to install and configure the required core services, products and technologies, and, at the end, to reduce the overall effort that is needed for such an environment. Thus, this document will leverage the Microsoft Azure environment along with the Azure PowerShell cmdlets to build the on-premises test lab environment to test and evaluate the above scenarios at the beginning of this section.

We hope that the provided experience will enable you to see all of the components and the configuration steps both on-premises and in the cloud that go into such a multi-products and services solution.

### Adding an Azure trial to the Office 365 account

Once you have [signed up](http://office.microsoft.com/en-us/business/redir/XT103040305.aspx)[[25]](#footnote-25) and established your organization with an account in Office 365 Enterprise E3, you can then add an Azure trial subscription to your Office 365 account. This can be achieved by accessing the Azure Sign Up page at <https://account.windowsazure.com/SignUp> with your Office 365 global administrator account. You need to select **Sign in with your organizational account** for that purpose.

Note You can log into the Office 365 administrator portal and go to the Azure Signup page or go directly to the signup page, select sign in with an organizational account and log in with your Office 365 global administrator credentials. Once you have completed your trial tenant signup you will be redirected to the [Azure account p](https://account.windowsazure.com/Subscriptions)ortal[[26]](#footnote-26) and can proceed to the Azure management portal by clicking Portal at the top right corner of your screen.

Note This notably enables you to [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)[[27]](#footnote-27) your Office 365 subscription with the access management and security features that Azure AD is offering. While there are and will be ongoing investments in the [Office 365 management portal](https://portal.microsoftonline.com)[[28]](#footnote-28), rich identity and access management capabilities are and will be exposed through the Active Directory section in the [Azure management portal](https://manage.windowsazure.com)[[29]](#footnote-29) first. For example, the [Application Access Enhancements for Azure AD](http://technet.microsoft.com/en-us/library/dn308588.aspx)[[30]](#footnote-30), which provides a streamlined access to [thousands](http://azure.microsoft.com/en-us/marketplace/active-directory/)[[31]](#footnote-31) of cloud SaaS pre-integrated applications like Box, GoToMeeting, Salesforce.com and others, (and even and more in the coming months,) can be only managed today by accessing the directory through the Azure management portal.

**At this stage, you should have an Office 365 Enterprise E3 trial subscription with an Azure trial subscription.**

### Setting up the Azure-based lab environment

**The whitepaper** [**Azure AD/Office 365 Single Sign-On with AD FS in Windows Server 2012 R2 - Part 2bis**](http://www.microsoft.com/en-us/download/details.aspx?id=36391)**[[32]](#footnote-32) fully depicts the setup of such an environment.**

**In order not to “reinvent the wheel”, this document leverages the instrumented end-to-end walkthrough provided in the above whitepaper to rollout a working single sign-on configuration for Azure AD/Office 365 with AD FS by featuring the** [**Azure Active Directory Connect (Azure AD Connect)**](http://www.microsoft.com/en-us/download/details.aspx?id=47594)**[[33]](#footnote-33) tool.**

Note Azure AD Connect provides a single and unified wizard that streamlines the overall onboarding process for directory synchronization (single or multiple directories), password sync and/or single sign-on, and that automatically performs the following steps: download and setup of all the prerequisites, download, setup and guided configuration of the synchronization, activation of the sync in the Azure AD tenant, setup, and/or configuration of AD FS – AD FS being the preferred STS, etc. Azure AD Connect is intended to be the one stop shop for sync, sign-on and all combinations of hybrid connections.

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)[[34]](#footnote-34), and the Microsoft articles [Integrating your on-premises identities with Azure Active Directory](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/)[[35]](#footnote-35) and [Azure Active Directory Connect](https://msdn.microsoft.com/en-us/library/azure/dn832695.aspx)[[36]](#footnote-36).

By following the instructions outlined in this whitepaper along with the provided Azure/Windows PowerShell scripts, you should be able to successfully prepare your Azure-base lab environment based on virtual machines (VMs) running in Azure.

Important note Some more advanced features may specifically require Windows Server 2016. When available, this document will be updated in accordance to reflect such dependencies. As of this writing, Windows Server 2016 is a prerelease software. You can start investigating [Windows Server 2016 Technical Preview 4](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview)[[37]](#footnote-37).

Important note Individual virtual machines (VMs) are needed to separate the services provided on the network and to clearly show the desired functionality. This being said, the suggested configuration to later evaluate the “Azure AD Join” is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab networking environment.

Any modifications that you make to the configuration details provided in the rest of this document may affect or limit your chances of successfully setting up the on-premises collaboration environment that will serve as the basis for the previously outlined scenarios.

Microsoft has successfully built the suggested environment with Azure IaaS, and Windows Server 2012 R2 virtual machines.

**Once completed the aforementioned whitepaper’s walkthrough, you’ll have in place an environment with** **a federated domain in the Azure AD tenant (e.g. *litware369.onmicrosoft.com*), the whitepaper has opted to configure the domain *litware369.com (LITWARE369)*. You will have to choose in lieu of a domain name of your choice whose DNS domain name is currently not in used on the Internet.** For checking purpose, you can for instance use the domain search capability provided by several popular domain name registrars.

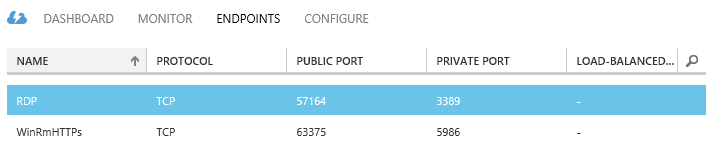
**Whenever a reference to *litware369.com* is made in a procedure later in this document, it has to be replaced by the DNS domain name of your choice to reflect accordingly the change in naming. Likewise, any reference to LITWARE369 should be substituted by the NETBIOS domain name of your choice.**

The Azure-based test lab infrastructure consists of the following components:

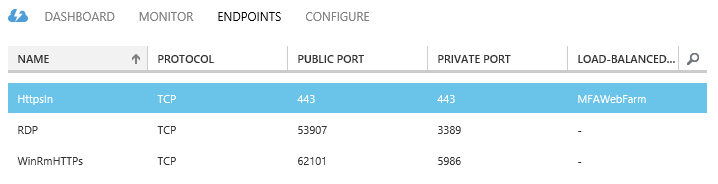
* One computer running Windows Server 2012 R2 (named DC1 by default) that is configured as a domain controller with a test user and group accounts, and Domain Name System (DNS) server.
* One intranet member server running Windows Server 2012 R2 (named ADFS1 by default) that is configured as an enterprise root certification authority (PKI server), and an AD FS federation server.
* One Internet-facing member server running Windows Server 2012 R2 (named EDGE1 by default) that is configured as a Web Application Proxy (WAP) server for the intranet ADFS1 federation server.

Note Windows Server 2012 R2 offers businesses and hosting providers a scalable, dynamic, and multitenant-aware infrastructure that is optimized for the cloud. For more information, see the Microsoft TechNet [Windows Server 2012 R2 homepage](http://technet.microsoft.com/en-US/windowsserver/hh534429)[[38]](#footnote-38).

The above VMs expose one public endpoint for remote desktop (RDP) and another one for remote Windows PowerShell (WinRMHTTPS) as illustrated hereafter.



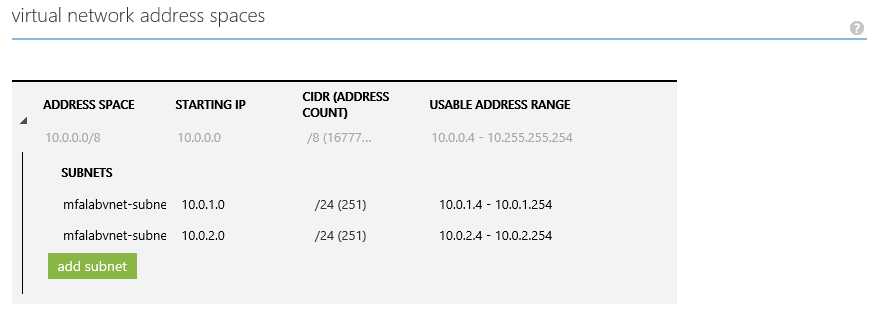
The EDGE1 VM exposes in addition a public endpoint for HTTPS (HttpsIn).



These VMs will enable you to create snapshots so that you can easily return to a desired configuration for further learning and experimentation.

The integrated test lab consists of:

* A first subnet (10.0.1.0/24) that will expose the test lab resources that require Internet connectivity/endpoint(s). It is separated from a second subnet that hosts the corporate intranet resources. The computer on this subnet is EDGE1.
* A second subnet (10.0.2.0/24) that simulates a private intranet. Computers on the Subnet2 subnet are DC1 and ADFS1.



For the sake of simplicity, the same password “*pass@word1*” is used throughout the configuration. **This is neither mandatory nor recommended in a real world scenario.**

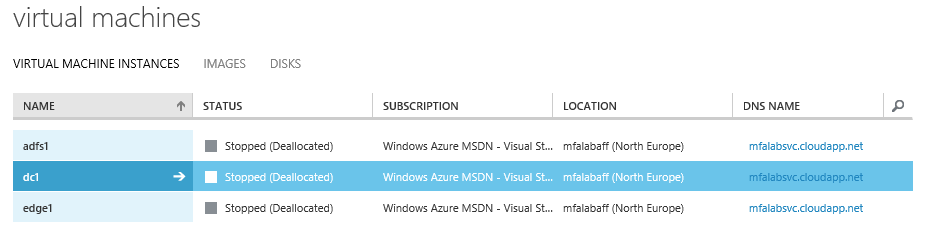
To perform all the tasks in this guide, we will use the LITWARE369 domain Administrator account AzureAdmin for each Windows Server 2012 R2 VM, unless instructed otherwise.

**The base configuration should now be completed at this stage if you’ve followed the whitepaper’s walkthrough.**

**To avoid spending your credit when you don’t work on the test lab, you can shut down the 3 VMs (DC1, ADFS1, and EDGE1) when you don’t work on the test lab.**

To shut down the VMs of the test lab environment, proceed with the following steps:

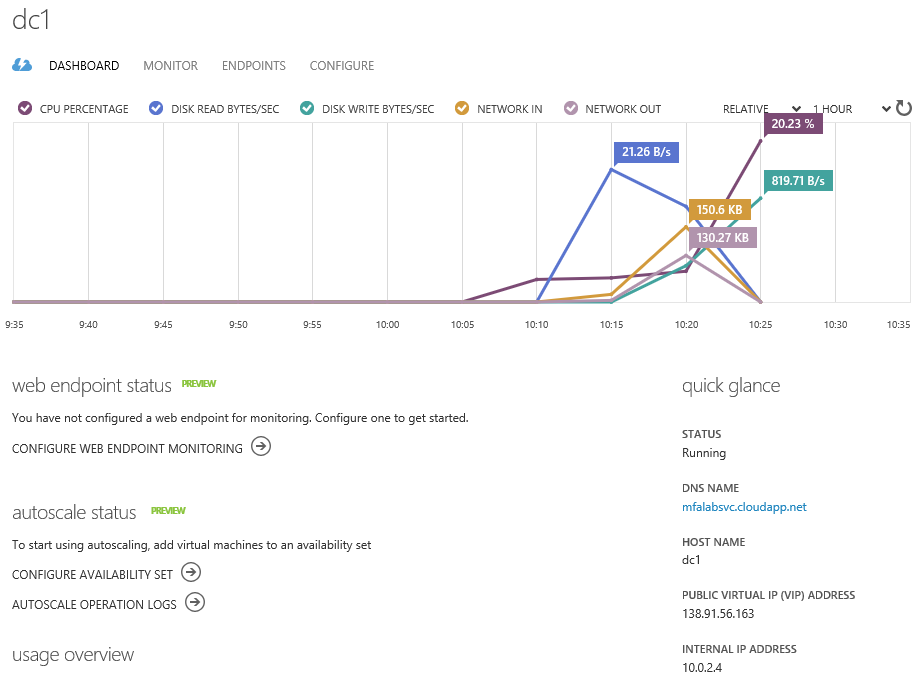
1. From within the Azure management portal, select **VIRTUAL MACHINES** on the left pane.
2. Under **VIRTUAL MACHINE INSTANCES**, select **edge1** and then click **SHUTDOWN** at the tray of the bottom.
3. Repeat step 2 with **adfs1**, and then **dc1**.
4. Once all the allocated resources will be deallocated, the status of the VMs will then change to **Stopped (Deallocated)**.



To resume working on the test lab, you will then need to start in order the DC1 computer, then the ADFS1 one, and finally EDGE1.

To start the VMs of the test lab environment, proceed with the following steps:

1. From within the Azure management portal, select **VIRTUAL MACHINES** on the left pane.
2. Under **VIRTUAL MACHINE INSTANCES**, select **dc1** and then click **START** at the tray of the bottom.
3. Click **dc1**, and then select **DASHBOARD**.



1. Verify under quick glance that the **INTERNAL IP ADDRESS** is set to 10.0.2.4 in our configuration.
2. Select **adfs1** on the left and then click **START** at the tray of the bottom.
3. Repeat step 5 with **edge1**.

**You are now in a position to notably configure the Azure AD Join capability with federated identities thanks on your on-premises test lab environment.**

## Building a Windows 10 image

### Understanding the Windows 10 prerequisites

The new Azure AD Join feature notably illustrated in this document requires Windows 10 Pro or Windows 10 Enterprise editions. Windows 10 Home isn’t able to join a domain. Each version works with a different identity provider with the Professional version straddling both the Microsoft Account (MSA) and the "Azure AD Join” world with the Work or School account in Azure AD:

* Windows 10 Pro edition offers both MSA and Azure AD options.
* Windows 10 Enterprise edition offers only Azure AD.
* Windows 10 Home edition offers only MSA.

Important note The above does not mean that Pro and Enterprise cannot join a traditional WSAD domain on-premises in the traditional manner. During the out-of-box experience (OOBE) illustrated later in this document, you can bypass Azure AD Join, create a local account, and join your device in the traditional manner.

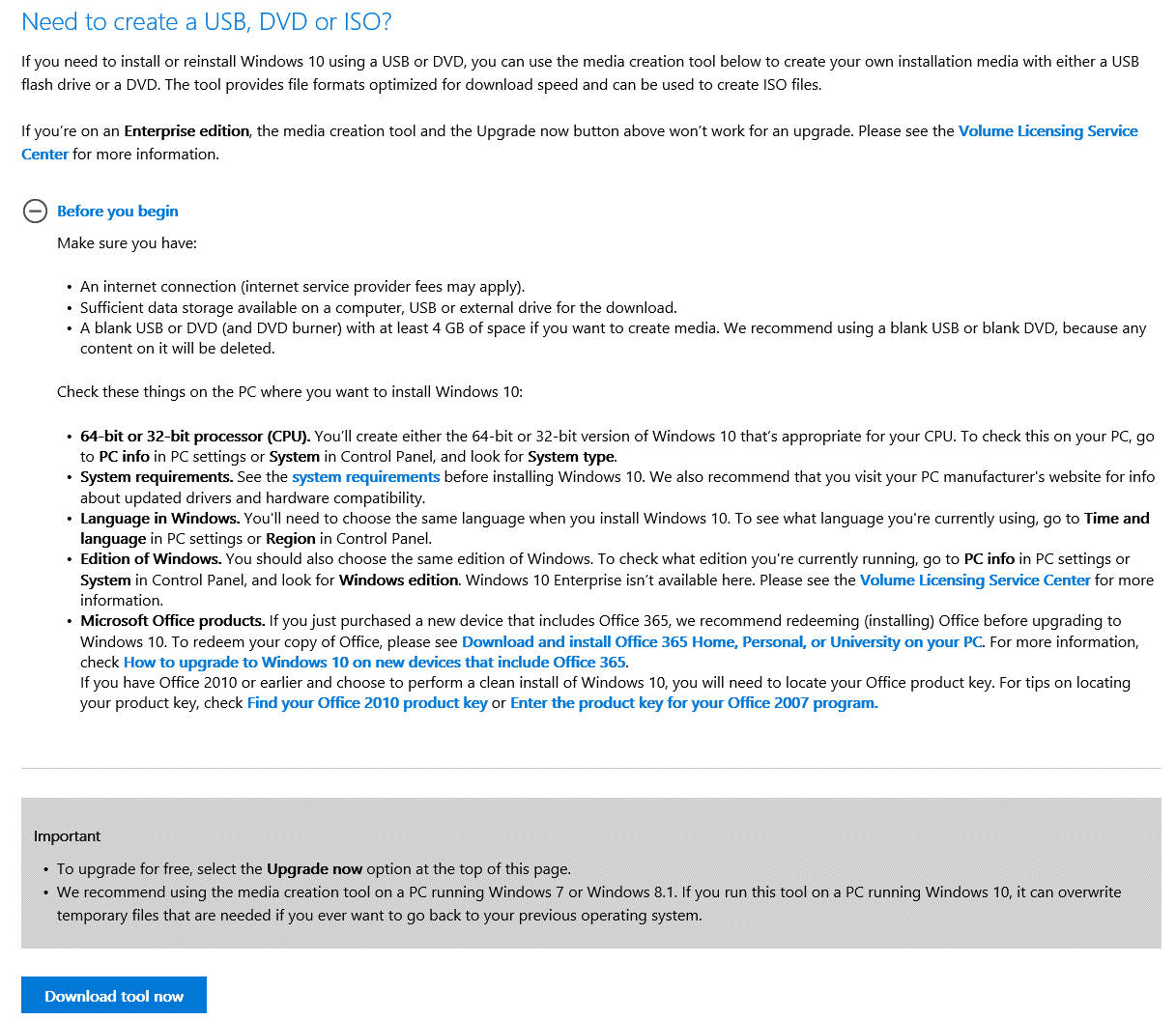
### DownloadingWindows 10

To build a Windows 10 Pro edition ISO file, proceed with the following steps:

1. Open a browsing session from your local machine and navigate to <http://www.microsoft.com/en-us/software-download/windows10>.

Important note As stated on the page, you will need Windows product key. For information about product keys and when they are required, see [Frequently Asked Questions](https://www.microsoft.com/en-us/software-download/faq)[[39]](#footnote-39).

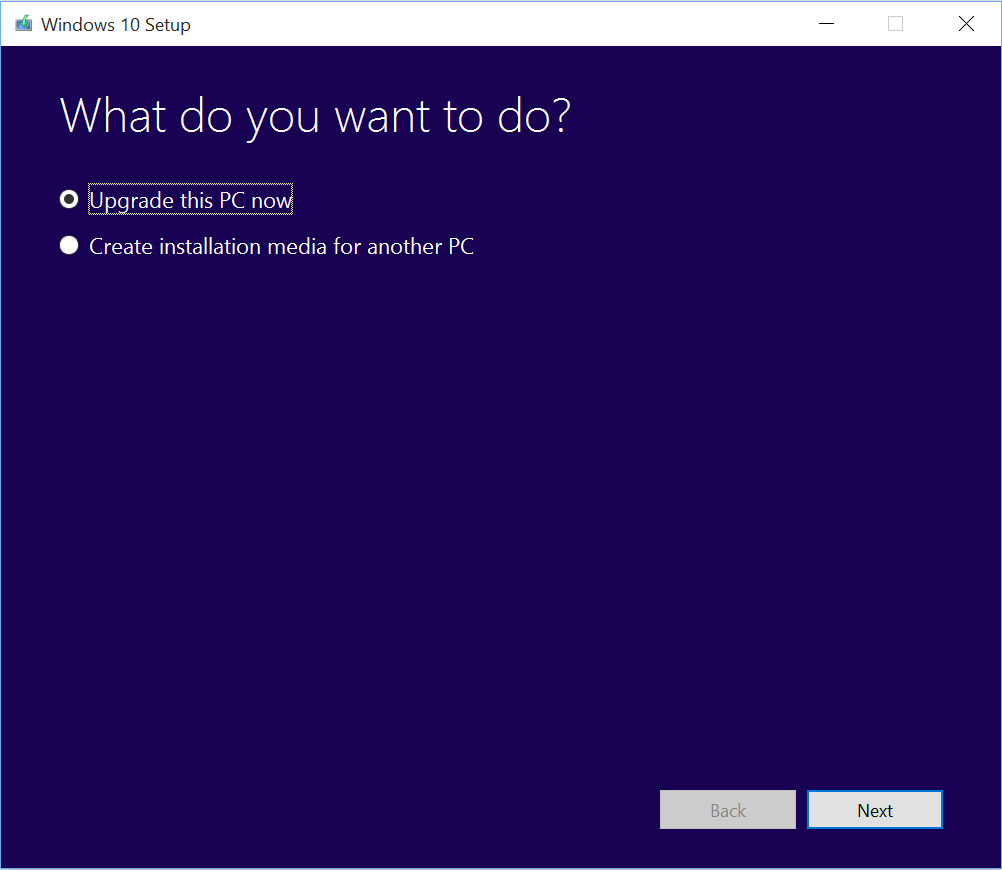
1. Scroll down to the **Need to create a USB, DVD or ISO?** section on this page.



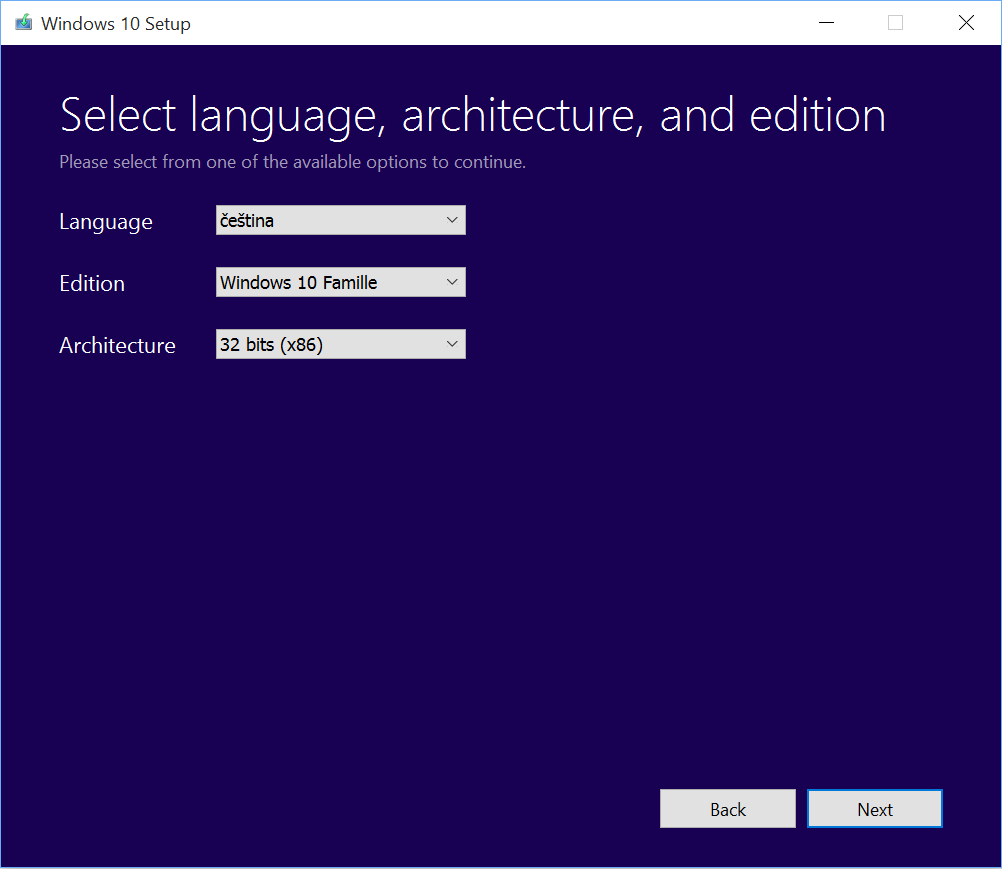
1. Click **Download Tool Now** to download the media creation tool. Amongst various interesting capabilities, the optimization for download speed being one of them, this tool allows the conversation to the ISO file format.

Note For additional information, see [Installing Windows 10 using the media creation tool](http://windows.microsoft.com/en-us/windows-10/media-creation-tool-install?ocid=ms_wol_win10)[[40]](#footnote-40).

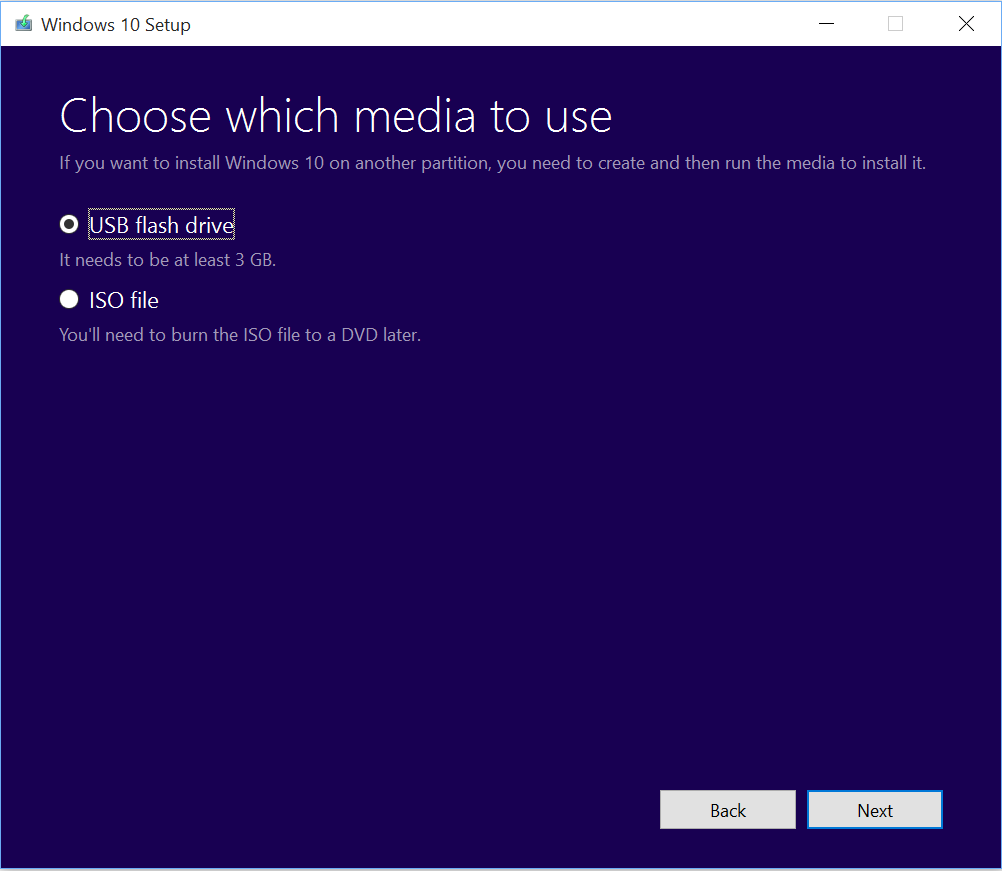
1. Click **Run** to execute the Download Tool (*MediaCreationTool.exe* file).
2. A **User Account Control** dialog pops up. Click **Yes**.
3. A **Windows 10 Setup** dialog shows up.



