

<Insert Author Name>

Abstract

Pass-Through Authentication and Seamless Single Sign-on allow your users to sign in to both on-premises and cloud-based applications using the same passwords with minimal on-premises footprint. Combined, these two new authentication options can provide a similar, and in some cases, better sign-on experience than can be achieved with federation.

Azure Active Directory Implementation Guide **Migration from Federation to Pass-Through Authentication**

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

## Confidentiality statement

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

Table of Contents

Table of Contents

[Introduction 5](#_Toc509221639)

[Purpose of document 5](#_Toc509221640)

[Confidentiality statement 5](#_Toc509221641)

[What is managed authentication 5](#_Toc509221642)

[What is Cloud Authentication with Pass-Through Authentication 5](#_Toc509221643)

[What is Seamless Single Sign-on 7](#_Toc509221644)

[Benefits of moving to Pass-through Authentication & Seamless SSO 7](#_Toc509221645)

[Licensing 8](#_Toc509221646)

[Azure Active Directory Licensing 8](#_Toc509221647)

[Project Scope 8](#_Toc509221648)

[Prerequisites 8](#_Toc509221649)

[In scope 9](#_Toc509221650)

[Out of scope 9](#_Toc509221651)

[Project Steps 9](#_Toc509221652)

[Planning for Pass-Through Authentication and Seamless SSO 10](#_Toc509221653)

[Review supported scenarios and limitations 10](#_Toc509221654)

[Authentication Agent placement 10](#_Toc509221655)

[Smart Lockout 11](#_Toc509221656)

[Change Communications 11](#_Toc509221657)

[Maintenance window 11](#_Toc509221658)

[Converting from Federation to PTA and Seamless SSO 13](#_Toc509221659)

[Verify Current User Sign-in settings 13](#_Toc509221660)

[Verify how Federation was configured 13](#_Toc509221661)

[Preparation steps 15](#_Toc509221662)

[Validate current AD FS usage 15](#_Toc509221663)

[Backup federation settings 16](#_Toc509221664)

[AD FS Branding 17](#_Toc509221665)

[Other ADFS customisations 17](#_Toc509221666)

[Azure AD Hybrid Join 18](#_Toc509221667)

[Enable Modern Authentication for all clients and services 18](#_Toc509221668)

[