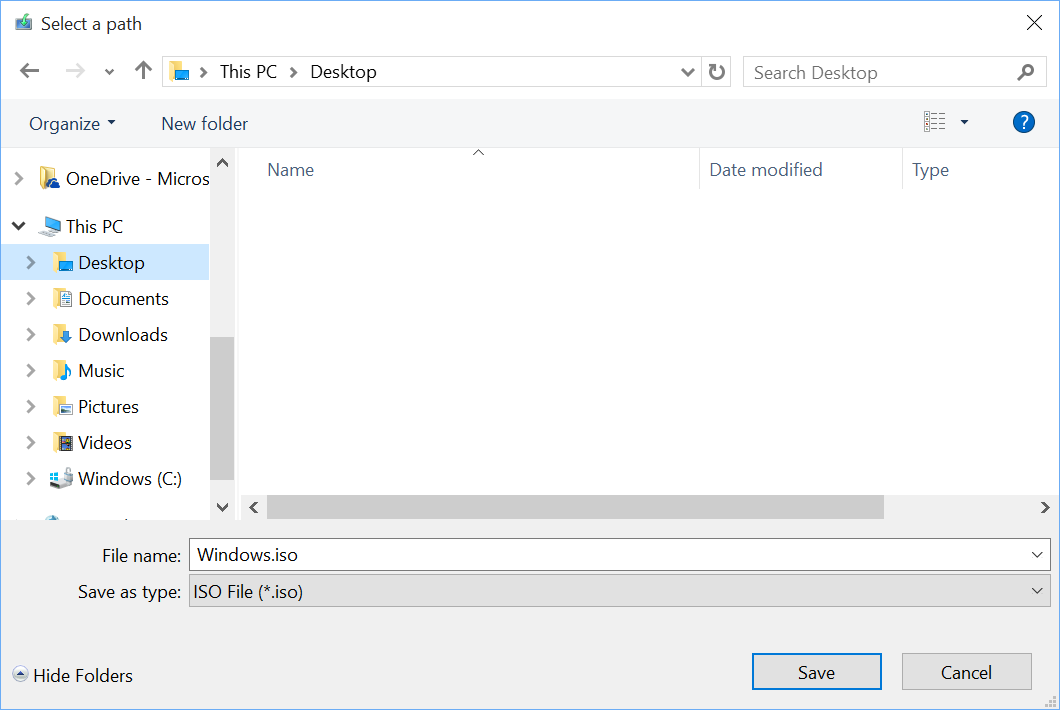
1. On the **What do you want to do?** screen, select **Create installation media for another PC**, and then click **Next**.



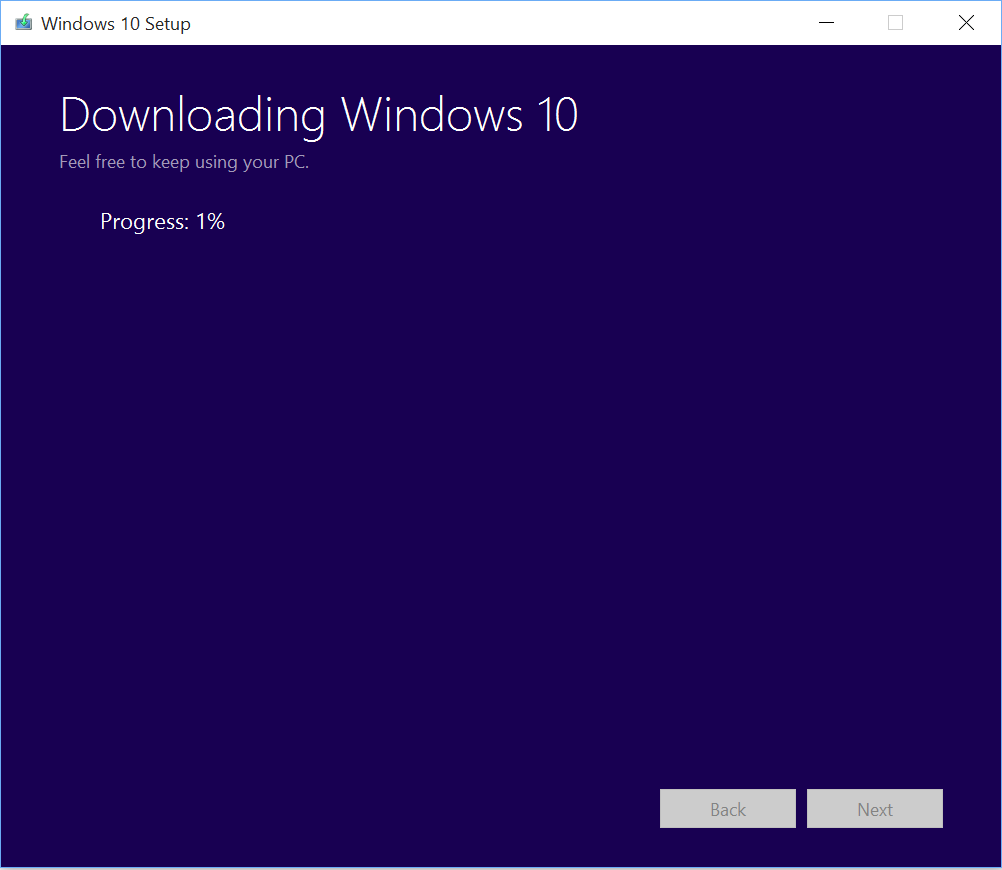
1. On the **Select language, architecture, and edition** Screen, select the following options, and the click **Next**:
   1. In **Language**, select **English (United States)**.
   2. In **Edition**, select **Windows 10 Professional**.
   3. In **Architecture**, select **64 bits (x64)**.



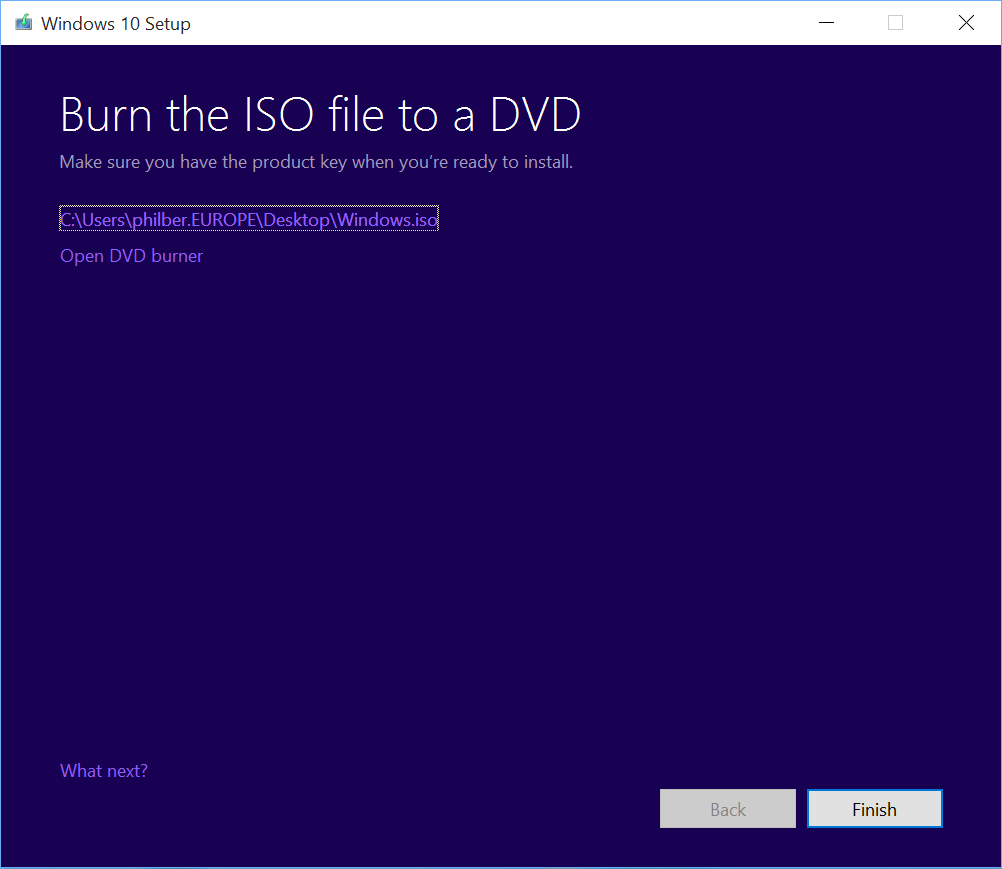
1. On the **Choose which media to use** screen, select **ISO file**, and the click **Next**. A **Select a path** dialog opens up.



1. Specify where to save the ISO file (named *Windows.iso* by default), and then click **Save**.



1. The download starts. After the download is complete and the *Windows.iso* media is created.



1. On the **Burn the ISO file to a DVD** screen, Click **Finish**.

### Creating aWindows 10 virtual machine

To ease the evaluation of the various user experiences, we advise building an individual virtual machine (VM) with the technology of your choice. For that purpose, this document will leverage the Hyper-V virtualization technology as available in Windows and Windows Server products, and more specifically Client Hyper-V.

Note The Windows 8.x Client Hyper-V enables to run more than one 32-bit or 64-bit x86 operating systems at the same time on the same host computer. But instead of working directly with the computer’s hardware, the operating systems run inside a VM. Client Hyper-V is the same computer virtualization technology that was previously available in Windows Server. In Windows 8.x, the technology is built into the non-server version of Windows, often called the “desktop” version because it does not run on server-class hardware. Client Hyper-V provides the same virtualization capabilities as Hyper-V in Windows Server 2012 (R2). For additional information on Client Hyper-V, please refer to the eponym Microsoft TechNet article[Client Hyper-V](http://technet.microsoft.com/en-us/library/hh857623.aspx)*[[41]](#footnote-41)*.

For the sake of brevity, we do not illustrate how to create such a virtual machine via the ISO file download in the previous step.

Note For information on how to create a virtual machine with the Client Hyper-V, see the Microsoft TechNet article [Install the Hyper-V role and configure a virtual machine](https://technet.microsoft.com/en-us/library/hh846766.aspx)[[42]](#footnote-42).

**The rest of the document supposes that you have an up and running Windows 10 virtual machine with an Internet connectivity along with adequate Name/IP resolution.**

# Testing the new capabilities for corporate owned devices

This walkthrough provides instructions for testing the new capabilities provided for **corporate owned devices** for joining Azure AD. As already noticed, joining a Windows 10 device to Azure AD allows you to simplify Windows deployment and access to your organizational apps and resources from that corporate owned device. This represents a new way to configure and deploy corporate owned Windows devices.

With **Azure AD Join**, a new feature of Windows 10, Windows authenticates directly to Azure AD, and NO WSAD Domain Controller (DC) are needed unless you want to use one of course. For that reasons, and as previously covered, two models are provided to organizations:

1. **The “Azure AD Join” model**. This model is a cloud-only model and only requires an Azure AD tenant.
2. **The “Domain Join” model**. This model constitutes an evolution of the traditional WSAD “Domain Join” model. As such, this model implies by nature a hybrid Active Directory environment with an on-premises WSAD infrastructure in place in addition to the above Azure AD tenant, along with at least synchronization capabilities between the two.

This section covers the two models.

**Please ensure that all the prerequisites mentioned earlier in section Building a test lab environment are fulfilled at this stage.**

**Indeed, whilst the former model only supposes that you’ve provisioned your Azure AD test tenant – unless you’d like to conduct some testing with a federated identity -, the latter requires and leverages the optional “on-premises” test lab environment deployed in Azure as per section entitled Building an on-premises test lab environment (Optional).**

Before considering these two models, let’s start by configuring the common settings for the Azure AD test tenant.

## Configuring your Azure AD tenant

Joining a corporate owned device to your Azure AD tenant requires in addition the followings:

* The Azure AD Device Registration Service enabled. The management of device registration policy is available in Azure management portal at <https://manage.windowsazure.com>.
* A DNS CNAME record that points to the A record associated with your Azure AD Device Registration Service record. Additional DNS CNAME record may be required for additional capabilities like the below optional Mobile Device Management (MDM) solution.
* Optional Multi Factor Authorization (MFA) for additional security.
* A Mobile Device Management (MDM) solution integrated with Azure AD. Such a MDM solution is optional, but is typically used in real world scenarios for applying policy to (mobile) devices. Examples are Mobile Device Management for Office 365 and Microsoft Intune. For the sake of the evaluation, and as already mentioned, this capability will be illustrated via Mobile Device Management for Office 365.
* And of course, some test users declared in Azure AD/Office 365.

The next sections guide you through the related steps.

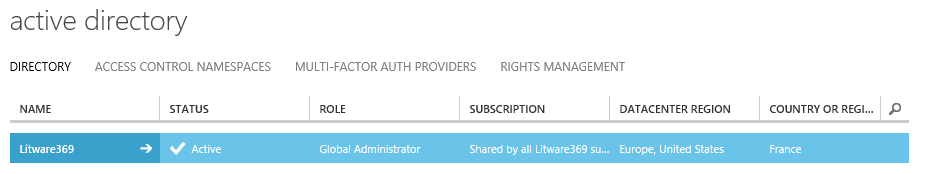
### Activating and configuring the Azure AD Device Registration Service

For an Azure AD user to be able to join their Windows 10 device to the Azure AD tenant (regardless of the chosen identity model (e.g. cloud identity, synchronized identity or federated identity), an IT professional must configure the Azure AD Device Registration Service.

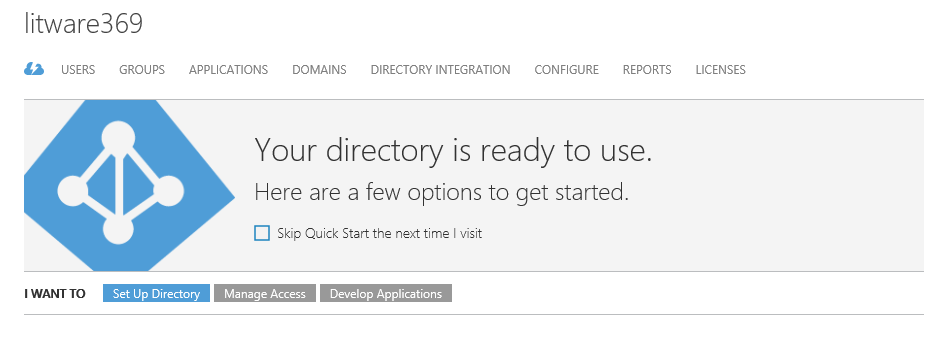
Note For additional information, see the Microsoft MSDN article [Azure Active Directory Device Registration Overview](https://msdn.microsoft.com/library/azure/dn903763.aspx)[[43]](#footnote-43).

To configure the Azure AD Device Registration Service via the Azure management portal, proceed with the following steps:

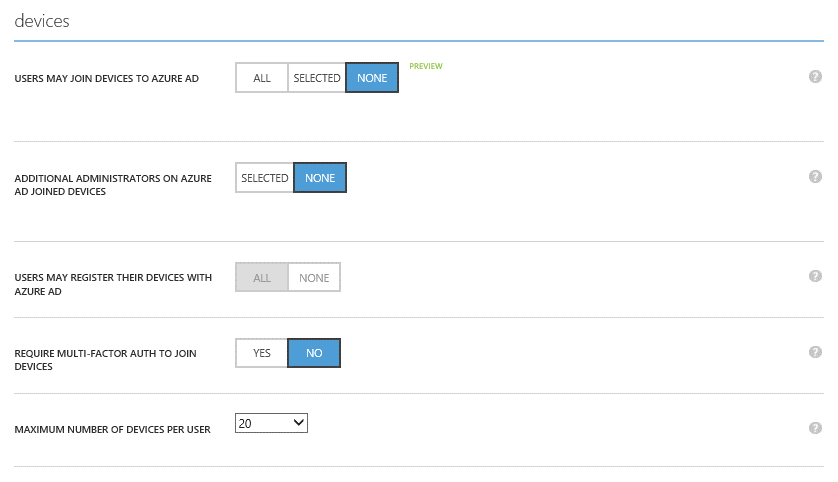
1. Open a browsing session from your local machine and navigate to the Azure management portal at <https://manage.windowsazure.com>.
2. Sign in with your administrative credentials.
3. On the left pane of the Azure management portal, click **ACTIVE DIRECTORY**.



1. On the **active directory** page, at the top, click your directory, e.g. Litware369 in our illustration.

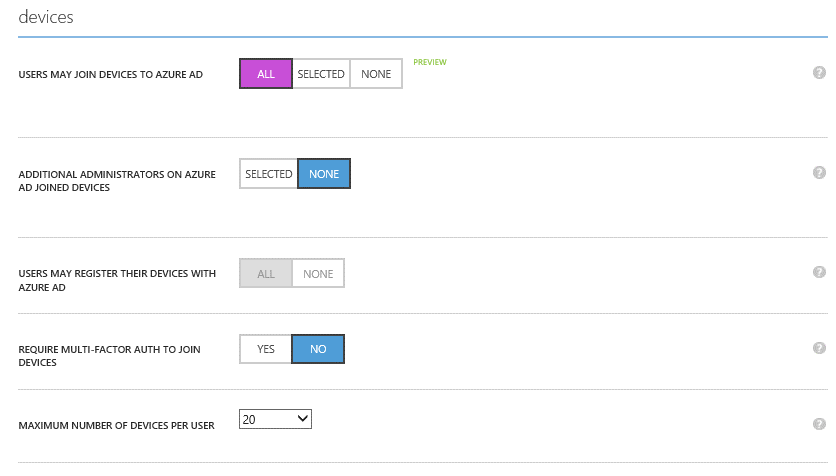


1. Click **CONFIGURE** and scroll down to **devices**.



1. Select **ALL** for **USERS MAY AZURE AD JOIN DEVICES**. **USERS MAY AZURE AD JOIN DEVICES** supersedes **USERS MAY REGISTER THEIR DEVICES WITH AZURE AD** that is thus grayed.

Note Enrollment with Mobile Device Management for Office 365 (or Microsoft Intune or) requires Workplace Join. If you have (already) configured either of these services, ****ALL**** is selected for USERS MAY REGISTER THEIR DEVICES WITH AZURE AD.



1. Select the maximum number of devices you want to authorize per user in **MAXIMUM NUMBER OF DEVICES PER USER**.
2. By default, multi-factor authentication (MFA) is not enabled for the service (**REQUIRE MULTI-FACTOR AUTH TO JOIN DEVICE**). However, MFA is recommended when registering a device. However, before requiring MFA for this service, you MUST prior configure a MFA solution and configure your user accounts for MFA, see next section.
3. Click **SAVE** and allow it to complete.

### Configuring Multi Factor Authorization (Optional)

As stated in the previous section, enabling multi-factor authentication for the Azure AD Device Registration Service requires a prior configuration of the related solution.

The configuration depends on the option you’ve opted for your test lab environment:

1. If you have NOT implement the optional “on-premises” test lab environment deployed in Azure as per section entitled Building an on-premises test lab environment (Optional), you must configure a multi-factor authentication provider in your Azure AD tenant and configure your user accounts for Multi-Factor Authentication.

Specifics instructions are provided in the Microsoft MSDN article [Adding Multi-Factor Authentication to Azure Active Directory](https://msdn.microsoft.com/library/azure/dn249466.aspx)[[44]](#footnote-44) as well as in the whitepaper Leverage Multi-Factor Authentication with Azure AD as part of the same series of documents on Azure AD available on the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[45]](#footnote-45).

1. Otherwise, if you are using AD FS with Windows Server 2012 R2, as instructed in the aforementioned section, you must configure a two-factor authentication module in AD FS, you can follow the walkthrough provided in the whitepaper Leverage Multi-Factor Authentication Server for Azure AD single sign-on with AD FS, which is also part of the same series of documents on Azure AD available on the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=36391)[[46]](#footnote-46).

Note For additional information, see the Microsoft TechNet article [Using Multi-Factor Authentication with Active Directory Federation Services](https://technet.microsoft.com/library/dn394281.aspx)[[47]](#footnote-47).

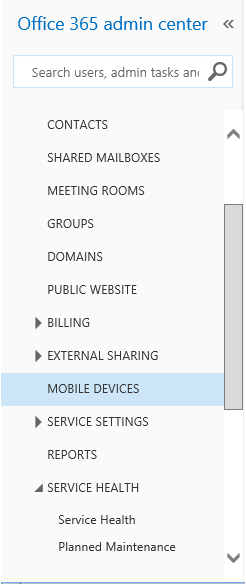
**Beyond the above links to the relevant documentation, this document doesn’t further illustrate the related configuration. For the sake of brevity, we do not illustrate this optional feature in the “Azure AD Join” process.**

### Activating and configuring Mobile Device Management for Office 365 (Optional)

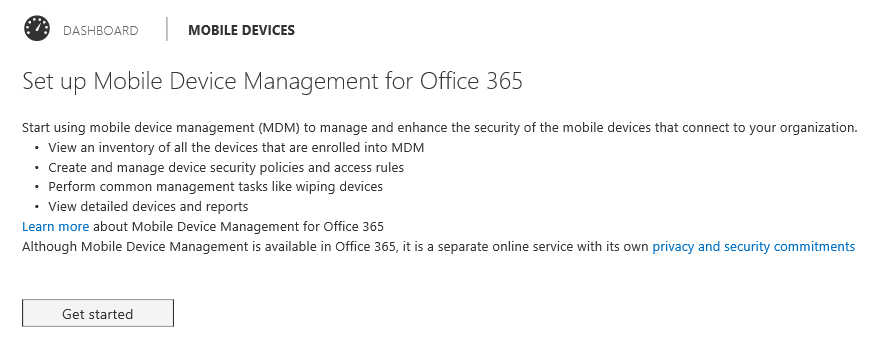
By default, Mobile Device Management for Office 365 is not activated when you sign up for your Office 365 account. To activate and setup Mobile Device Management for Office 365, proceed with the following steps:

Note For additional information, see the Microsoft TechNet article [Overview built-in Mobile Device Management for Office 365](https://technet.microsoft.com/en-us/library/ms.o365.cc.devicepolicy.aspx)[[48]](#footnote-48) along with [Manage mobile devices in Office 365](https://support.office.com/en-us/article/Manage-mobile-devices-in-Office-365-dd892318-bc44-4eb1-af00-9db5430be3cd)[[49]](#footnote-49).

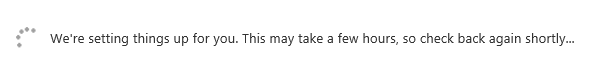
1. Open a browsing session from your local machine and navigate to the Office 365 management portal at <https://portal.microsoftonline.com>.
2. Sign in with your administrative credentials.
3. If the Office 365 admin center is not visible, open the apps launcher in the top left corner and select **Admin**.



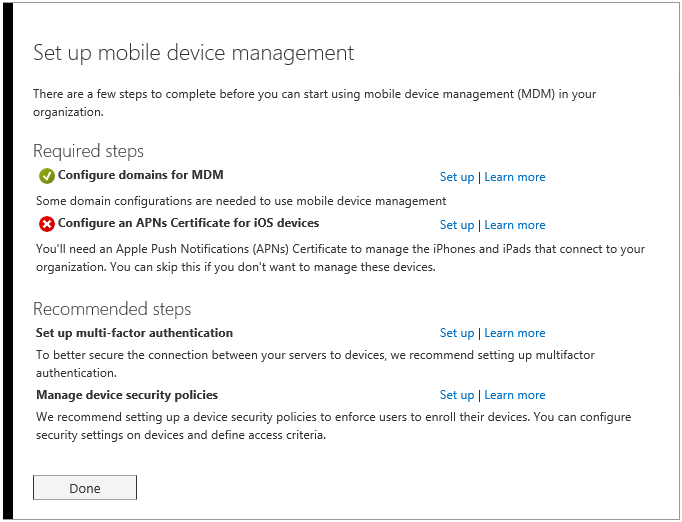
1. In the left pane of the admin center, click **MOBILE DEVICES**.



1. Under **Set up Mobile Device Management for Office 365**, click **Get started to kick off the activation process**. It may take some time for the service to be provisioned.



1. When it's done, you'll see the new **Mobile Device Management for Office 365** page.
2. Complete the required steps to finish setup. You may need to click **Manage settings** on this page to see the following settings.



1. Click **Done**.
2. At this stage, your Azure AD/Office 365 tenant is enabled for MDM. You can then enable some policies. To do so, click **Manage device security policies and access rules**. You’ll be taken to **Compliance Center** where you’ll click **Manage device access settings**.

Note For additional information, see the Microsoft TechNet article [Create and deploy device security policies](https://technet.microsoft.com/en-us/library/ms.o365.cc.newdevicepolicy.aspx)[[50]](#footnote-50).

### Configuring the domains for Azure AD Device Registration Service and Mobile Device Management for Office 365

**If you don't have a custom vanity domain associated with your Azure AD/Office 365 subscription, you can skip this section.**

This is the case in the suggested test lab environment if you’ve decided not to implement the optional steps outlined in section Building an on-premises test lab environment (Optional). In this case, you only have the default domain (e.g. *litware369.onmicrosoft.com* in our illustration).

Otherwise, if you’ve rather opted to configure the equivalent of the vanity domain litware369.com (LITWARE369) in our illustration with the domain name of your choice whose DNS domain name that is currently not in used on the Internet, you'll need to add DNS records for the domain at your DNS host.

If you've added the records already, you're all set. After you add these records in your domain registrar, users in your organization who sign in on their device with an email address that uses your custom domain can register to your Azure AD tenant and then be redirected to enroll in Mobile Device Management for Office 365.

To add these record, proceed with the following steps:

1. Find your domain registrar in the list provided in [Create DNS records for Office 365 when you manage your DNS records](https://support.office.com/en-gb/article/create-dns-records-for-office-365-when-you-manage-your-dns-records-b0f3fdca-8a80-4e8e-9ef3-61e8a2a9ab23)[[51]](#footnote-51) and select the registrar name to go to step-by-step help for creating DNS records.
2. Use those instructions to add the following two records for your vanity domain:

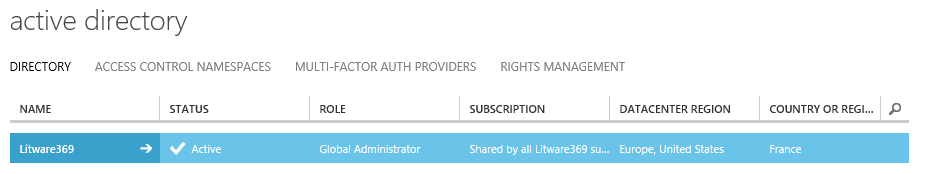
|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Value | TTL |
| enterpriseregistration | CNAME | enterpriseregistration.windows.net | 3600 |
| enterpriseenrollment | CNAME | enterpriseenrollment.manage.microsoft.com | 3600 |

1. After you add the two records, go back to **Office 365 admin center** > **MOBILE DEVICES** > **Manage settings** to complete setup.

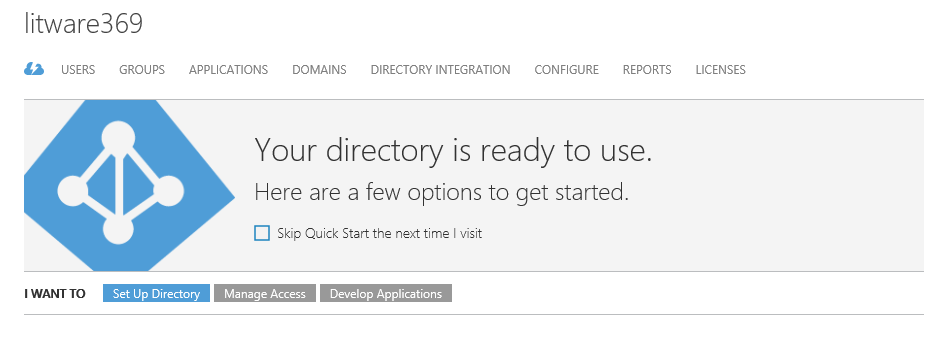
### Creating a test user

To create a test user, proceed with the following steps:

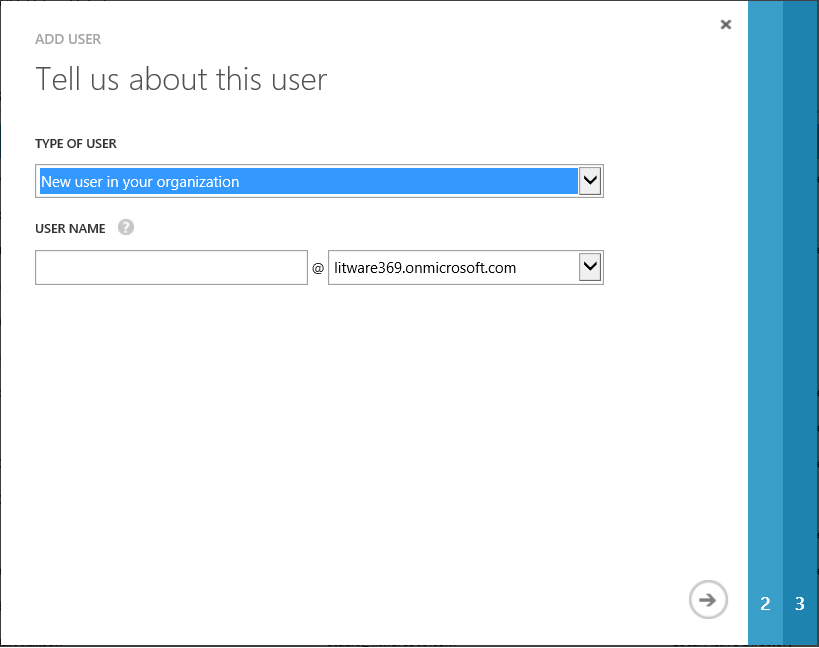
1. Open a browsing session from your local machine and navigate to the Azure management portal at <https://manage.windowsazure.com>.
2. Sign in with your administrative credentials.
3. On the left pane of the Azure management portal, click **ACTIVE DIRECTORY**.



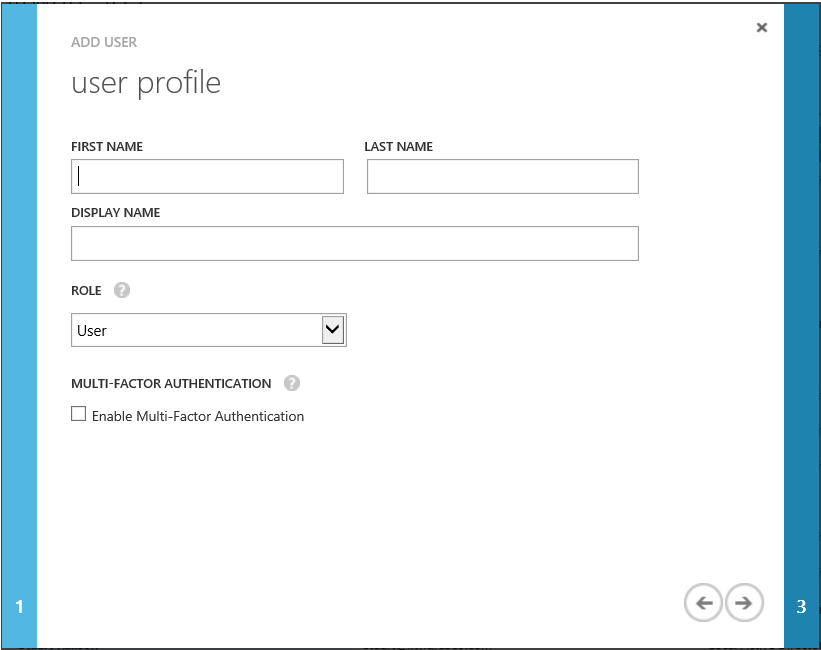
1. On the **active directory** page, at the top, click your directory, e.g. Litware369 in our illustration.



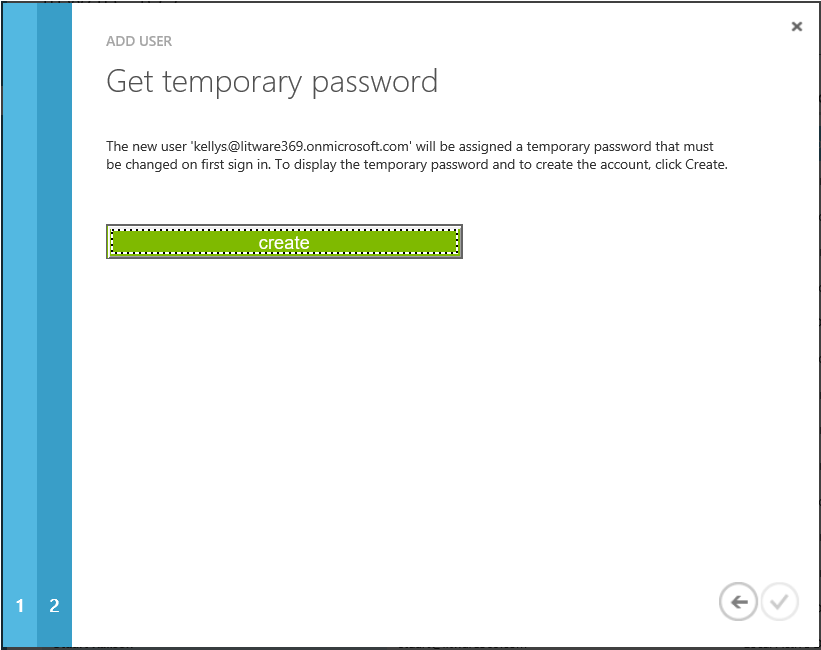
1. Click **USERS** and then **ADD USER** at the bottom of the page. The process of adding a new user start with the page **Tell us about this user**.



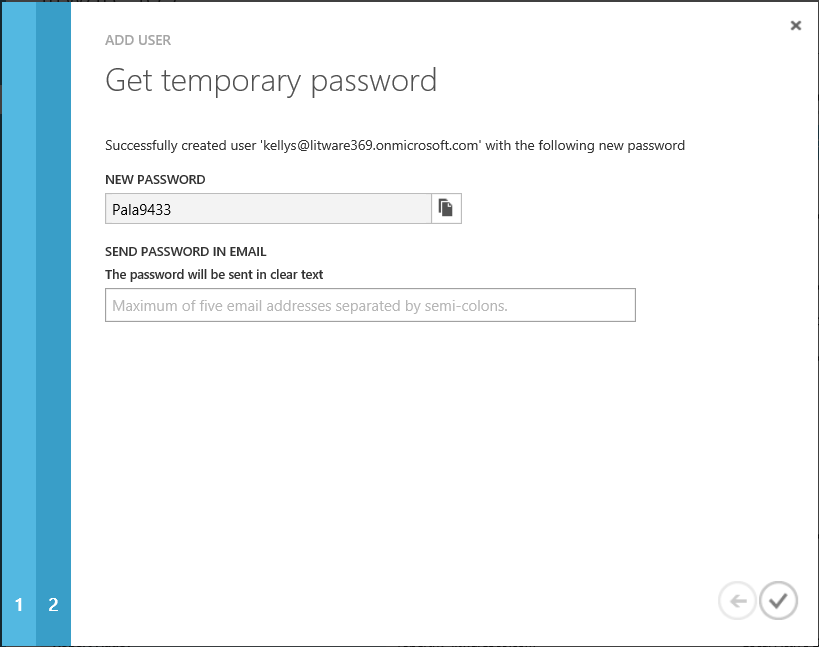
1. Keep New user in your organization and specify the user name, for example “*kellys*” in our illustration. Select the arrow key to go to the next page **user profile**.



1. Fill in the user's first name and last name plus their display name in the eponym fields, for example respectively type “*Kelly*”, “*Smith*”, and “*Kelly Smith*”. Make sure the role is set to **User**. Do not select Multi-Factor Authentication.
2. Click the right arrow to go to the next page **Get temporary password**.



1. Click **create**.



1. A new temporary password is created. You can either copy the password to the clipboard or send it in email in clear text. Write down the password and then click the check box to complete the new user process.

Our new user *kellys@litware369.onmicrosoft.com* is created and we have our temporary password. You can copy and paste the password from here or email it to the user.

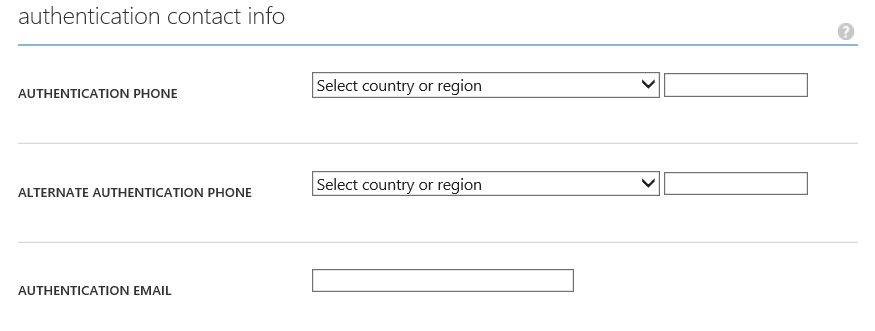
Note Passwords emailed from this screen are sent as clear text and may not be secure. In a production environment, encourage the user to change their password as soon as possible.

Note If you would like to test the accounts before evaluating the new capabilities in Windows 10 in the rest of this document, try logging on to <http://manage.windowsazure.com> with the new account and test. If this is the first time you have used the account, you will be prompted to change your password.

1. Change the password, for example to “*pass@word1*” in our illustration.

If you’d like to optionally configure a multi-factor authentication, you’ll have to allow the users to prove who they say they are when performing the “Azure AD Join” process. If so, proceed with the following additional optional steps:

1. Click **Kelly Smith** and select the **WORK INFO**.
2. Scroll down and locate **authentication contact info**.



1. The authentication contact is either a telephone call, a text message, or an application on your phone:
2. Fill in a valid phone number you can test with such as your cell phone or your desk phone.
3. Add an alternate authentication phone number.
4. Add an authentication email.
5. Do not forget to save your changes. Click **SAVE** in the bottom of the tray.

**Your Azure AD tenant (along with additional services) are now configured at this stage. This allows a user to join their Windows 10 device to Azure AD.**

## Joining a device to Azure AD in a cloud-only environment

This section provides instructions for configuring and testing the “Azure AD Join” model for corporate owned devices.

As already noticed, joining a Windows 10 device to Azure AD allows you to simplify Windows deployment and access to your organizational apps and resources from that corporate owned device. This represents a new way to configure and deploy corporate owned Windows devices.

As Windows authenticates to Azure AD in the cloud, one should note that this model works with both cloud and federated identities. As far as the latter is concerned, it requires and leverages the optional “on-premises” test lab environment deployed in Azure as per section Building an on-premises test lab environment (Optional). In this case, the authentication is delegated to the on-premises identity infrastructure

The next sections guide you through these two scenarios and their pre-requisites if any and describe in the context of our test lab environment each of these related steps.

### Joining a device in the out-of-box experience with a cloud user

This section will take what you’ve learned and configured so far and build upon it by demonstrating how you can join a Windows 10 device to your corporate owned Azure AD tenant. As you will see, this brings significant flexibility and cost savings to the deployment process within the organization. End-users will be able to automatically Azure AD join during the initial startup experience, i.e. the out-of-box experience (OOBE), which will register the device in the organization's Azure AD tenant and enroll it in their Mobile Device Management (MDM) solution, for example Mobile Device Management for Office 365 in our configuration.

As a reminder, only Pro and Enterprise versions of Windows 10 can join Azure AD. The experience will be slightly different for both. See later in this section.

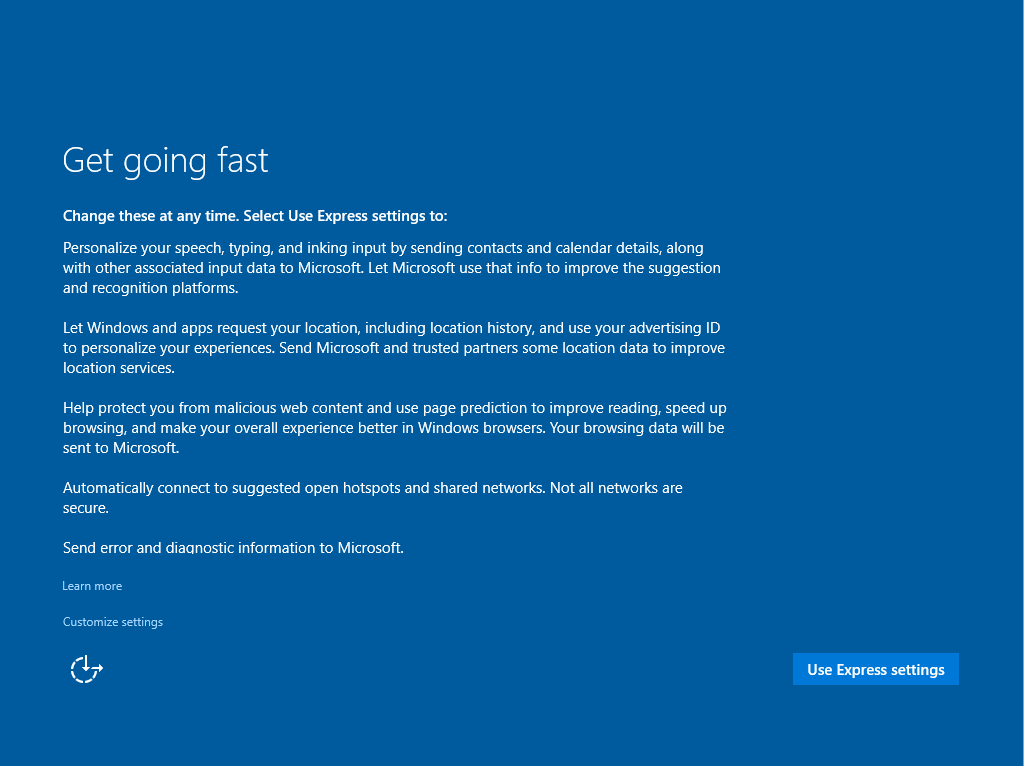
This section requires a new installation of Windows 10 so you can walk through the out-of-box experience (OOBE).

Note Based on the image you may have built as part of the setup of the test lab environment, you can manage the various installations suggested in this document by leveraging for instance the checkpoints features of the Client Hyper-V environment on your local Windows machine.

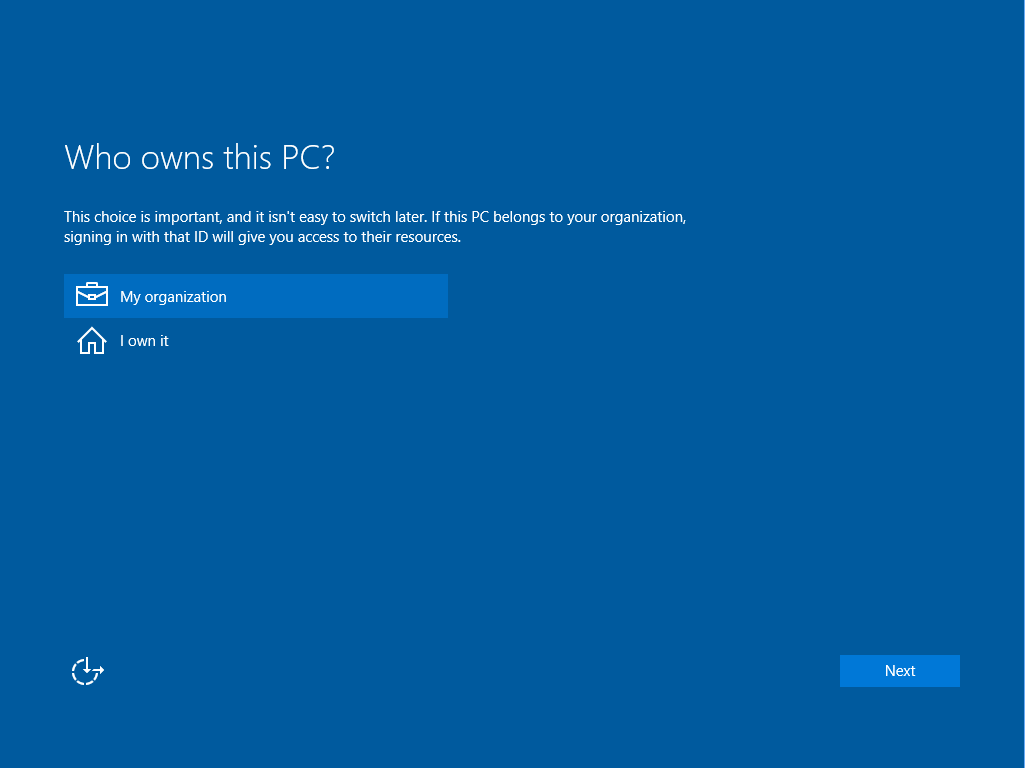
A sign-in to the Azure AD tenant will automatically authenticate cloud users. For this to work, this new installation of Windows 10 will simply need an Internet connectivity with Name/IP resolution.

With all the above in mind, let’s walk through the out of box experience (OOBE). Proceed with the following steps:

1. Boot a new image of Windows 10 that fulfills the pre-requisites described above. After booting, you’re presented with the regional settings screen.

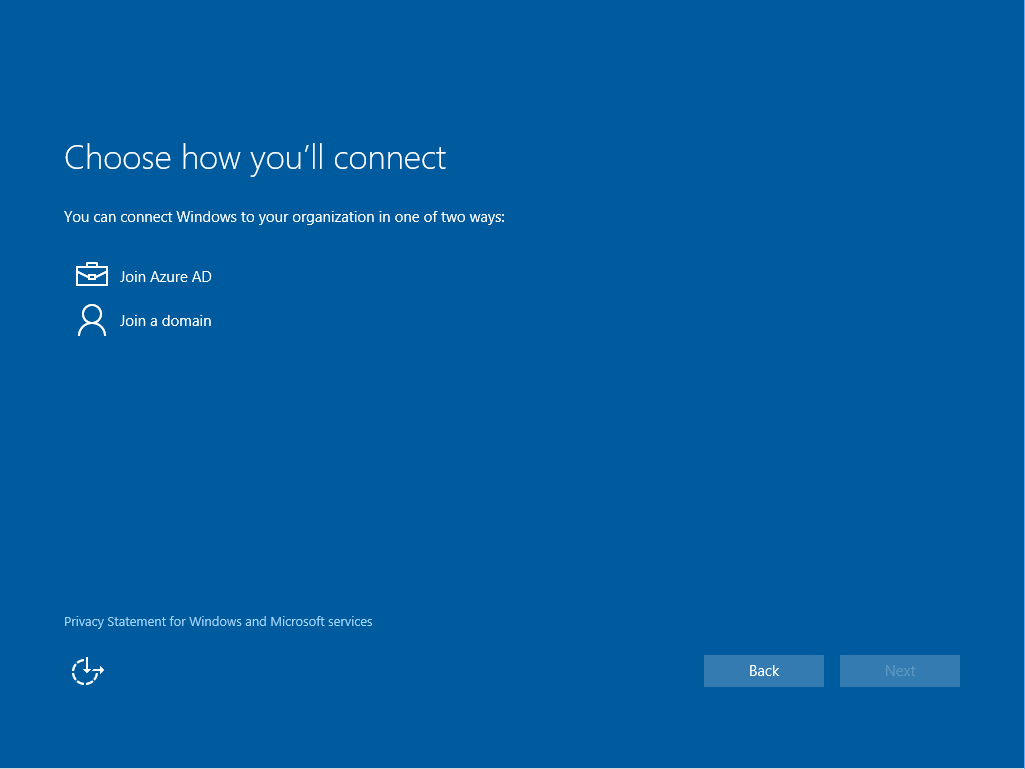


1. Configure your country or region, app language, keyboard layout, and time zone as necessary and click **Next**
2. Click **Use express settings**. If the connection to the Internet works, you should be then presented with a big question: **Who owns this PC?**



The above two options and depending upon your choice will determine what resources you can access:

1. **My organization**. This option indicates that you will sign in with your work account in WSAD/Azure AD and be able to benefit from single sign-on (SSO) for corporate resources.
2. **I own it**. This option during OOBE will prompt you for a Microsoft Account (MSA) and is used by consumers. If you do need to access corporate devices, you will not experience SSO to those applications.
3. For this scenario, select **My organization**, and then click **Next**. Allow it to spin and move to the next screen.

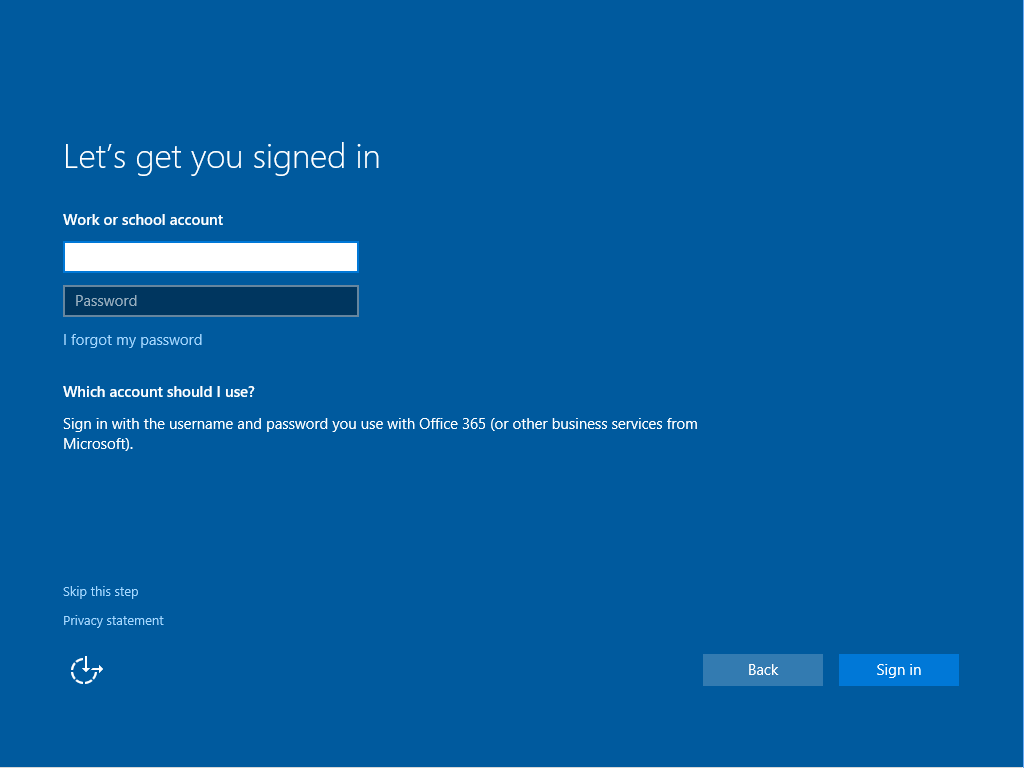


The above two options and depending upon your choice will determine how to connect Windows 10 to your organization:

1. **Join Azure AD**. This option corresponds to the Azure AD Join and you will prompt you for your Azure AD/Office 365 work or school account.
2. **Join a domain**. This option allows you to join your machine to the traditional WSAD domain on-premises using your corporate work account

Note This would be a good place to create a checkpoint of your virtual machine in the event you make a mistake or would like to see what a mistake looks like.

1. For this scenario, select **Join Azure AD**, and then click **Next**. It may take a few minutes to get to the next screen.



1. Enter your Azure AD account credential to join your Windows 10 device to your Azure AD, for example, in our illustration:

Username: *kellys@litware369.onmicrosoft.com*

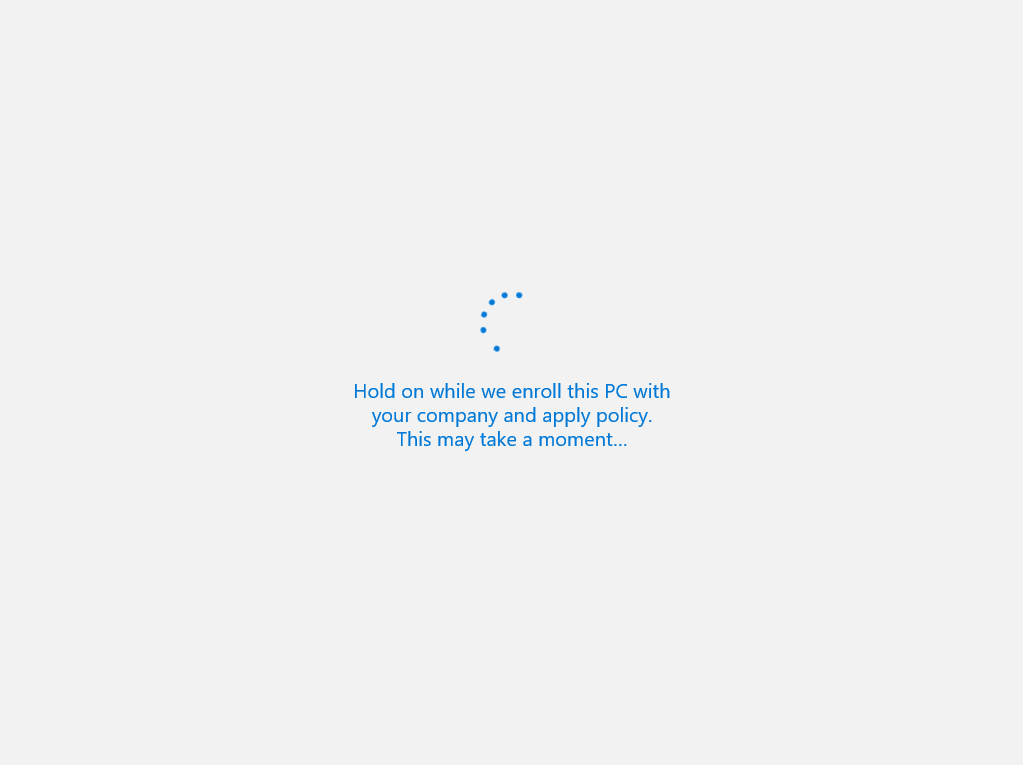
Password: *pass@word1*

1. Click **Sign in**. You are then prompted to update your password if this is the first time you have logged on with this account. Please do so and click **Sign in** once more. If you have setup the optional multi-factor authentication, you are also prompted to provide a second factor of authentication at this point. This is not illustrated here.
2. Azure AD then checks whether the device should be enrolled in a MDM solution, for example Mobile Device Management for Office 365 in our configuration. ((Windows 10 uses a secure channel over any internet connection to communicate with Azure AD). If so, a screen appears informing you of the automatic device enrollment process.

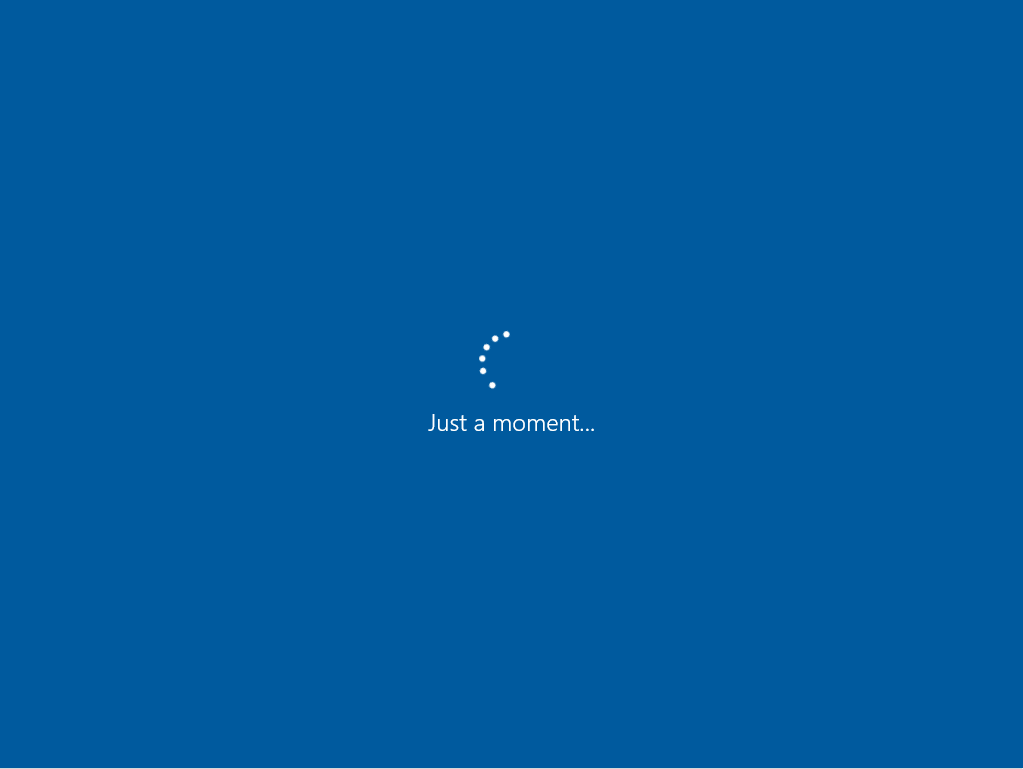
Note If the organization specifies a custom Terms of Use, the user will need to consent to continue through enrollment.

Windows 10 registers the device in the organization’s Azure AD tenant and enroll it in the MDM solution.

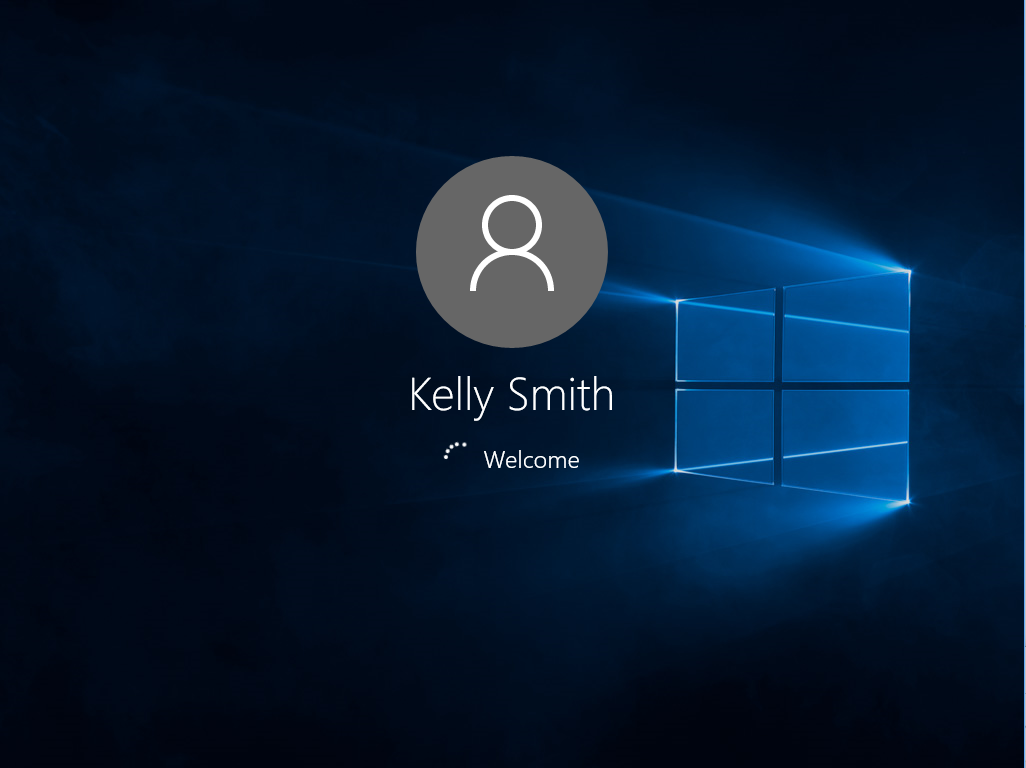
Note Some organizations may choose to download apps and policy as part of the “Azure AD Join” process, once the device is enrolled in the MDM solution, and as per solution features.



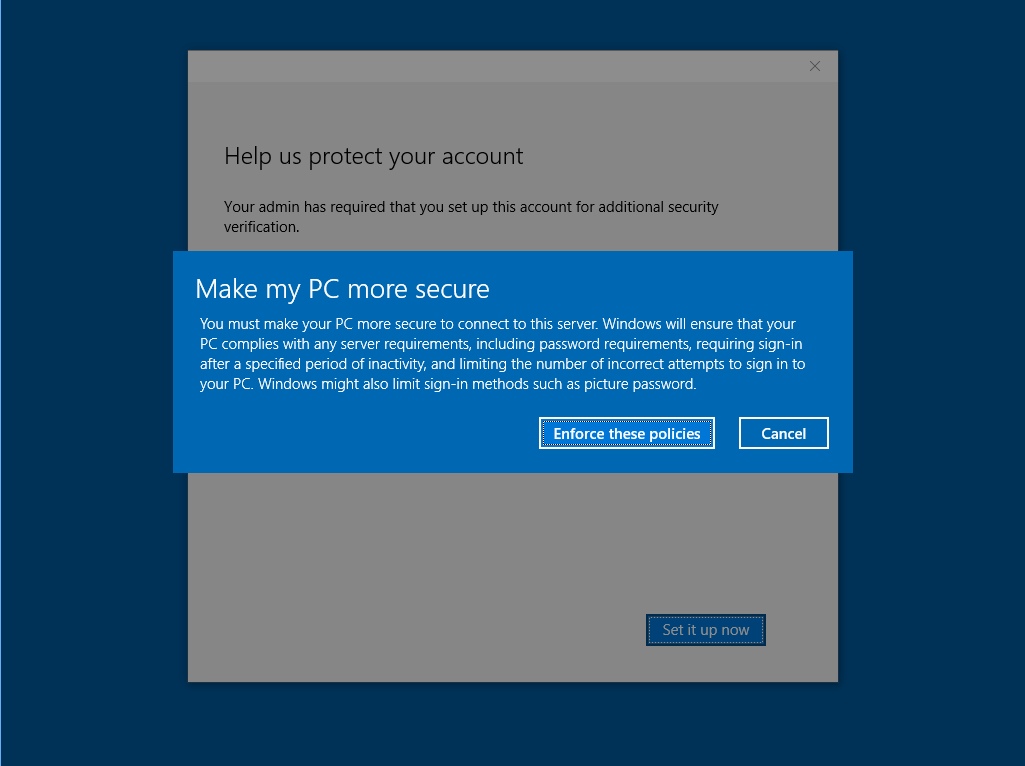
1. The login continues.



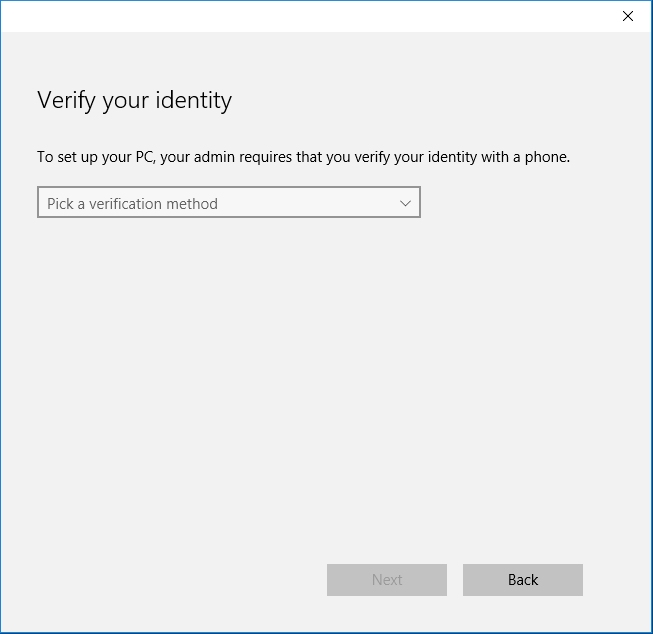
1. Wait for it to complete.



1. A successful logon will proceed to setting up a work PIN, your Microsoft Passport gesture. Prior to doing that, you’re invited to make your PC more secure.



1. Click **Enforce these policies**. A **Verify your identity** dialog shows up.



* 1. Select one of the verification methods listed, and then click **Next**:

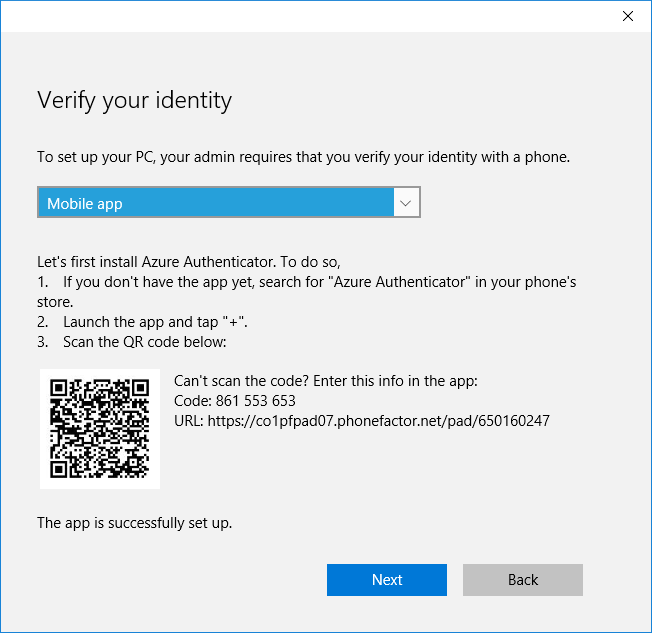
|  |  |
| --- | --- |
| 1. Text message |  |
| 1. Phone call |  |
| 1. Mobile app |  |

We illustrate here the latter one. You can off course select the one that is the most appropriated in your own context.

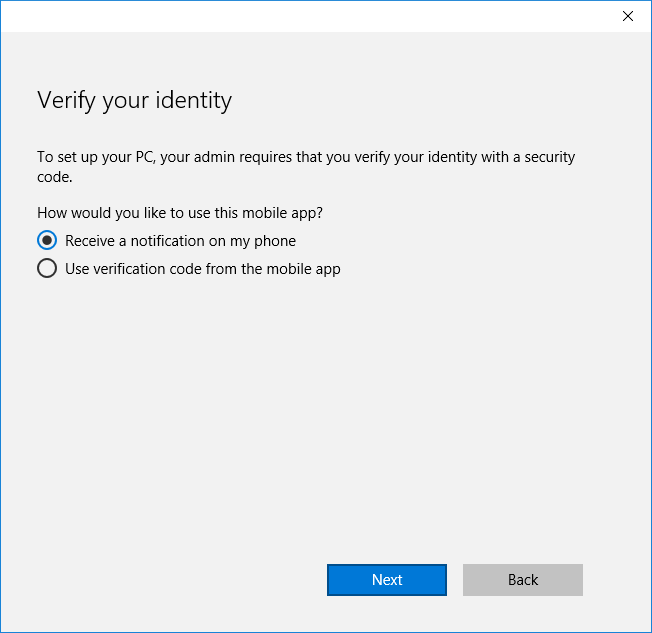
* 1. **The mobile app method, as its name suggest, requires a prior installation on your mobile phone of the Azure Authenticator app.** Install the app from the [Windows Phone](http://aka.ms/windowsphoneappblogpost)[[52]](#footnote-52), [iOS](http://aka.ms/iosappblogpost)[[53]](#footnote-53) or [Android](http://aka.ms/androidappblogpost)[[54]](#footnote-54) app store.

Note The Azure Authenticator allows you to secure your account with two-step verification. With two-step verification, you sign in using something you know (your password) and something you have (your mobile device). For additional information on Azure Authenticator app, see the blog post [Try the new Azure Authenticator application!](http://blogs.technet.com/b/ad/archive/2015/06/29/try-the-new-azure-authenticator-app.aspx)[[55]](#footnote-55),

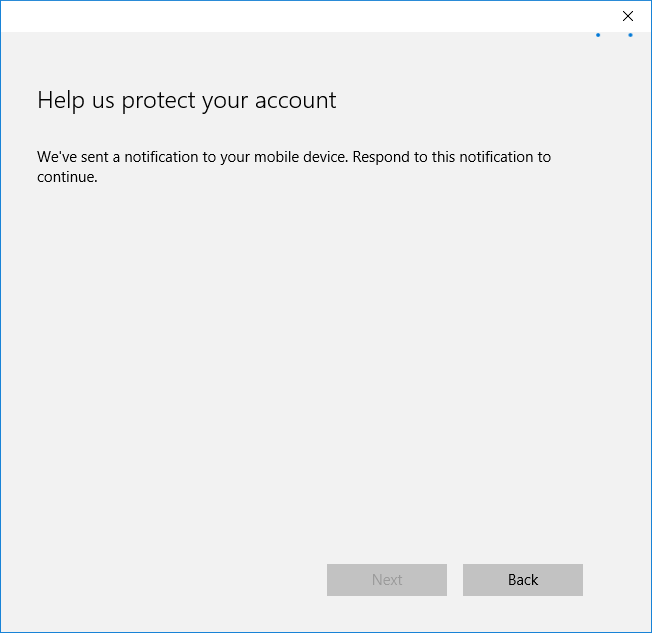
* 1. Launch the app and tap “+”.
  2. Scan the above QR code.



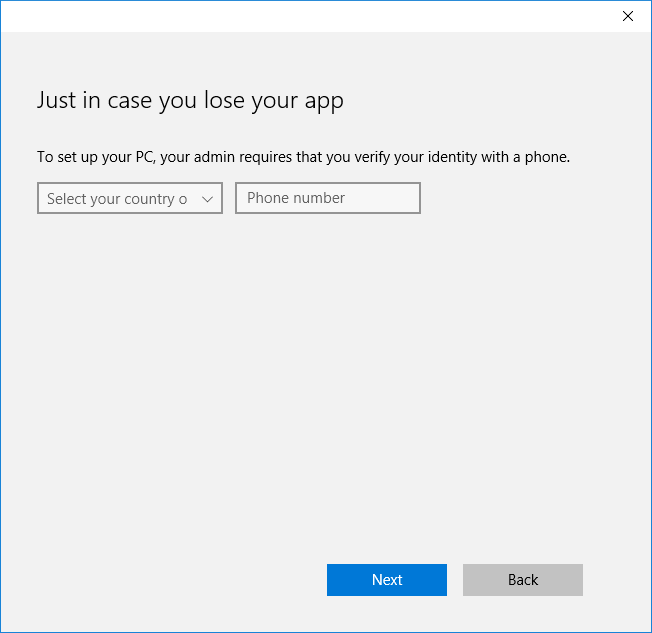
* 1. Click **Next**. Now that the app is successfully installed, you’re invited to specify how you’d like to use the app: receive a notification on your phone vs. use a verification code from the app.



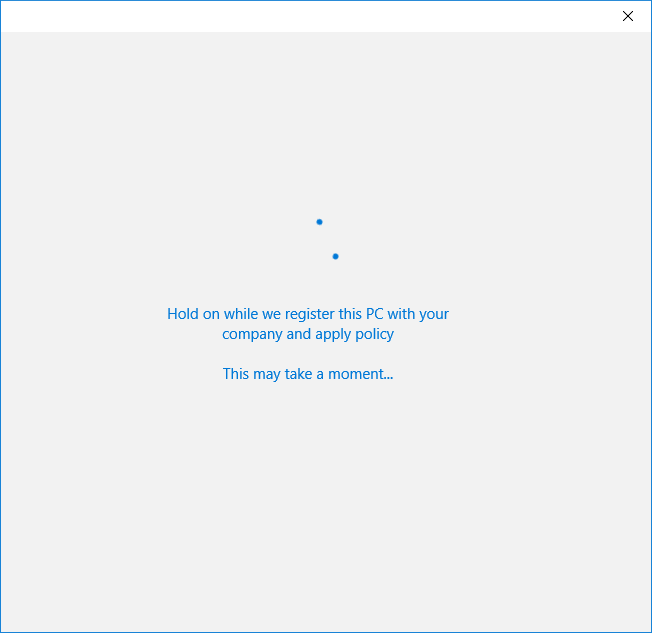
* 1. Select **Receive a notification on my phone**, and then click **Next**.



* 1. Tap **Verify** on your app.

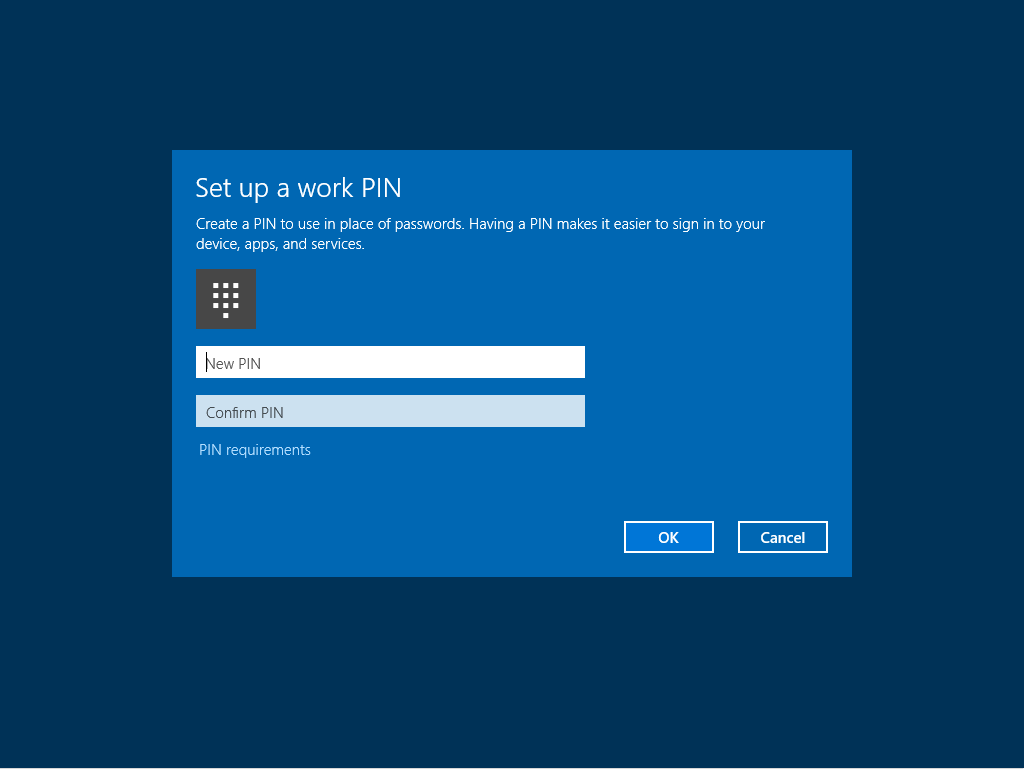


* 1. Set your phone number, and then click **Next**.



* 1. The company policies are applied.

1. You will proceed to setting up a work PIN, your Microsoft Passport gesture.



Note Microsoft Passport, formerly called Next Generation Credentials or NGC constitutes a long-term initiative for Microsoft to aid in securing credentials making Windows 10 the most secure Windows Microsoft have shipped. Microsoft Passport is specifically to remove the need to enter user name and passwords for all compliant websites, applications, and resources. For that purpose, Microsoft Passport seeks to change the raw user credential from a symmetric, memorized secret to an asymmetric, hardware (TPM 1.2 or 2.0) bound or software (based on policy) key. Unlocking this key with a gesture will provide users access to resources without using passwords. Supported gesture are PIN as well as biometric gestures with Windows Hello, a new feature of Windows 10.

For the IT professional, Microsoft Passport means an ability to get strong authentication guarantees similar to virtual smart cards from both corporate-owned (and personal, a.k.a. BYOD) devices, with a significantly reduced deployment and management burden. Microsoft Passport adds the ability to manage various aspects of this, such as PIN complexity and reset.

From a technology perspective, Microsoft Passport is a container of keys. The keys and container are managed as securely as the platform permits, which means hardware-bound where possible. Each key requires authentication at key-specific intervals (ranging from per transaction to once every set amount of time). The keys stored in the Microsoft Passport container will be used to authenticate at a supported Identity Provider – like Azure AD and WSAD in [Windows Server 2016 Technical Preview 4](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview)[[56]](#footnote-56) or a non-Microsoft service that supports the [FIDO 2.0 Technical specifications](http://fidoalliance.org/specifications)[[57]](#footnote-57) of the [Fast IDentity Online (FIDO) Alliance](https://fidoalliance.org/)[[58]](#footnote-58) - in this manner, not requiring the users to type in their passwords.

For additional information on Microsoft Passport, see the blog post [Microsoft Passport and Azure AD: Eliminating passwords one device at a time!](http://blogs.technet.com/b/ad/archive/2015/07/22/microsoft-passport-and-azure-ad-eliminating-passwords-one-device-at-a-time.aspx)[[59]](#footnote-59), the Microsoft MSDN article [Microsoft Passport overview](https://msdn.microsoft.com/en-us/library/dn985839(v=vs.85).aspx)[[60]](#footnote-60) the webcasts [The End Game for Passwords and Credential Theft?](http://channel9.msdn.com/Events/Ignite/2015/BRK2333)[[61]](#footnote-61), and [Secure Authentication with Windows Hello](http://channel9.msdn.com/Events/Ignite/2015/BRK2324)[[62]](#footnote-62).

1. Click **PIN requirements** to see what is required and then set your PIN according to the organization requirements. Under the covers this provisions Microsoft Passport.
2. Enter your chosen PIN that conforms to the requirements twice, and then click **OK**. Once the PIN is created, you are good to go.

Note For additional information, see the blog post [Azure Active Directory and Windows 10: Bringing the cloud to enterprise desktops!](http://blogs.technet.com/b/ad/archive/2015/05/13/azure-active-directory-and-windows-10-making-the-enterprise-cloud-a-reality.aspx)[[63]](#footnote-63).

### Joining a device in the out-of-box experience with a federated user (Optional)

The main difference with the previous section lays in the fact that a sign-in to the Azure AD tenant will automatically authenticate federated users with their on-premises corporate identity infrastructure. For this to work with our on-premises test lab environment, the computer will need the following:

* Name/IP resolution for the AD FS server(s). Azure AD will send the authentication request from the device to your Internet-facing WAP server, i.e. the EDGE1 computer in our configuration. WAP will then redirect these requests to your internal AD FS servers, i.e. the ADFS1 computer in our configuration.

1. Register the ADFS URL in your extranet DNS so that it resolves correctly.
2. You will also need to allow traffic on port 443 through the firewall to the WAP.

* Trust of the AD FS SSL/TLS certificate. Using a SSL/TLS certificate that chains to a recognized root CA certificate eases the configuration.

Important note Administrator have the ability to require a multi-factor authentication (MFA) of the end-users during a device registration process such the “Azure AD Join” or the “Add a work account to Windows” (Workplace Join).

These settings are configured using the Azure AD extension in the Azure management portal if you recall the REQUIRE MULTI-FACTOR AUTH TO JOIN DEVICE setting earlier in this document. There are separate policies for allowing users to perform “Azure AD Join” or “Add a work account to Windows”) but the MFA policy is global for all device registration processes.

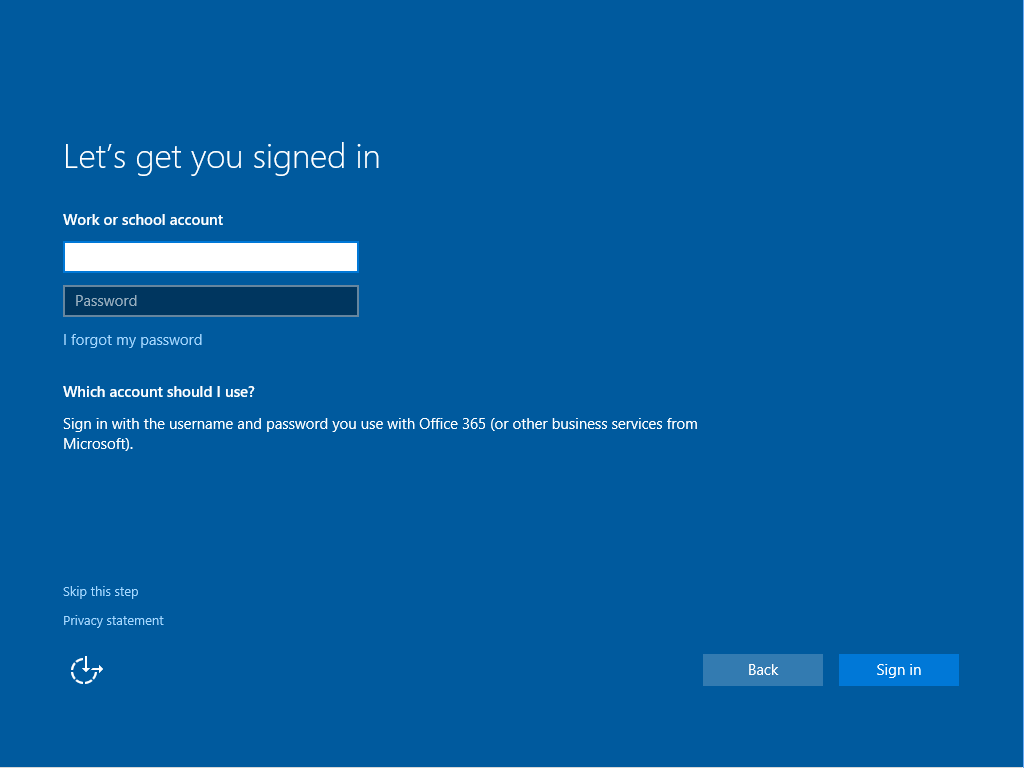
Using MFA during the OOBE join experience WILL FAIL with a federated account if a Federation Property flag called SupportsMFA is set to true.

(When this flag is set to true, a second factor authentication – in addition to the password - is expected to be performed by the organization’s identity infrastructure on-premises. Conversely, if the flag is set to false then the second factor authentication is rather expected to be performed by Azure MFA service. Likewise, if the flag is not set, it is assumed to be false. This flag is set with the [Set-MsolDomainFederationSettings](https://msdn.microsoft.com/en-us/library/azure/dn194088.aspx)[[64]](#footnote-64) cmdlet.)

In such situation (SupportsMFA == true), the Azure AD Join will NOT complete. This is because the on-premises multi-factor authentication server is attempted to be used rather than the Azure MFA service.

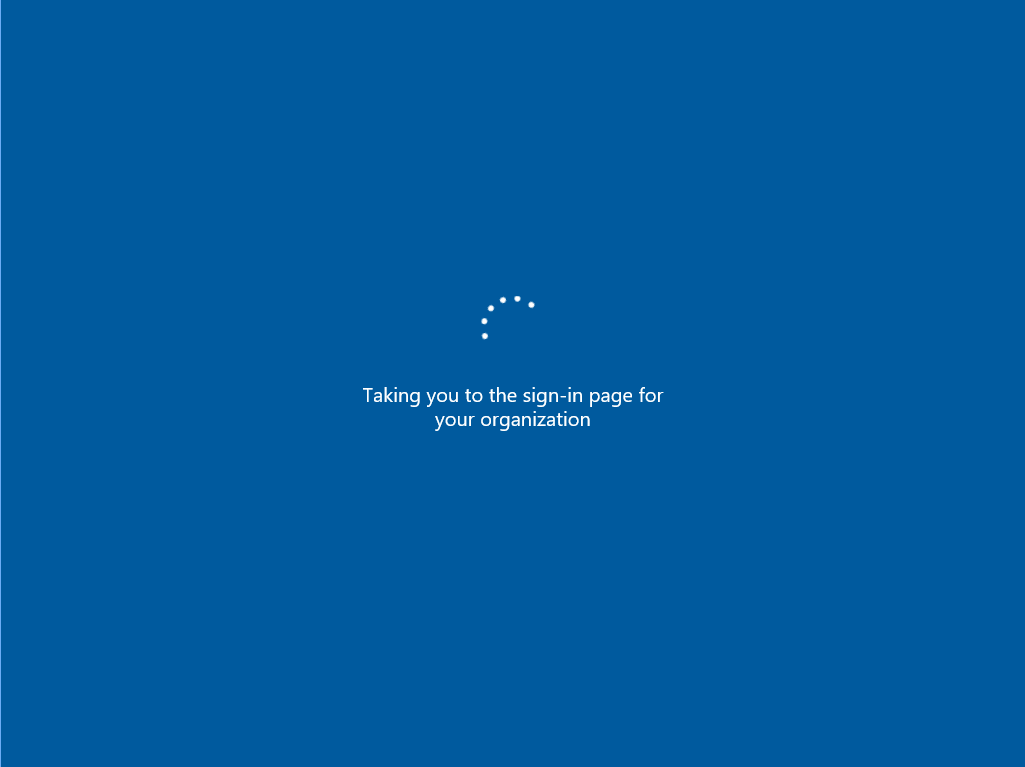
Let’s walk through the out of box experience (OOBE). Proceed with the following steps:

1. Boot a new image of Windows 10 that fulfills the pre-requisites described above.
2. Repeat the steps 2 to 4 of the section Joining a device in the out-of-box experience with a cloud user.
3. Like before, the screen gets to **Set up Windows for this work or school PC**.

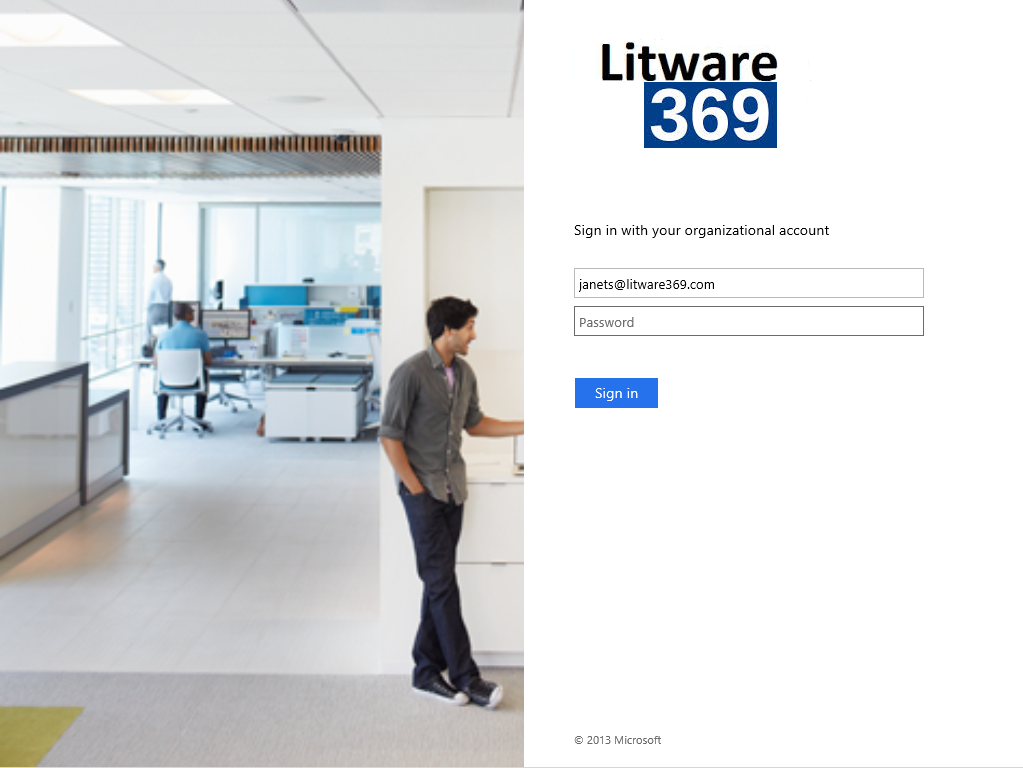


1. Type the username of a federated Azure AD account, for example in our illustration *janets@litware369.com* and press ENTER.

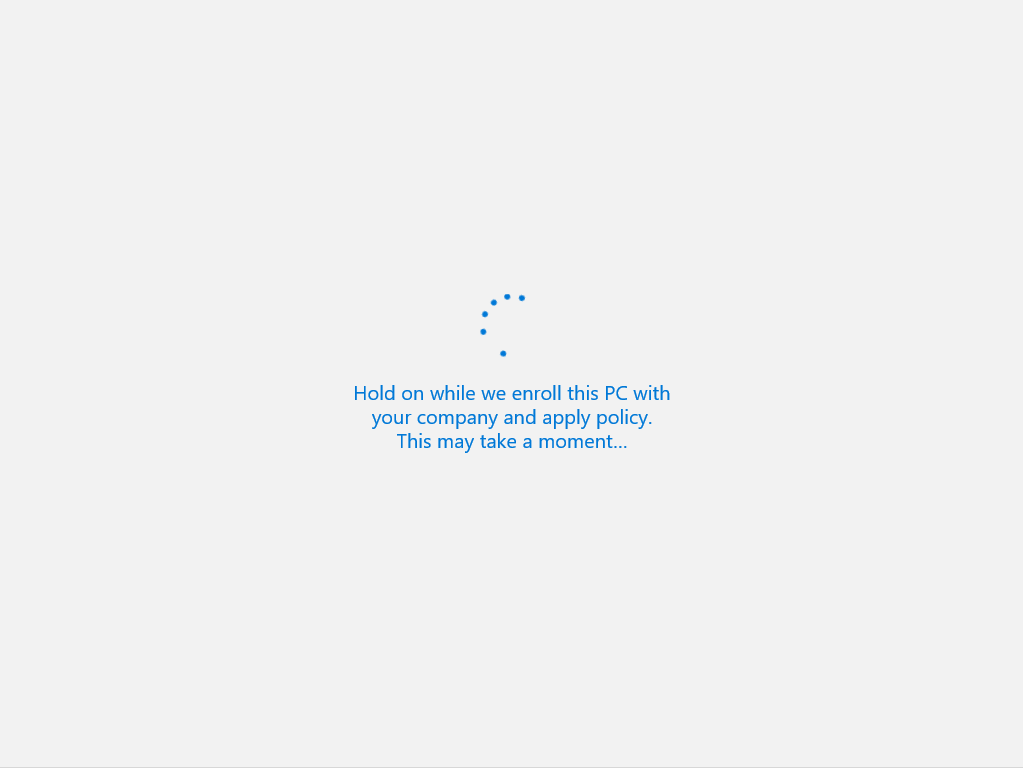
You are then automatically redirected to your on-premises identity infrastructure.



In our optional configuration for the test lab environment, the AD FS sign-in page is then displayed after a successful redirection.



1. Enter the password of your Azure AD account credential, for example, in our illustration *“pass@word1*”.
2. Click **Sign in**. You are then prompted to update your password if this is the first time you have logged on with this account. Please do so and click **Sign in** once more. A screen appears informing you of the device enrollment process and the login continues.



1. Wait for it to complete.



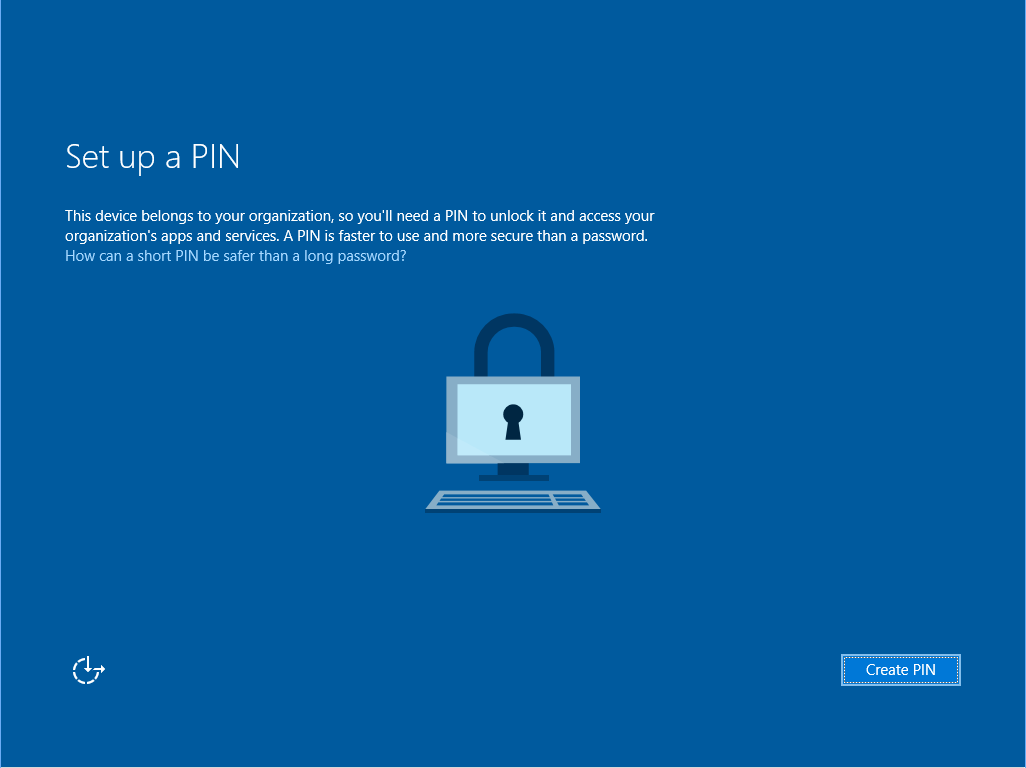
1. Logon with your work account, for example, in our illustration and press ENTER:

Username: *janets@litware369.onmicrosoft.com*

Password: *pass@word1*



1. A successful logon will proceed to setting up a work PIN, your Microsoft Passport gesture.



1. Once the PIN is created, you are good to go.

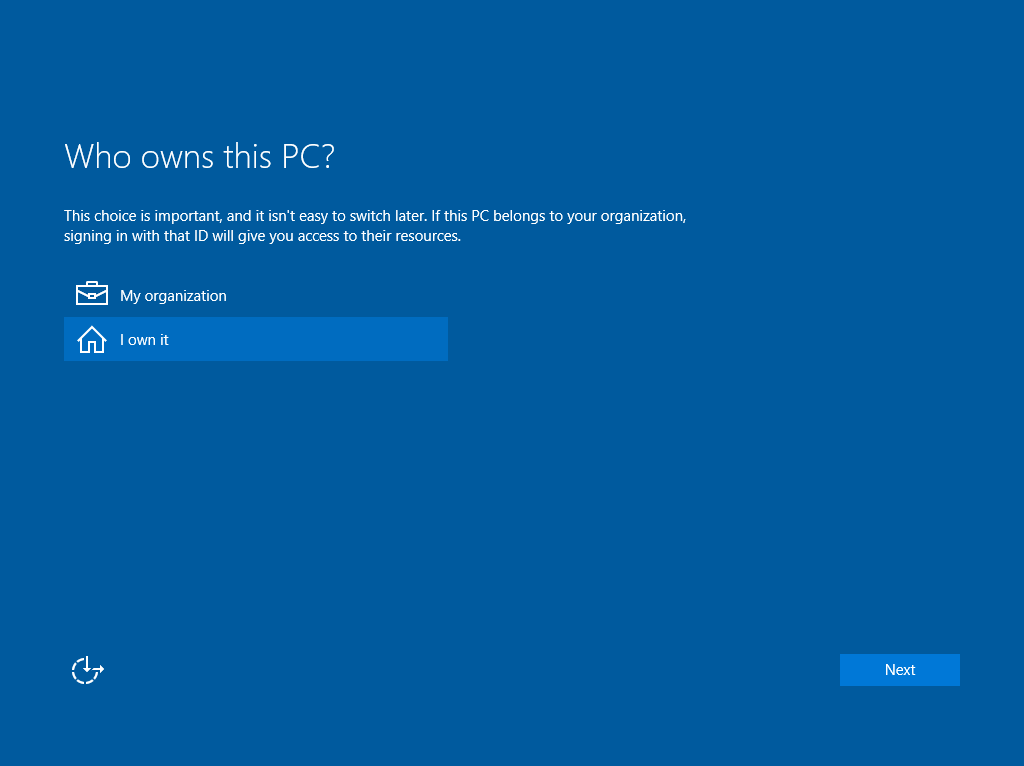
### Joining a device from system Settings

If the user doesn’t have network connectivity during OOBE, and wants to join the corporate owned device to Azure AD once a network is available, the user can leverage the system Settings.

Note There will be also times when the above OOBE domain join experience may fail for some reasons and in lieu of a local account may be created. Should the process fail, on should note that there is a hidden command that can be used to allow access to the event logs. During OOBE, pressing Shift F10 will launch a command window that allows simple shell commands to be executed. This will require the machine to be rebooted, because the command is only available on the first screen. Once the command window is open, normal connectivity tests can be performed as well as launching the Event Viewer. Test the network connectivity and troubleshoot as normal, using the errors in the event logs as a starting point.

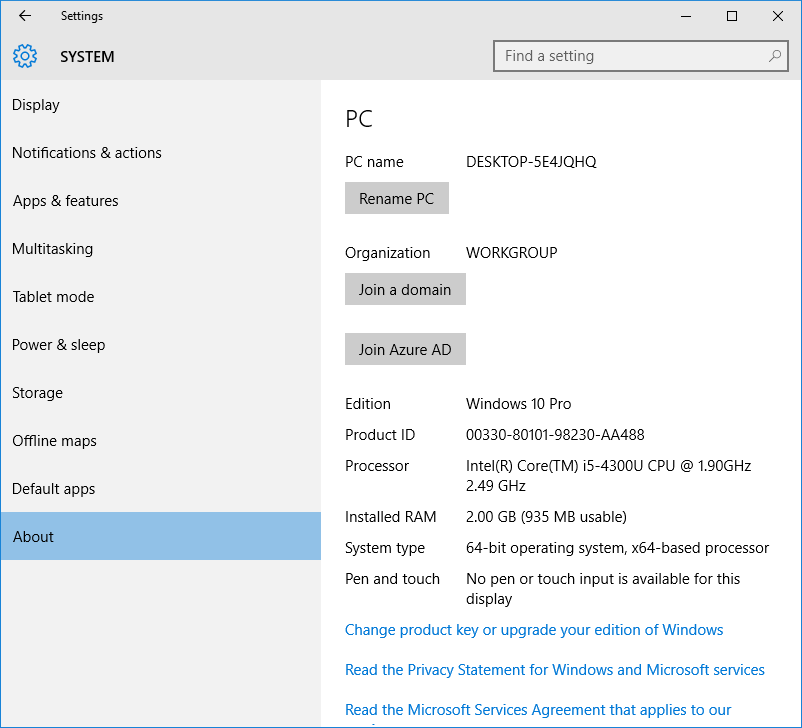
To joining a device to Azure AD from the system Settings proceed with the following steps:

1. During the OOBE, in the **Who owns this PC?** page, select **I own it** to create a local account.



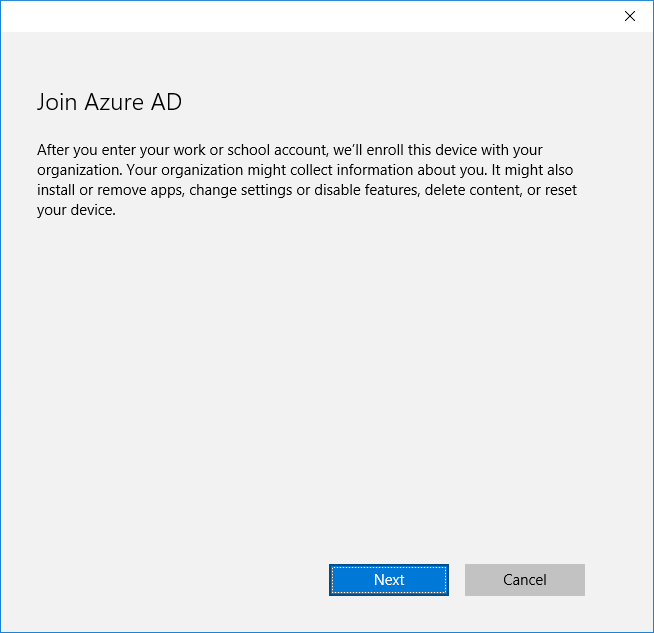
A standard dialog to create a local account begins. Like earlier versions of Windows, administrator is a reserved account so choose your first name and a password that you will remember.

1. Once you arrive at the desktop with a local account, you may then choose to join Azure AD. Press the Windows key + I. The **Settings** dialog opens up.
2. Select **Settings** > **System** > **About**.

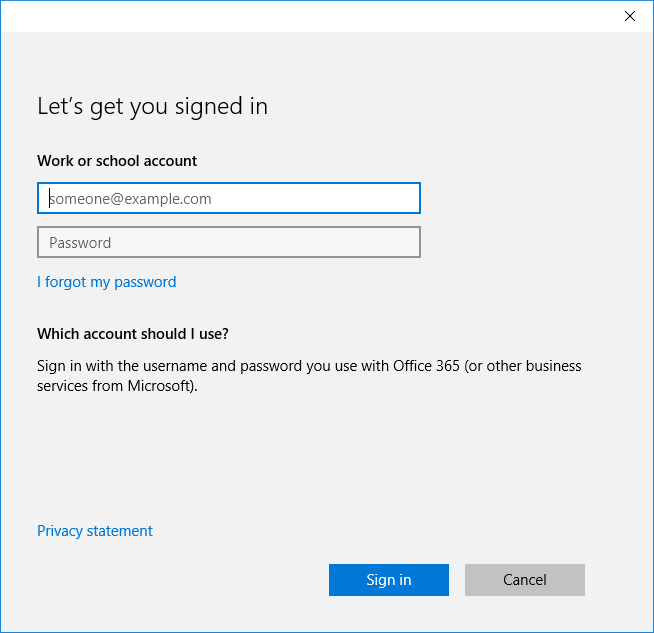


1. Click **Join Azure AD**. An eponym dialog opens up.

Important note You cannot be a member of two domains. If your device is already a member of a traditional WSAD domain, following the Join Azure AD dialog will result in an error and be logged in the netsetup.log file.



1. Click **Next**. Allow it to spin and move to the next eponym page. This may sound familiar now.

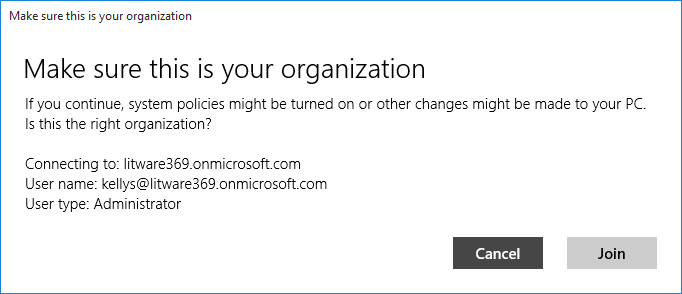


1. Enter your Azure AD account credential, for example, in our illustration:

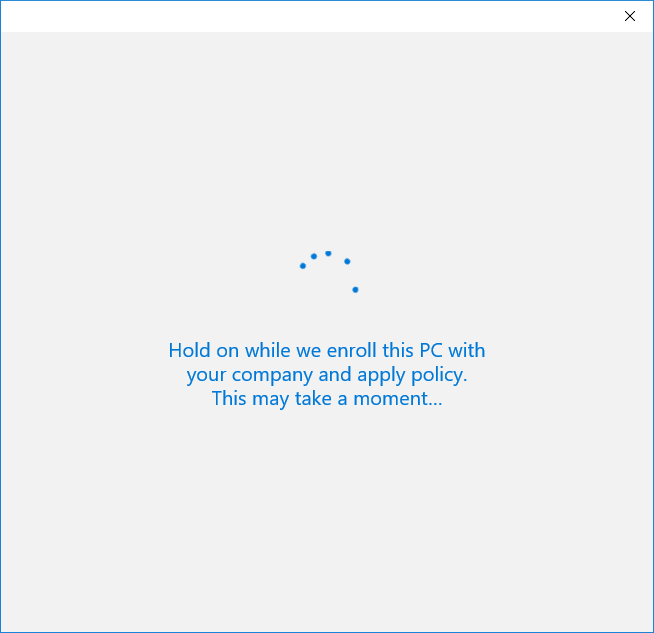
Username: *kellys@litware369.onmicrosoft.com*

Password: *pass@word1*

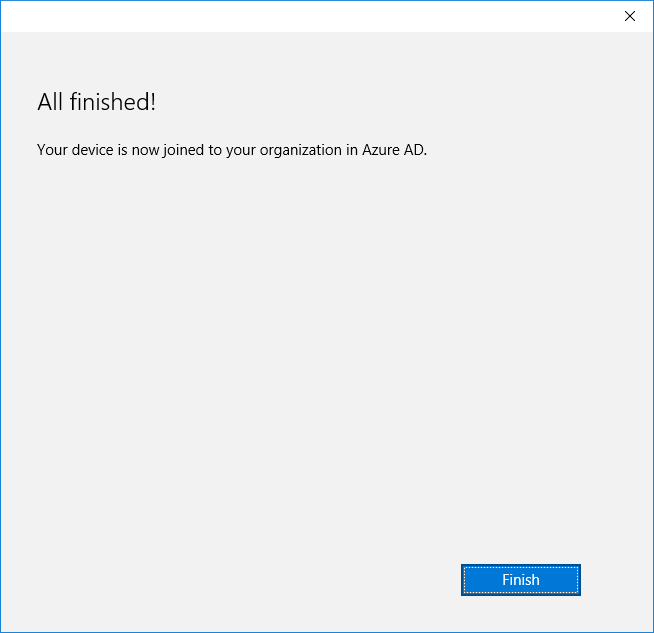
1. Click **Sign in**. Your device is now about to be enrolled. A **Make sure this is your organization** dialog pops up.



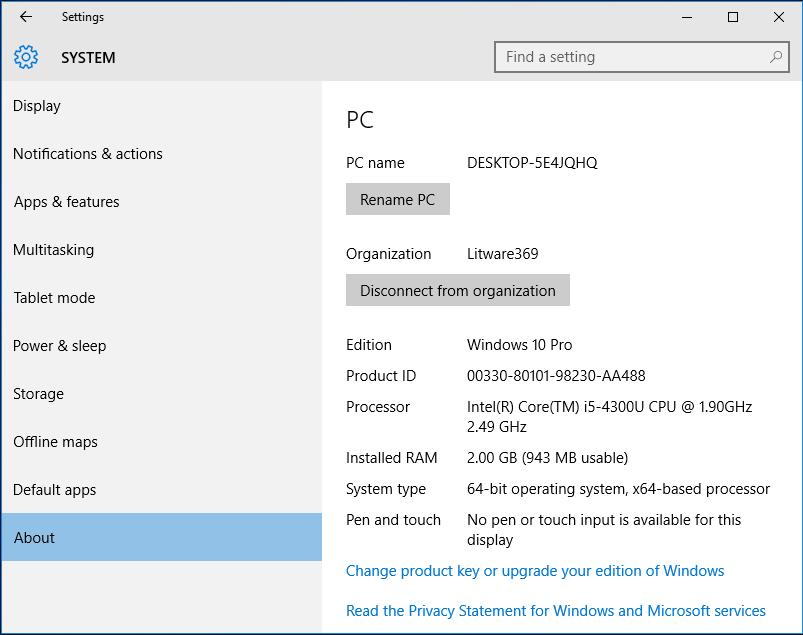
1. Click **Join** to confirm.



1. Once enrolled, the device has joined the organization.



1. Click **Finish**.

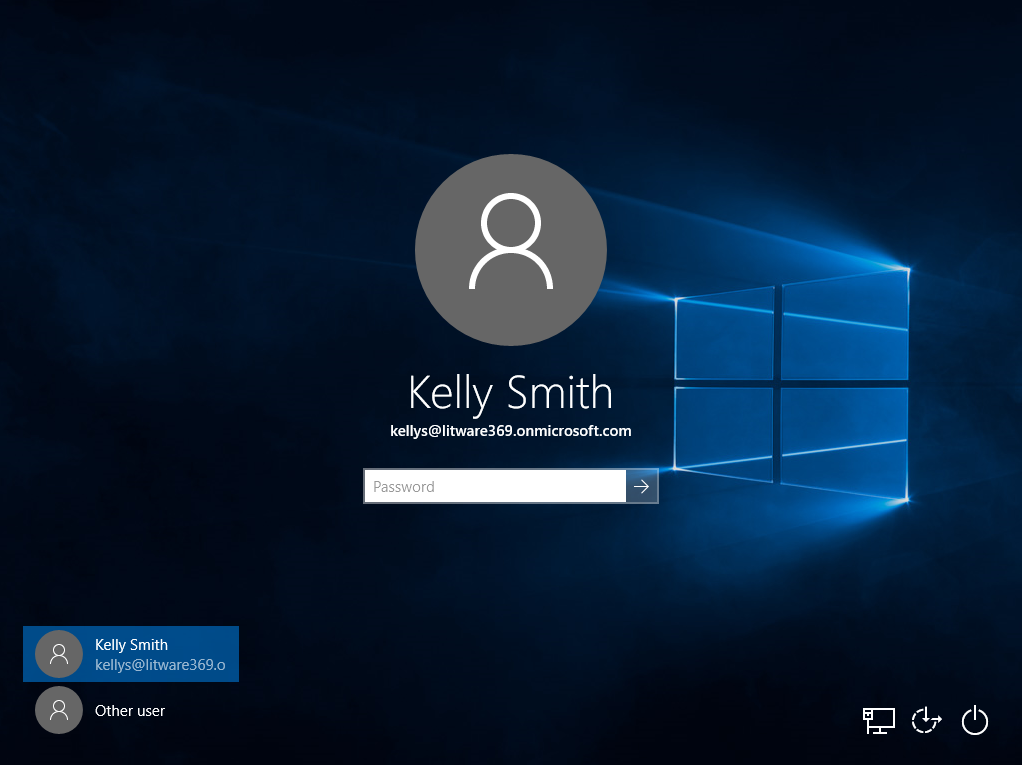


### Signing in with the Azure AD account

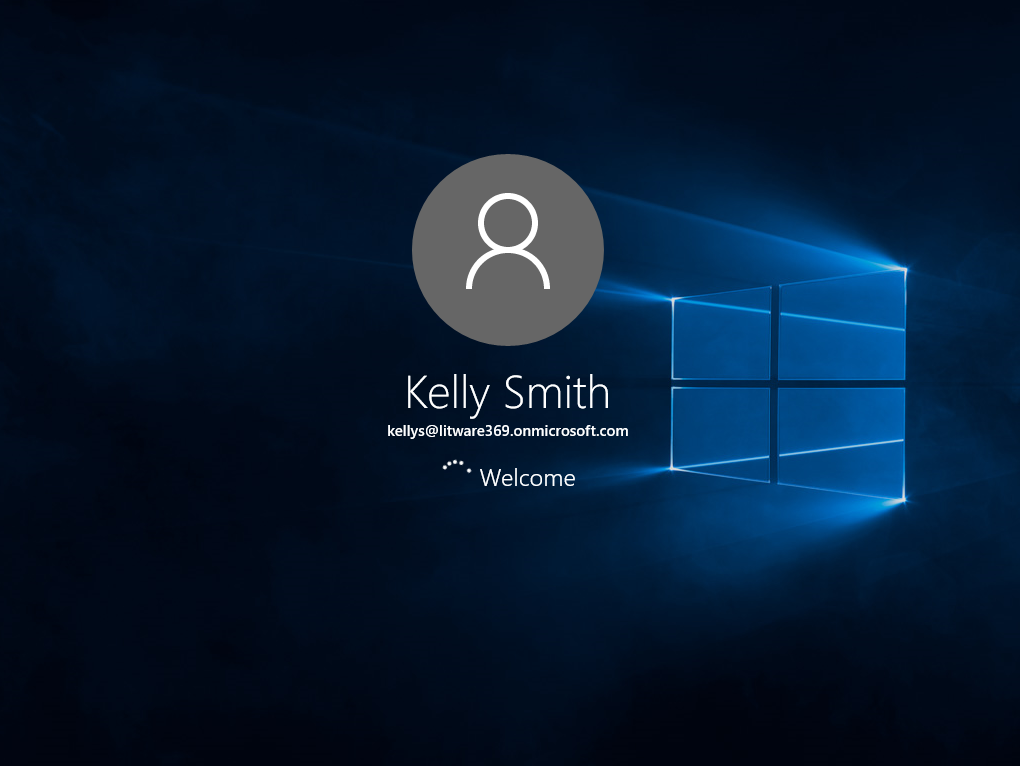
Regardless of the above methods used to join the corporate owned device to Azure AD, the user can actually use their Azure AD work or school account during their normal logon. Windows 10 uses then Azure AD to authenticate the user for login.

Note If network connectivity is not available at that time, Windows 10 will use cached credentials, assuming that there is no policy applied that prevents it. The access will be available as long as the token has not expired.

To sign-in with your Azure AD work or school account, proceed with the following steps:



1. Enter the password of your (managed or federated) Azure AD account credential, for example, in our illustration“*pass@word1*”, and then press ENTER:



The user will enjoy the following benefits:

1. True SSO (i.e. a seamless access without any prompt) to cloud-based, and on-premises modern and traditional resources from anywhere.

Note SSO to resources protected by Azure AD like Office 365 or even on-premises resources via Azure AD Application Proxy does not requires any specific deployment in the on-premises. In absence of Azure AD Application Proxy, the user will also enjoy SSO to modern applications on-premises that trust AD FS (not Kerberos-based). This will require AD FS in Windows Server 2016 in order to adequately leverage the Primary Refresh Token (PRT) issued by Azure AD after a successful logon. The PRT can be seen as the cloud “equivalent” of the well-known Kerberos Ticket Granting Ticket (TGT) in the on-premises. For more information on the next version of AD FS, see the webcast [What’s New in Active Directory Domain and Federation Services in Windows Server vNext](http://channel9.msdn.com/Events/Ignite/2015/BRK3871)[[65]](#footnote-65). As previously noticed Windows Server 2016 is a prerelease software. You can start investigating in parallel [Windows Server 2016 Technical Preview 4](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview)[[66]](#footnote-66)

Note The device can participate in conditional access as “domain joined” and “registered/managed” devices.

1. Roaming of settings across devices where users sign-in with their corporate credentials.
2. Access to the organization’s private catalog on the enterprise-ready Windows store.

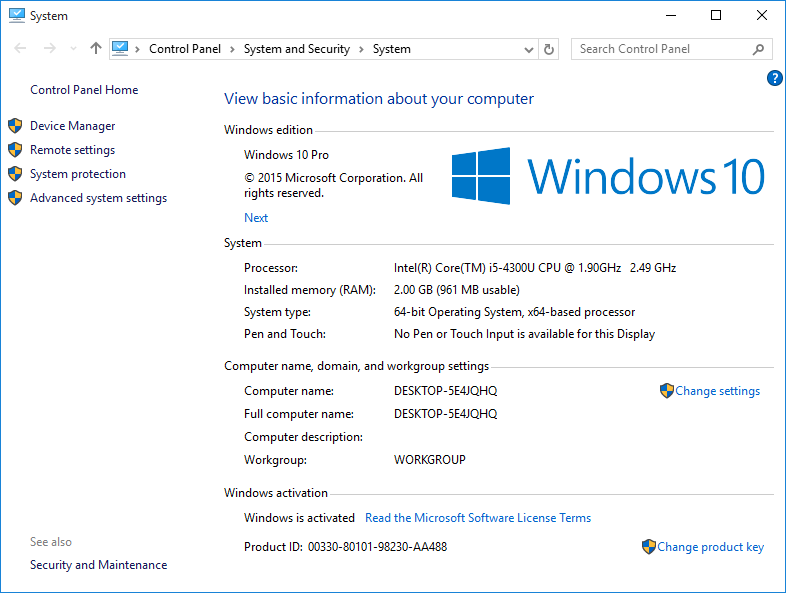
Note For more information, see the webcast [Using the Business Store Portal with Windows 10 Devices](http://channel9.msdn.com/Events/Ignite/2015/BRK3338)[[67]](#footnote-67).

1. Microsoft Passport to greatly reduce the risk of credential theft.

### Verifying the "Azure AD Join" process on the device

Let’s see how to verify a successful "Azure AD Join" process from the above Windows session.

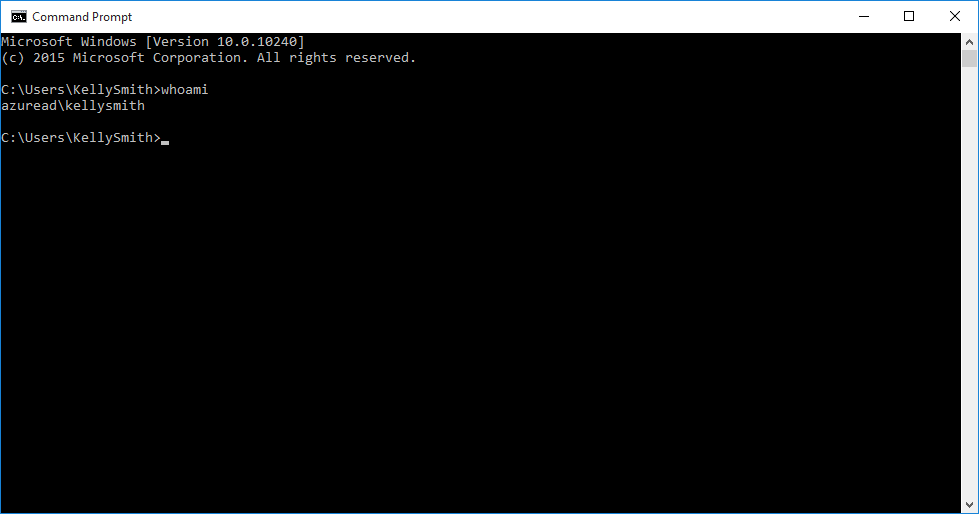
One should note the traditional System properties does not demonstrate a successful Azure AD Join. When viewing the **System** dialog (*sysdm.cpl*) the information for domain status is not reflected correctly and can be misleading. System Properties will indeed show that the device is in a workgroup as illustrated hereafter under **Computer name domain and workgroup settings**.



#### Verifying using the whoami command

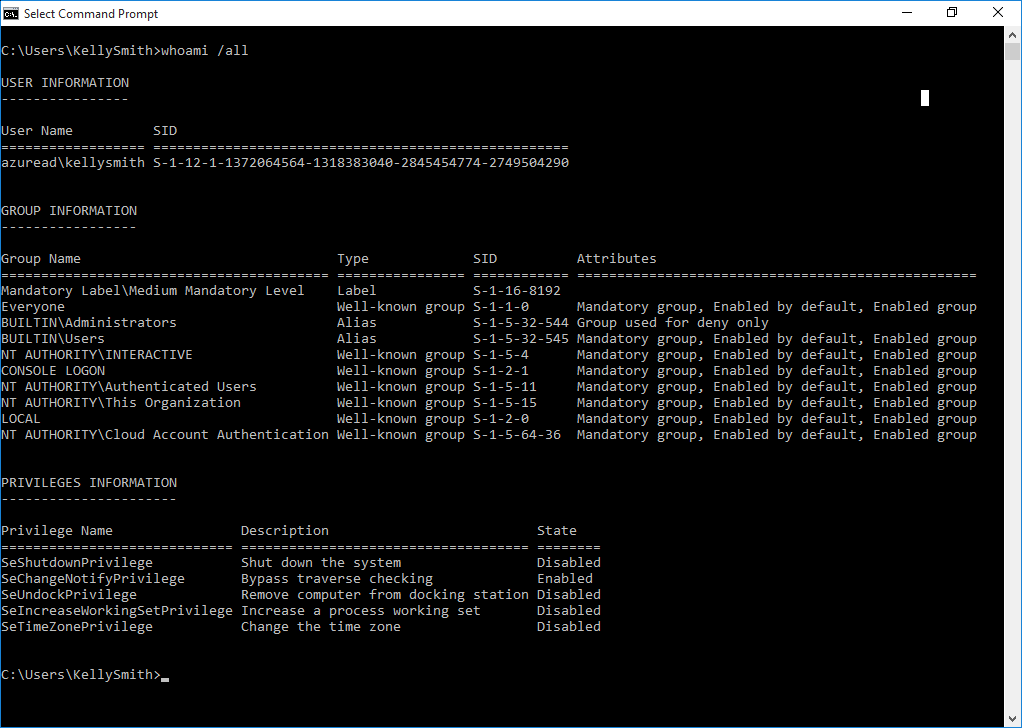
Using a simple **whoami** from a command window displays the user's domain and the user executing the command. Proceed with the following steps:

1. Right-click the **START** button in the lower left window and then select **Run**.
2. Type “*cmd*”.
3. When the command prompt opens up, type “*whoami*”and press ENTER. The command should complete and display *azuread\kellysmith* (cloud identity) or *azuread\janetschorr* (federated identity) if you followed earlier steps or the user name you’ve chosen when configuring your Azure AD test user(s). It should look like the snapshot hereafter.



Note This display format is different from what you will see with a traditional WSAD domain join whoami command. Whoami on traditional WSAD domain will return a NetBIOS format such as *litware369\janets* but on an Azure AD joined machine the command returns a combination of givenName + SN without a space.

1. For additional information and notably the group membership, type “*whoami /all*”and press ENTER.

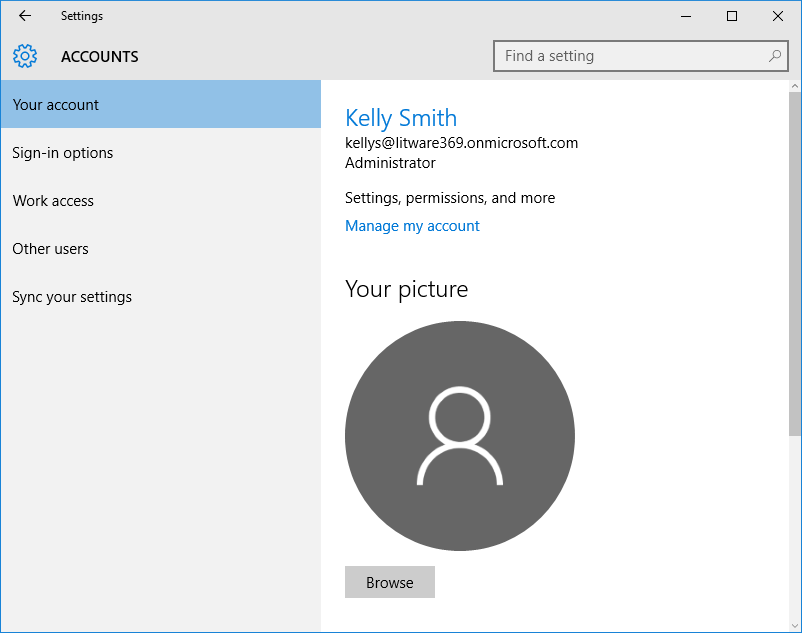


#### Verifying via the Settings page

The **Accounts** page under the **Settings** option in Windows 10 also shows you what type of account is being used.

To open the **Accounts** page and verify the process, proceed with the following steps:

1. Press the Windows key + I. The **Settings** dialog opens up.
2. Select **Settings** > **Accounts** > **Your account**.



The AAD Token Broker plugin is underneath used for this account. This plugin is designed for a seamless Single Sign-On (SSO) experience.

Note Token Broker in Windows 10 is a new authentication framework that improves upon the former Web Application Broker in Windows 8.x and which is designed to provide Single Sign-On (SSO) for browser, [modern business applications](http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx)[[68]](#footnote-68), and services.

If you think of the aforementioned Microsoft Passport as a locked box of secrets then the Token Broker is the master of keys, matching credentials with identity providers. The Token Broker enables identity providers like Azure AD in this illustration but also Microsoft Account (MSA), Facebook, etc. to natively plug into Windows in order to provide apps and services with tokens to access web resources.

As a result, users like Kelly enjoy a seamless authentication experience when connecting to online services for Azure AD here, and other identities and don’t have enter their credentials multiple times. For example, this enable in our illustration seamless access to protected Azure AD resources wherever they reside and where Kelly can enjoy modern applications that integrate with their favorite web services in a secure and frictionless way.

This also provides in terms of additional benefits Web authorization experience consistency and higher-level integration into account management, selection, switching, etc.

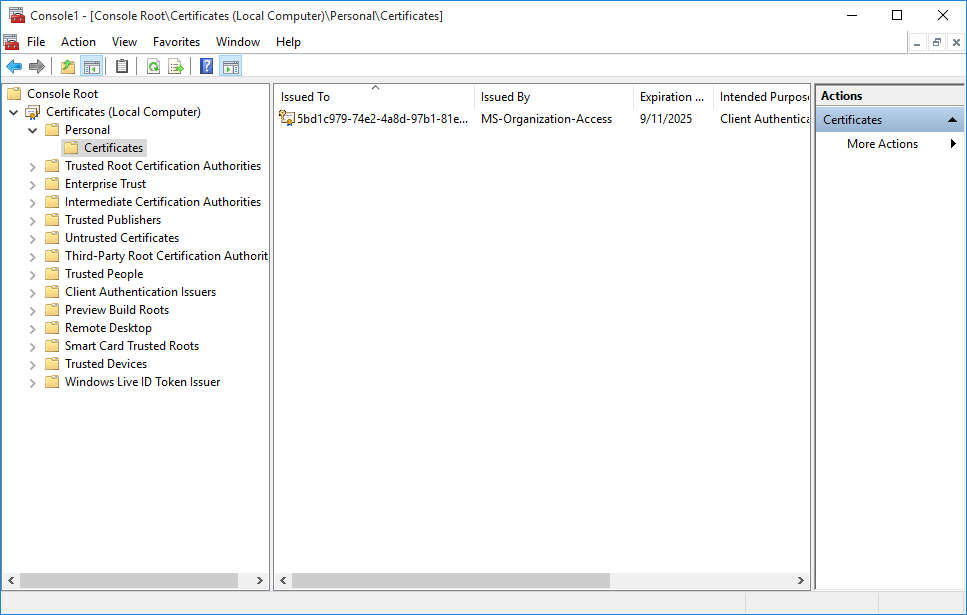
#### Verifying the machine certificate

Once a device is joined to Azure AD, a certificate is issued to that device by the Azure AD Device Registration Service as part of the process.

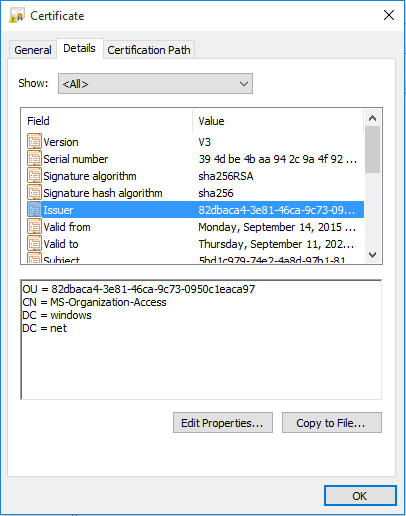
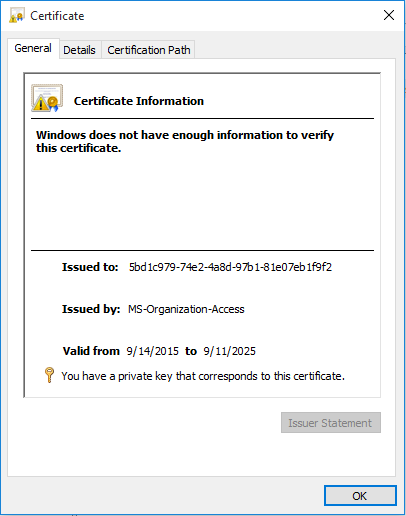
Note For additional information, please refer to the specification [[MS-DVRE]: Device Registration Enrollment Protocol](https://msdn.microsoft.com/en-us/library/dn410252.aspx)[[69]](#footnote-69).

To view this certificate, proceed with the followings steps:

1. Click **Start** and type “*mmc*” in the search box. Accept the UAC prompt.
2. Once the mmc console opens up, select **File** then **Add/Remove Snap-in...**, select **Certificates**, and then **Add.**
3. Select **Computer Account**, **Next**, **Local Computer**, and **Finish.**
4. Click **OK** and drill down into the **Computer Personal Certificate** store to see a certificate issued to your device ID.



1. Double click the certificate to see its properties.

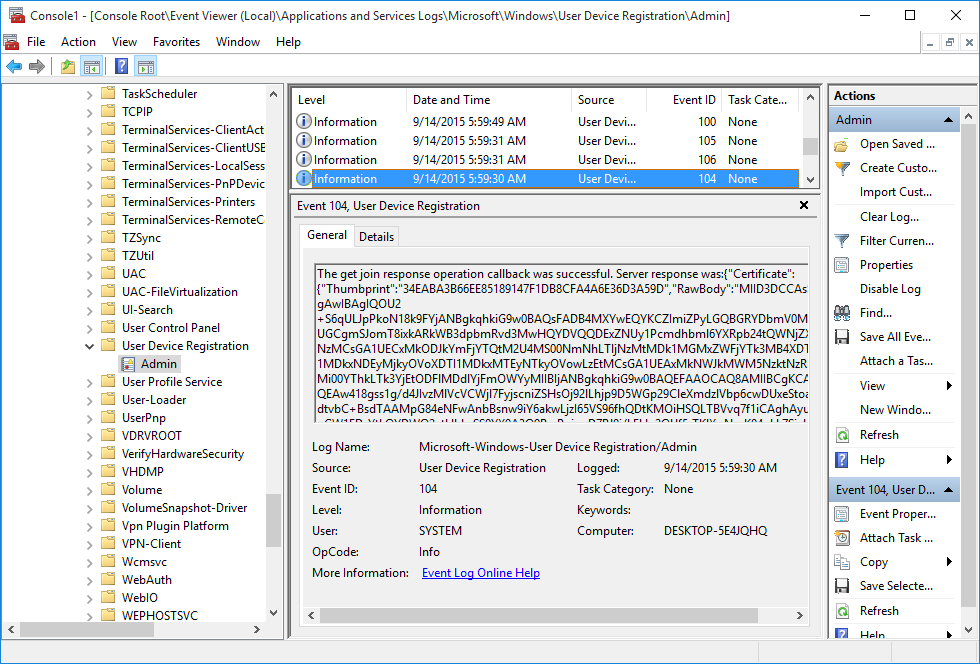


#### Verifying via event logs

The “Azure AD Join” process does not write to the netsetup.log like a traditional WSAD domain join of a Windows machine to the on-premises Active Directory. In fact, the netsetup.log will be blank so determining a successful join will require other clues to aid the IT professional.

However, Windows 10 allows you to confirm via the **User Device Registration Admin** log. Proceed with the following steps:

1. Open your event viewer. Right-click the **START** button in the lower left window and then select **Run**.
2. Type “*eventvwr*”.
3. Drill down under **Microsoft and Windows** until you get to the **User Device Registration** log.
4. Confirm there are no errors. Your event logs should be similar to the one below.



Examine your own event logs and compare them with what you see in this above illustration.

### Verifying the "Azure AD Join" process in your Azure AD tenant

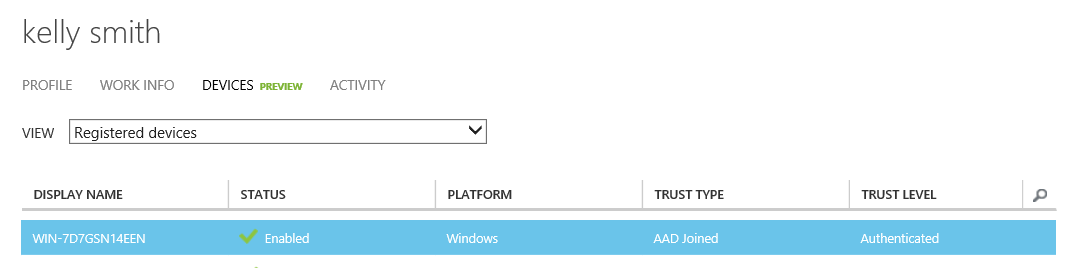
Let’s wear the IT professional clothes to verify a successful "Azure AD Join" process in the Azure AD tenant as well as in the Mobile Device Management for Office 365 if you’ve activated this solution.

#### Verifying from the Azure management portal

If you know your hostname you can verify a successful Azure AD Join by reviewing the **Devices** tab on the user account who joined the Windows 10 device to Azure AD.

Proceed with the following steps:

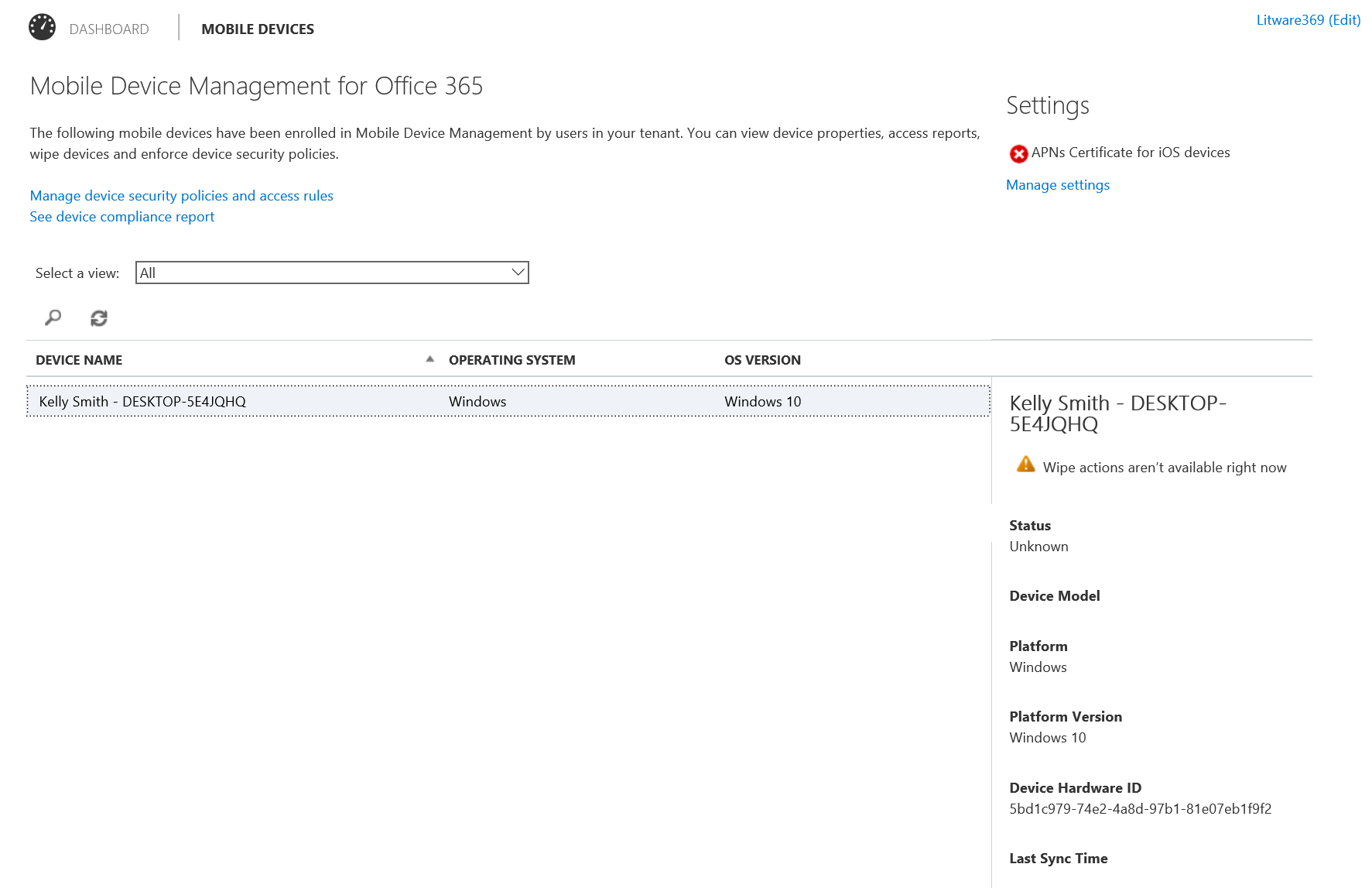
1. First determine your hostname on the Windows 10 client. This is done via **Computer properties** or from the command line. See the above images for an example.
2. Navigate to the Azure management portal at <https://manage.windowsazure.com> and sign-in.
3. Locate your Directory. Double click on the Directory and select the Users tab at the top by clicking on it.
4. Double click on the user that joined the computer to the domain and select **DEVICES**. The display name of the workstation will be shown along with the trust type of **AAD Joined**.



#### Verifying from the Office 365 management portal (Optional)

Proceed with the following steps:

1. Open a browsing session from your local machine navigate to the Office 365 management portal at <https://portal.microsoftonline.com>, and then sign in with your administrative credentials.
2. If the Office 365 admin center is not visible, open the apps launcher in the top left corner and select **Admin**.
3. In the left pane of the admin center, click **MOBILE DEVICES**. You should see Kelly’s enrolled device listed under **DEVICE NAME**.

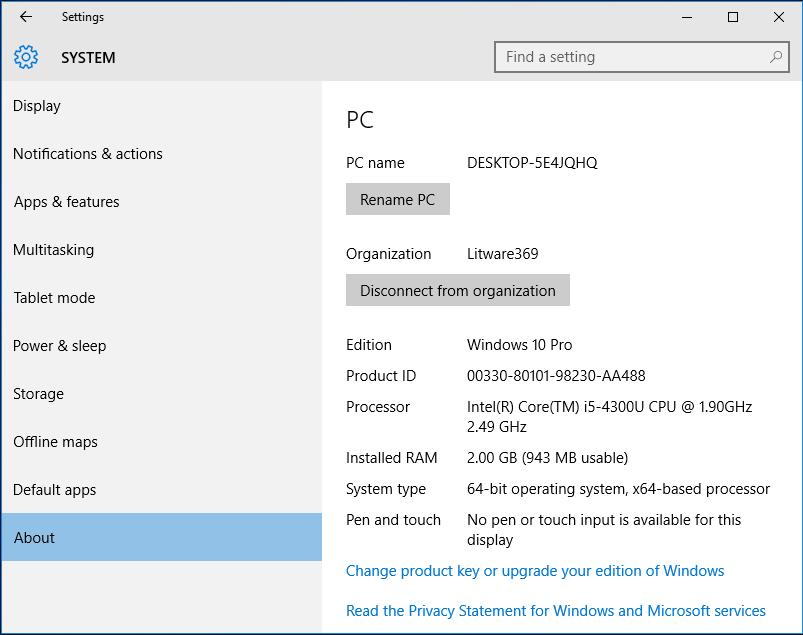


### Leaving the organization

There may come a time when you wish to leave the organization.

To leave the organization, proceed with the following steps:

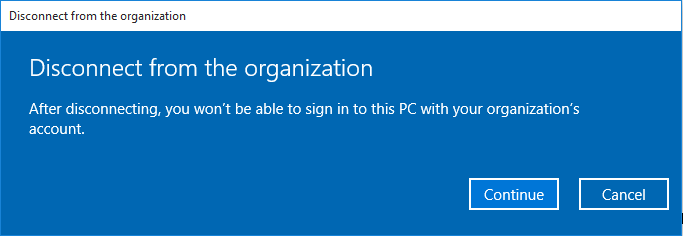
1. Press the Windows key + I. The **Settings** opens dialog up.
2. Select **Settings** > **System** > **About**.



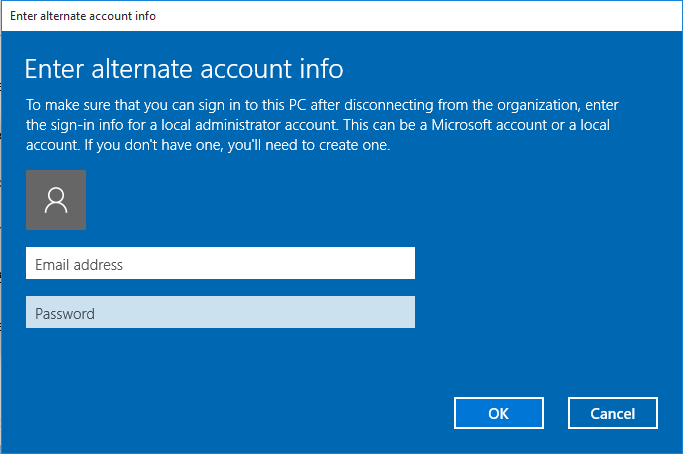
1. Click **Disconnect from organization** ONLY after you have created a local administrative account for you to use after leaving the organization.

Important note Failing to create a local or Microsoft Account (MSA) account with administrative rights on the computer before leaving the organization will cause the user to lose all access to the machine and leave it in an unusable state.

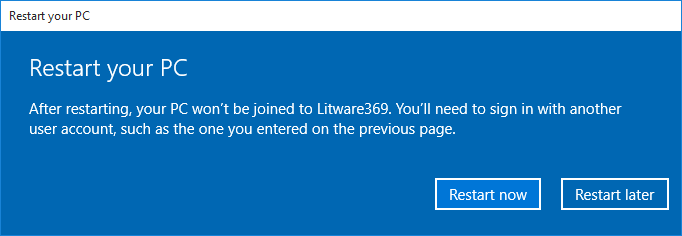
A **Disconnect from the organization** dialog shows up.



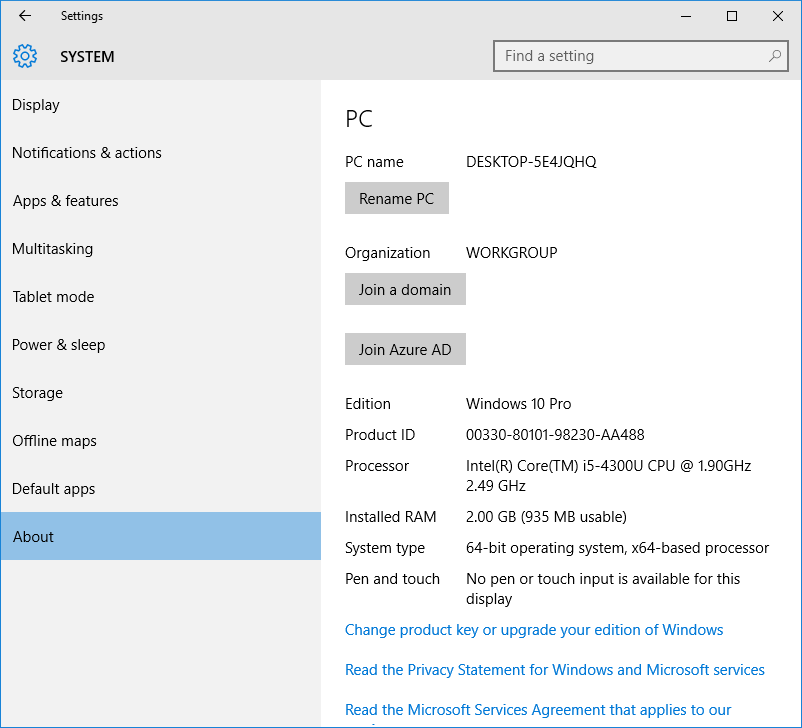
1. Click **Continue**.



1. Enter your local or MSA account credentials and click **OK**. A **Restart PC** dialog shows up.



1. Click **Restart now**. After rebooting, open a session with your local or MSA account credentials.
2. Press the Windows key + I. The **Settings** opens dialog up. Select **Settings** > **System** > **About**.



## Joining a device to a domain in a hybrid AD environment (Optional)

This section is intended to provide instructions for configuring and testing the "Domain Join” in a hybrid Active Directory environment as the title indicates. It thus will require the optional “on-premises” test lab environment deployed in Azure as per section entitled Building an on-premises test lab environment (Optional).

Windows 10 domain joined computers (build 10551 and above) will automatically and silently connect to the cloud. They will do so by contacting and authenticating directly with Azure AD Device Registration Service.

The article [Connect domain-joined devices to Azure AD for Windows 10 experiences](https://azure.microsoft.com/en-us/documentation/articles/active-directory-azureadjoin-devices-group-policy/)[[70]](#footnote-70) fully described how to update the above optional “on-premises” test lab environment deployed in Azure.

This requires to:

1. Deploy a custom installation of AAD Connect in order to enable Windows 10 domain joined computers on-premises to be provisioned as device objects in the cloud.

Note For more information, see the article [Custom installation of Azure AD Connect](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-get-started-custom/)[[71]](#footnote-71).

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/)[[72]](#footnote-72).

1. Create a service connection point (SCP) in on-premises AD in order to allow Windows 10 domain joined computers to discover Azure AD tenant information at the time of auto-registration with Azure AD Device Registration Service.
2. Configure AD FS claim rules in order to enables instantaneous registration of Windows 10 domain joined computers with Azure AD Device Registration Service by allowing computers to authenticate using Kerberos/NTLM via AD FS. Without this step, computers will get to Azure AD in a delayed manner (subject to Azure AD Connect sync’ times).

Note Windows 10 domain joined computers will authenticate using Windows Integrated authentication to an active WS-Trust endpoint hosted by AD FS. You must ensure this endpoint is enabled. Since the optional “on-premises” test lab environment deployed in Azure is using the Web Authentication Proxy, you must also ensure this endpoint is published through the proxy. You can do this by checking that the adfs/services/trust/13/windowstransport shows as enabled in the AD FS management console under Service > Endpoints.

1. Configure automatic device registration via Group Policy in AD in order to configure Windows 10 domain joined devices to automatically register with Azure AD.

Note As noticed earlier in this document, WSAD in Windows Server 2016 is needed to enable Microsoft Passport and Windows Hello. As of this writing, Windows Server 2016 is a prerelease software. You can start investigating [Windows Server 2016 Technical Preview 4](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview)[[73]](#footnote-73). For more information, see the webcast [What’s New in Active Directory Domain and Federation Services in Windows Server vNext](http://channel9.msdn.com/Events/Ignite/2015/BRK3871)[[74]](#footnote-74).

Thanks to the above steps, and excepted the fact that the user will sign with their “regular” WSAD account, they will enjoy the same benefits as the ones outlined in section Signing in with the Azure AD account.

# Testing the new capabilities for personal devices

This walkthrough provides instructions for testing the new capabilities provided for **personal devices** by combining Azure AD and Windows 10 features.

**Please ensure that all the prerequisites mentioned earlier in section** Building a test lab environment **are fulfilled at this stage.**

## Configuring your Azure AD tenant

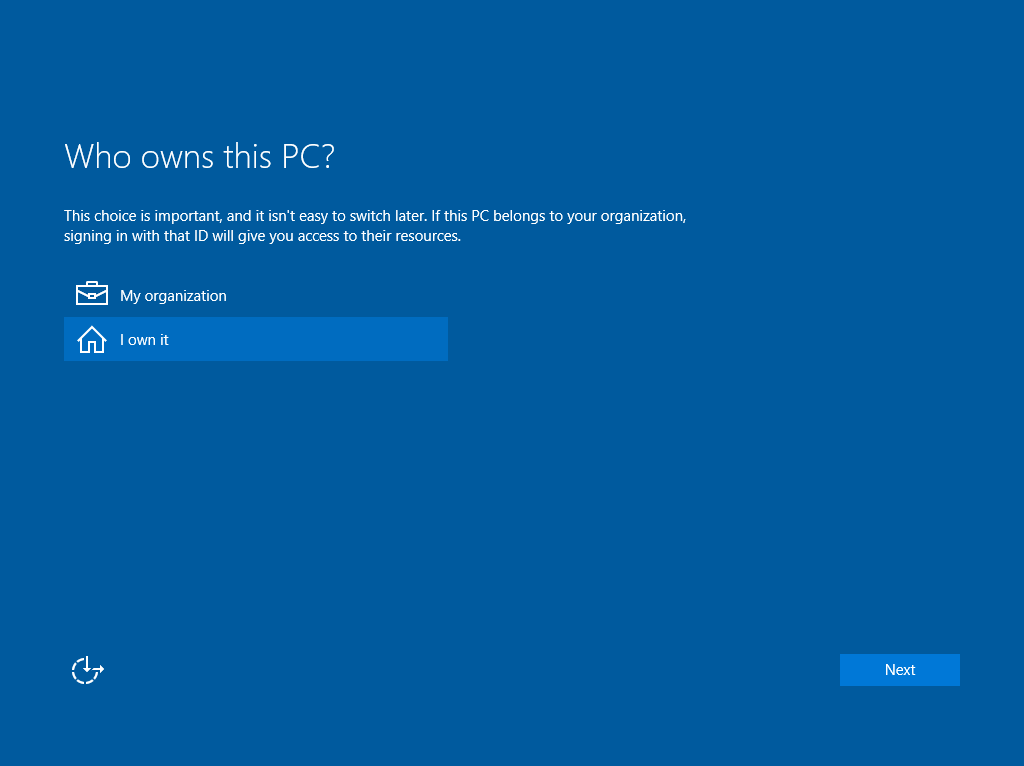
Adding an Azure AD account to a personal device has the same additional requirements as the one outlined in the eponym section of the section Testing the new capabilities for corporate owned devices.

Please refer to this section and its instructions to configure your test lab environment in accordance if you’ve not already done it.

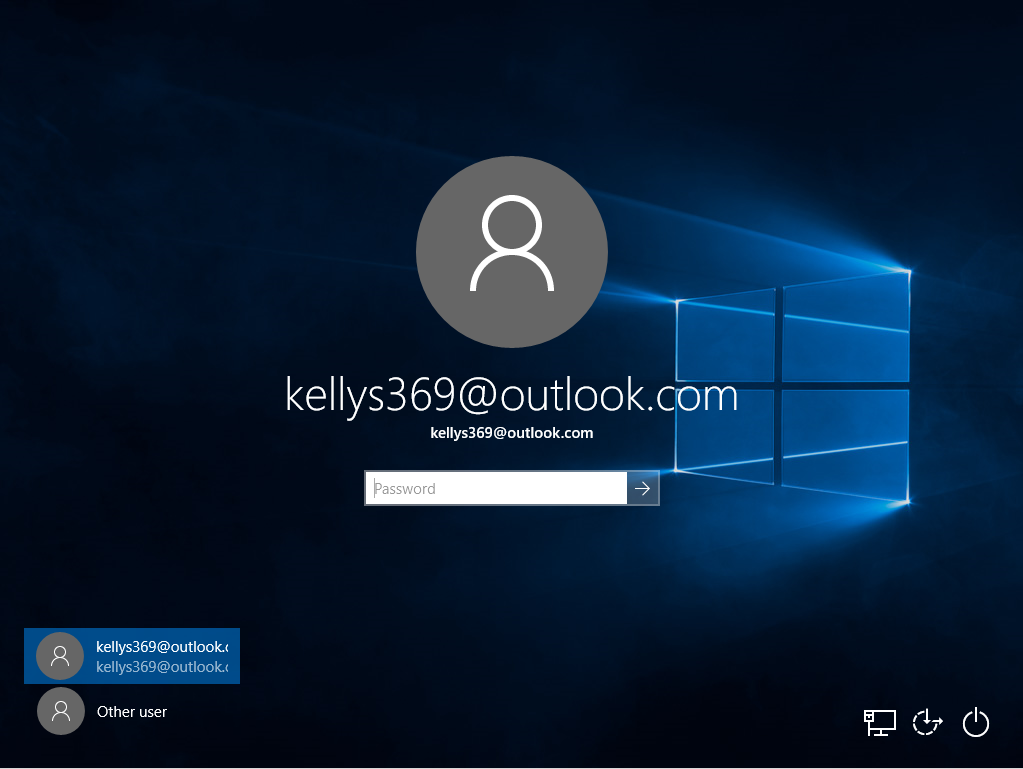
## Adding an Azure AD account to a device

Let’s walk through from the out of box experience (OOBE). Proceed with the following steps:

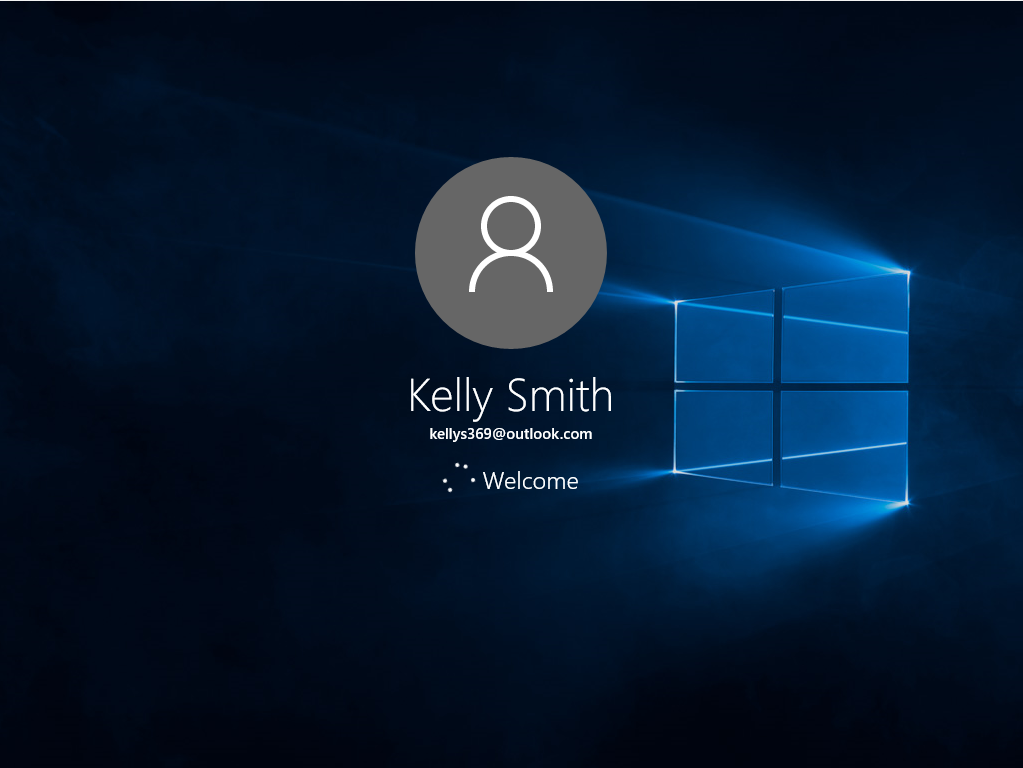
1. Boot a new image of Windows 10.
2. After booting, you’re presented with the regional settings screen. Configure your country or region, app language, keyboard layout, and time zone as necessary and click **Next**. The **License Agreement** screen shows up.
3. Click **Accept** and continue. **The** Setup screen shows up. This page enables you to customize certain settings such as search engines, app updates, and your browser. Click **Use express settings**. If the connection to the Internet works, you should be then presented with the screen **Who owns this PC?** like before.



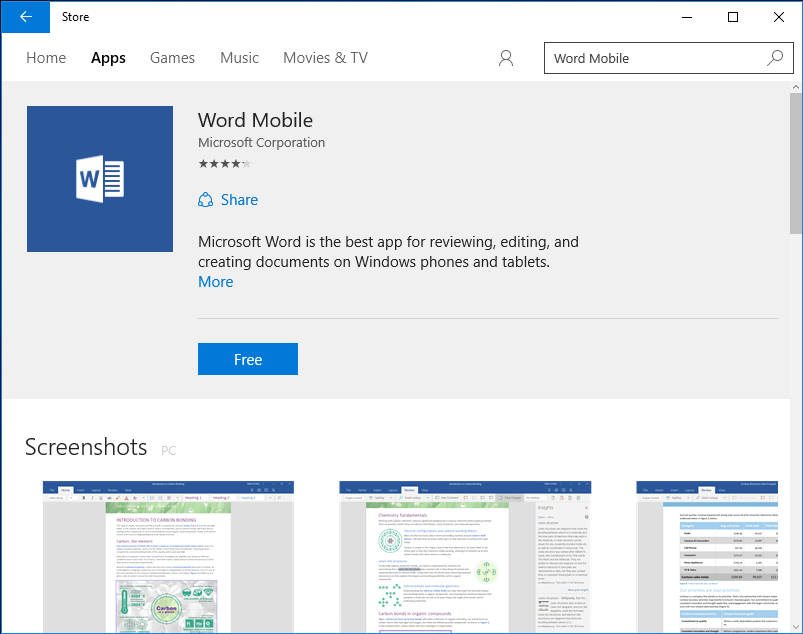
1. For this scenario, select **I own it** and click **Next**.
2. When prompted for a local account, create a local account or specify your MSA account, for example *kellys369@outlook.com* in our illustration. Complete the setup.



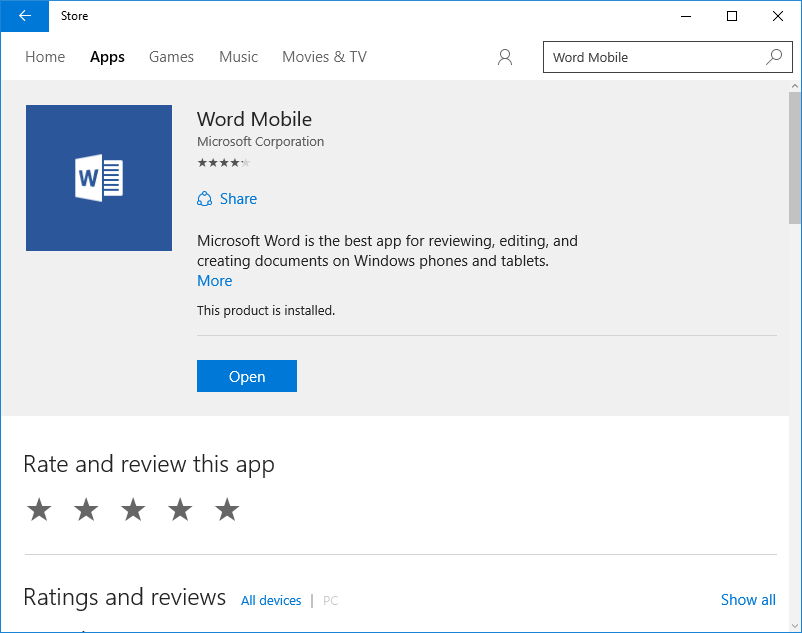
1. When invited, sign in with your local or MSA account credentials to open a Windows session, for example *kellys369@outlook.com* in our illustration.



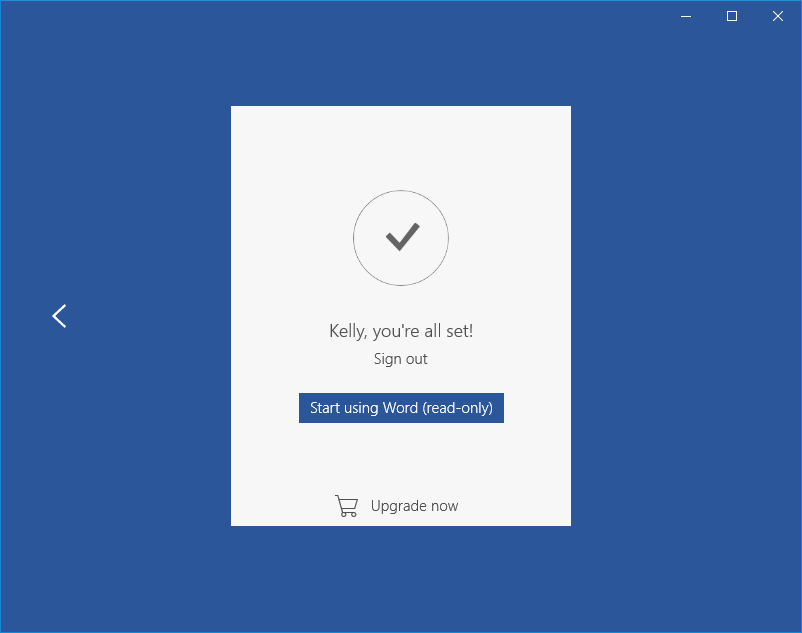
1. Imagine at this stage that you have to create a work document on your personal device. Start by downloading Word Mobile from the Store.



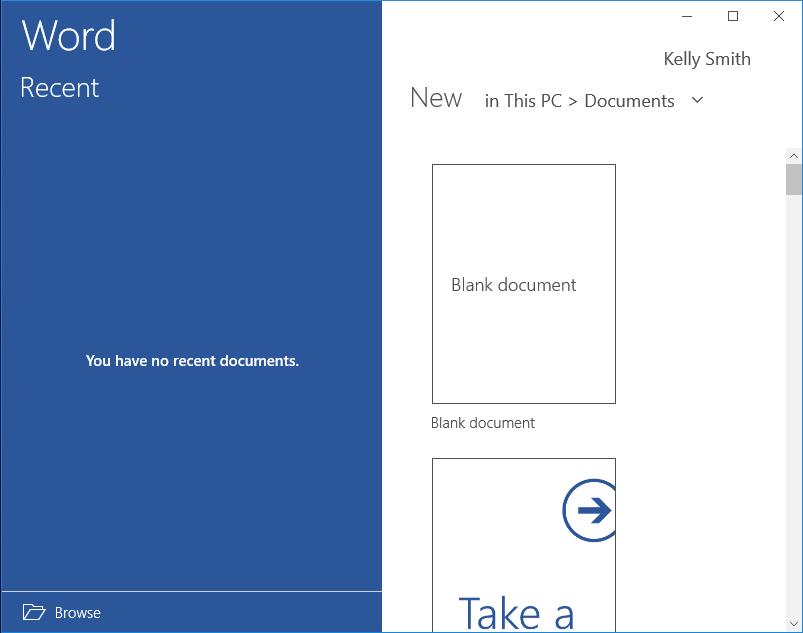
1. Click Free to install Word Mobile.



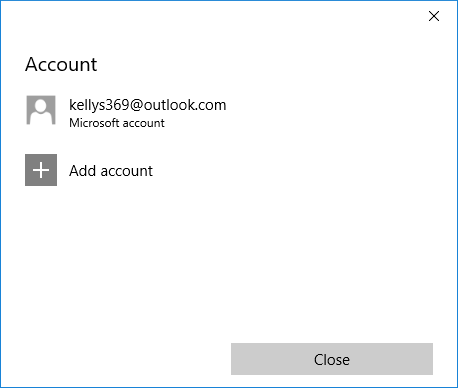
1. Click **Open** to launch Word Mobile.



1. Click **Start using Word (read-only)**.

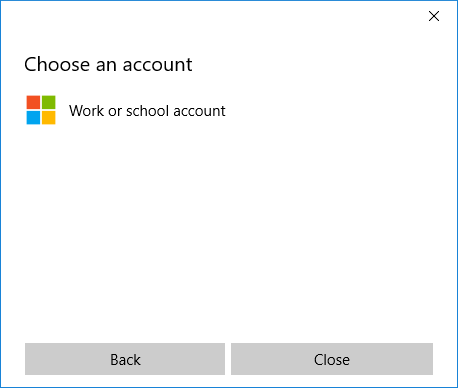


1. Click **Kelly Smith**. The **Account** dialog opens up.

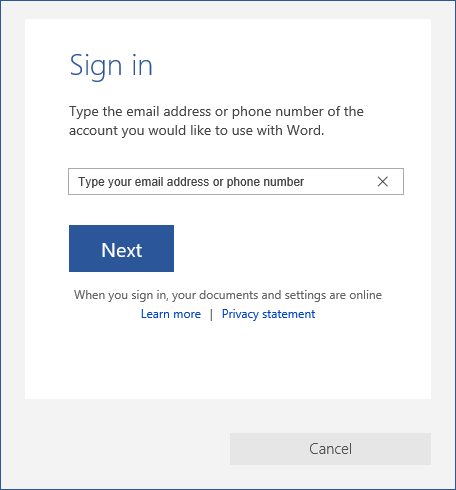


1. Click **Add account**.

Note While application experiences may differ from on to another, one can expect that most applications will have a Sign in button or an Add Account in the application settings as illustrated here with Word Mobile.

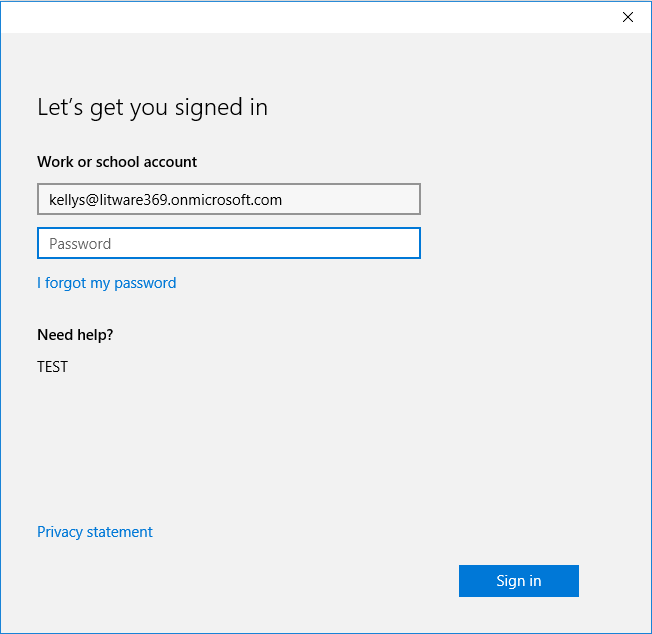


1. In the **Choose an account** screen, click **Work or school account**. A **Sign in** dialog pop up.

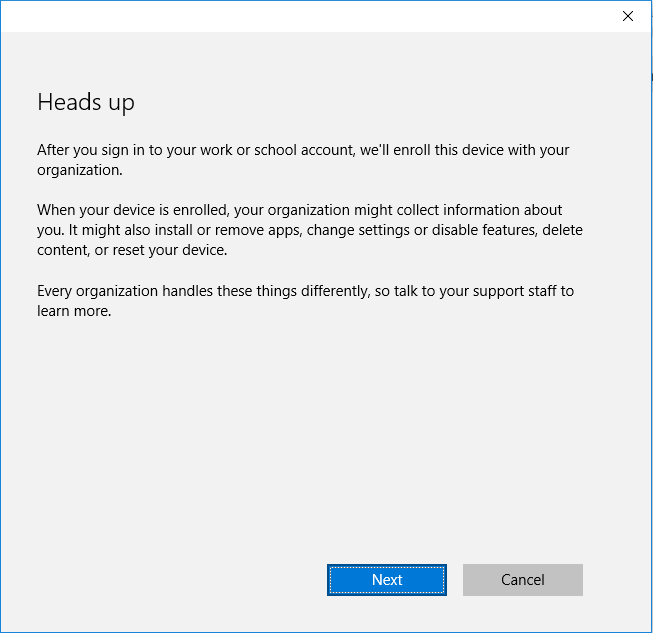


1. Specify a work account, for example *kellys@litware369.onmicrosoft.com* in our illustration, and then Click **Next**. Enter the work account credentials when prompted:

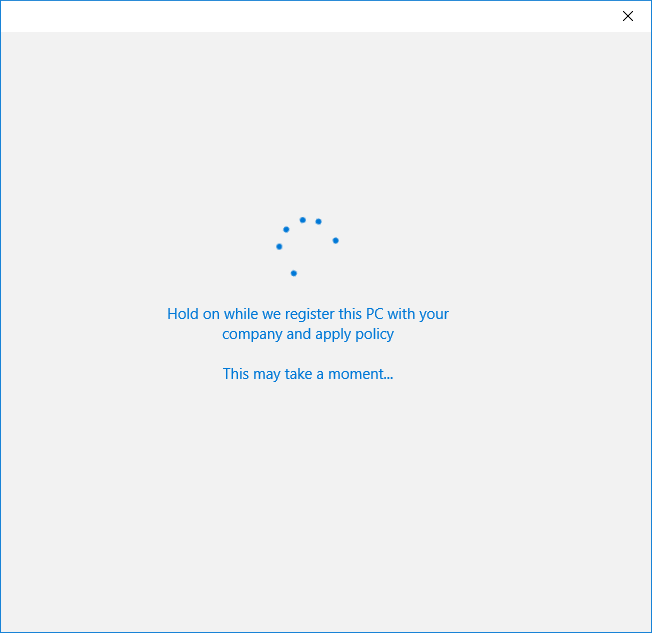
Password: *pass@word1*



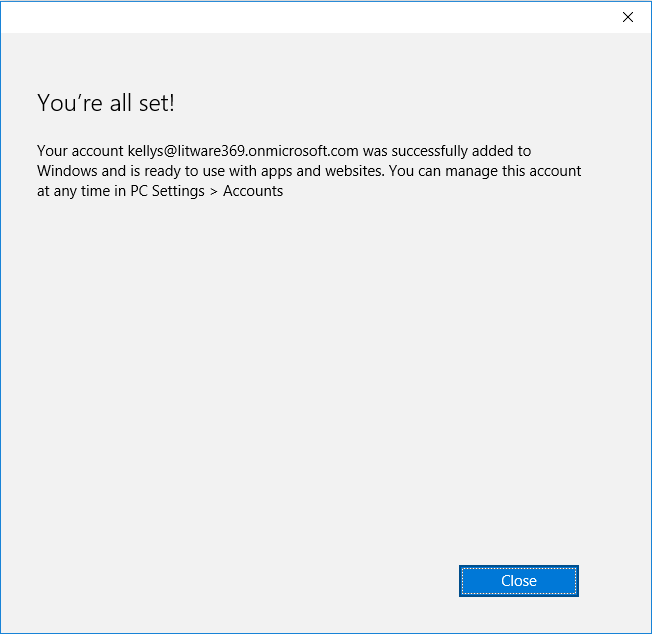
1. Click **Sign in**. After a successful authentication, MDM enrollment may occur (if configured by IT professionals) on some Windows 10 editions.



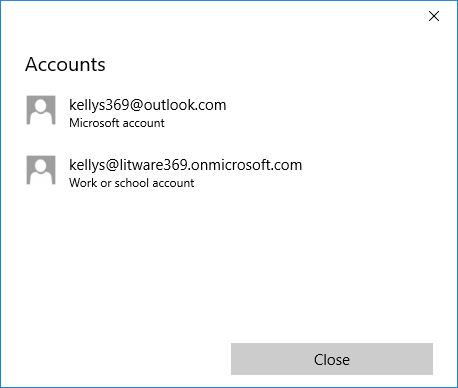
1. Click **Next**. Your device is now enrolled in the MDM solution.



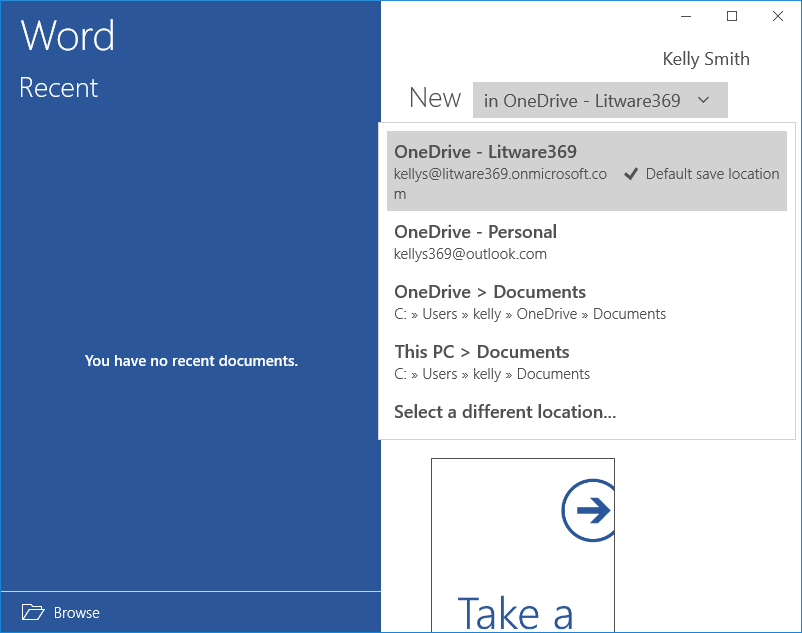
1. The device is registered in the organization’s Azure AD tenant and enrolled in the MDM solution.



1. Click **Close**.

e

1. The work is ready for use for access corporate resources like the organization’s OneDrive for Business. Click **Close** to close the dialog.
2. Click **in OneDrive – Litware369**.



Kelly’s work account is configured to be used with the Litware369 organization’s OneDrive for Business where as Kelly’s personal MSA account is configured to use her personal OneDrive.

1. Close **Word Mobile**.

Compared to what we already have covered in this paper regarding the “Azure AD Join” and “Domain Join” processes and related user experience, the major difference here resides in the fact that you will use your personal account to sign in and open a Windows session.

In other words, once an Azure AD account has been added, users will enjoy many of the same benefits on their personal device as they would on a corporate owned device joined to Azure AD.

This notably includes:

1. True SSO to resources protected by Azure AD from anywhere.

Note The device can participate in conditional access for user.

1. Access to the organization’s private catalog on the enterprise-ready Windows store.

Modern Windows services (a.k.a. Windows connected services) such roaming of personal settings will continue to be driven by your personal MSA account.

Note For additional information, see the blog post [Azure AD on Windows 10 Personal Devices](http://blogs.technet.com/b/ad/archive/2015/05/21/azure-ad-on-windows-10-personal-devices.as)[[75]](#footnote-75).

We hope that you are now equipped with a better understanding of the benefits that Azure AD and Windows 10 can provide together where:

* **User is productive in a mobile world with minimum IT**. Starting with a self-service configuration, users enjoy true SSO with both cloud and on-premises resources from everywhere, modern Windows services through their Azure AD work or school identity (enterprise-ready Windows store, etc.)
* **IT has the tools to manage devices, secure access and protect data**. (Automatic) auto-enrolment in an Azure AD integrated MDM solution indeed allows IT professionals to managed devices from the start while offering with solutions like Microsoft Intune and Mobile Device Management for Office 365 simple management through the cloud.

This concludes this document.

|  |
| --- |
| 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. Microsoft Azure is a flexible and open cloud computing platform hosted in Microsoft datacenters delivering scalable and reliable Internet-scale services. As an Infrastructure as-a-Service (IaaS) platform, Microsoft Azure Infrastructure Services enables to deploy (complex) workloads (servers, networking and storage infrastructure) in the cloud that you can control and manage on your terms. Also, as a Platform as-a-Service (PaaS) platform, it includes a number of features, which can be used individually or composed together in a public or hybrid cloud fashion. [↑](#footnote-ref-1)
2. Active Directory from on-premises to the cloud: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-2)
3. Using Application Proxy to publish applications for secure remote access: https://msdn.microsoft.com/en-us/library/azure/dn768219.aspx [↑](#footnote-ref-3)
4. Azure Active Directory editions: http://msdn.microsoft.com/en-us/library/azure/dn532272.aspx [↑](#footnote-ref-4)
5. Azure Active Directory Pricing: http://azure.microsoft.com/en-us/pricing/details/active-directory/ [↑](#footnote-ref-5)
6. Azure AD service limits and restrictions: http://msdn.microsoft.com/en-us/library/azure/dn764971.aspx [↑](#footnote-ref-6)
7. Azure Multi-Factor Authentication: https://azure.microsoft.com/en-us/services/multi-factor-authentication/ [↑](#footnote-ref-7)
8. Getting started with Azure AD: http://msdn.microsoft.com/en-us/library/dn655157.aspx [↑](#footnote-ref-8)
9. An overview of Azure AD: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-9)
10. Azure Active Directory community forum: http://social.msdn.microsoft.com/Forums/en-US/WindowsAzureAD/ [↑](#footnote-ref-10)
11. Azure blog: http://blogs.msdn.com/b/windowsazure/ [↑](#footnote-ref-11)
12. Microsoft Azure Active Directory and Windows 10: Better Together for Work or School: http://channel9.msdn.com/Events/Ignite/2015/BRK3332 [↑](#footnote-ref-12)
13. Microsoft Intune: http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/default.aspx [↑](#footnote-ref-13)
14. Azure Active Directory and Windows 10: Bringing the cloud to enterprise desktops!: http://blogs.technet.com/b/ad/archive/2015/05/13/azure-active-directory-and-windows-10-making-the-enterprise-cloud-a-reality.aspx [↑](#footnote-ref-14)
15. Azure AD joint on Windows 10 devices: http://blogs.technet.com/b/ad/archive/2015/05/21/azure-ad-on-windows-10-personal-devices.aspx [↑](#footnote-ref-15)
16. Managing Azure Active Directory joined devices with Microsoft Intune: http://blogs.technet.com/b/in\_the\_cloud/archive/2015/05/28/managing-azure-active-directory-joined-devices-with-microsoft-intune.aspx [↑](#footnote-ref-16)
17. Azure AD, Microsoft Intune and Windows 10 – Using the cloud to modernize enterprise mobility: http://blogs.technet.com/b/ad/archive/2015/06/12/azure-ad-microsoft-intune-and-windows-10-using-the-cloud-to-modernize-enterprise-mobility.aspx [↑](#footnote-ref-17)
18. Windows 10, Azure AD and Microsoft Intune: Automatic MDM enrollment powered by the cloud: http://blogs.technet.com/b/ad/archive/2015/08/14/windows-10-azure-ad-and-microsoft-intune-automatic-mdm-enrollment-powered-by-the-cloud.aspx [↑](#footnote-ref-18)
19. Azure AD on Windows 10 Personal Devices: http://blogs.technet.com/b/ad/archive/2015/05/21/azure-ad-on-windows-10-personal-devices.aspx [↑](#footnote-ref-19)
20. Office 365 Enterprise: http://office.microsoft.com/en-us/business/office-365-enterprise-e3-business-software-FX103030346.aspx [↑](#footnote-ref-20)
21. Overview built-in Mobile Device Management for Office 365: https://technet.microsoft.com/en-us/library/ms.o365.cc.devicepolicy.aspx [↑](#footnote-ref-21)
22. Introducing built-in mobile device management for Office 365: http://blogs.office.com/2014/10/28/introducing-built-mobile-device-management-office-365/ [↑](#footnote-ref-22)
23. Built-in mobile device management now generally available for Office 365 commercial plans: http://blogs.office.com/2015/03/30/announcing-general-availability-of-built-in-mobile-device-management-for-office-365/ [↑](#footnote-ref-23)
24. Sign in to Office 365: http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff637600.aspx [↑](#footnote-ref-24)
25. Office 365 Enterprise E3 Trial: http://office.microsoft.com/en-us/business/redir/XT104175934.aspx [↑](#footnote-ref-25)
26. Azure account portal: https://account.windowsazure.com/Subscriptions [↑](#footnote-ref-26)
27. 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-27)
28. Office 365 management portal: https://portal.microsoftonline.com [↑](#footnote-ref-28)
29. Azure management portal: https://manage.windowsazure.com [↑](#footnote-ref-29)
30. Application access enhancements for Azure AD: http://technet.microsoft.com/en-us/library/dn308588.aspx [↑](#footnote-ref-30)
31. Windows Azure Active Directory Applications: http://azure.microsoft.com/en-us/marketplace/active-directory/ [↑](#footnote-ref-31)
32. Azure AD/Office 365 Single Sign-On with AD FS in Windows Server 2012 R2 – Part 2: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-32)
33. Azure Active Directory Connect: http://www.microsoft.com/en-us/download/details.aspx?id=47594 [↑](#footnote-ref-33)
34. 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-34)
35. Integrating your on-premises identities with Azure Active Directory: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/ [↑](#footnote-ref-35)
36. Azure Active Directory Connect: https://msdn.microsoft.com/en-us/library/azure/dn832695.aspx [↑](#footnote-ref-36)
37. Windows Server 2016 Technical Preview 4: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview [↑](#footnote-ref-37)
38. Windows Server 2012 R2: http://technet.microsoft.com/en-US/windowsserver/hh534429 [↑](#footnote-ref-38)
39. Frequently Asked Questions: https://www.microsoft.com/en-us/software-download/faq [↑](#footnote-ref-39)
40. Installing Windows 10 using the media creation tool: http://windows.microsoft.com/en-us/windows-10/media-creation-tool-install?ocid=ms\_wol\_win10 [↑](#footnote-ref-40)
41. Client Hyper-V: https://technet.microsoft.com/en-us/library/hh857623.aspx [↑](#footnote-ref-41)
42. Install Hyper-V and create a virtual machine: https://technet.microsoft.com/en-us/library/hh846766.aspx [↑](#footnote-ref-42)
43. Azure Active Directory Device Registration Overview: https://msdn.microsoft.com/library/azure/dn903763.aspx [↑](#footnote-ref-43)
44. Adding Multi-Factor Authentication to Azure Active Directory: https://msdn.microsoft.com/library/azure/dn249466.aspx [↑](#footnote-ref-44)
45. Active Directory from on-premises to the cloud – Azure AD whitepapers: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-45)
46. Ibid [↑](#footnote-ref-46)
47. Using Multi-Factor Authentication with Active Directory Federation Services: https://technet.microsoft.com/library/dn394281.aspx [↑](#footnote-ref-47)
48. Overview built-in Mobile Device Management for Office 365: https://technet.microsoft.com/en-us/library/ms.o365.cc.devicepolicy.aspx [↑](#footnote-ref-48)
49. Manage mobile devices in Office 365: https://support.office.com/en-us/article/Manage-mobile-devices-in-Office-365-dd892318-bc44-4eb1-af00-9db5430be3cd [↑](#footnote-ref-49)
50. Create and deploy device security policies: https://technet.microsoft.com/en-us/library/ms.o365.cc.newdevicepolicy.aspx [↑](#footnote-ref-50)
51. Create DNS records for Office 365 when you manage your DNS records: https://support.office.com/en-gb/article/create-dns-records-for-office-365-when-you-manage-your-dns-records-b0f3fdca-8a80-4e8e-9ef3-61e8a2a9ab23 [↑](#footnote-ref-51)
52. Azure Authenticator (Windows Phone): https://www.microsoft.com/en-us/store/apps/azure-authenticator/9nblgggzmcj6 [↑](#footnote-ref-52)
53. Azure Authenticator (iOS): https://itunes.apple.com/us/app/azure-authenticator/id983156458?mt=8 [↑](#footnote-ref-53)
54. Azure Authenticator (Android): https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en [↑](#footnote-ref-54)
55. Try the new Azure Authenticator application!: http://blogs.technet.com/b/ad/archive/2015/06/29/try-the-new-azure-authenticator-app.aspx [↑](#footnote-ref-55)
56. Windows Server 2016 Technical Preview 4: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview [↑](#footnote-ref-56)
57. FIDO 2.0 Technical specifications: http://fidoalliance.org/specifications [↑](#footnote-ref-57)
58. Fast IDentity Online (FIDO) Alliance: https://fidoalliance.org/ [↑](#footnote-ref-58)
59. Microsoft Passport and Azure AD: Eliminating passwords one device at a time!: http://blogs.technet.com/b/ad/archive/2015/07/22/microsoft-passport-and-azure-ad-eliminating-passwords-one-device-at-a-time.aspx [↑](#footnote-ref-59)
60. Microsoft Passport overview: https://msdn.microsoft.com/en-us/library/dn985839(v=vs.85).aspx [↑](#footnote-ref-60)
61. The End Game for Passwords and Credential Theft?: http://channel9.msdn.com/Events/Ignite/2015/BRK3332 [↑](#footnote-ref-61)
62. Secure Authentication with Windows Hello: http://channel9.msdn.com/Events/Ignite/2015/BRK2324 [↑](#footnote-ref-62)
63. Azure Active Directory and Windows 10: Bringing the cloud to enterprise desktops!: http://blogs.technet.com/b/ad/archive/2015/05/13/azure-active-directory-and-windows-10-making-the-enterprise-cloud-a-reality.aspx [↑](#footnote-ref-63)
64. Set-MsolDomainFederationSettings: https://msdn.microsoft.com/en-us/library/azure/dn194088.aspx [↑](#footnote-ref-64)
65. What’s New in Active Directory Domain and Federation Services in Windows Server vNext: http://channel9.msdn.com/Events/Ignite/2015/BRK3871 [↑](#footnote-ref-65)
66. Windows Server 2016 Technical Preview 4: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview [↑](#footnote-ref-66)
67. Using the Business Store Portal with Windows 10 Devices: http://channel9.msdn.com/Events/Ignite/2015/BRK3338 [↑](#footnote-ref-67)
68. Modern business applications: http://www.microsoft.com/en-us/server-cloud/cloud-os/modern-business-apps.aspx [↑](#footnote-ref-68)
69. [MS-DVRE]: Device Registration Enrollment Protocol: https://msdn.microsoft.com/en-us/library/dn410252.aspx [↑](#footnote-ref-69)
70. Connect domain-joined devices to Azure AD for Windows 10 experiences: https://azure.microsoft.com/en-us/documentation/articles/active-directory-azureadjoin-devices-group-policy/ [↑](#footnote-ref-70)
71. Custom installation of Azure AD Connect: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-get-started-custom/ [↑](#footnote-ref-71)
72. Azure AD Connect: Version Release History: https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-version-history/ [↑](#footnote-ref-72)
73. Windows Server 2016 Technical Preview 4: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-technical-preview [↑](#footnote-ref-73)
74. What’s New in Active Directory Domain and Federation Services in Windows Server vNext: http://channel9.msdn.com/Events/Ignite/2015/BRK3871 [↑](#footnote-ref-74)
75. Azure AD on Windows 10 Personal Devices: http://blogs.technet.com/b/ad/archive/2015/05/21/azure-ad-on-windows-10-personal-devices.as [↑](#footnote-ref-75)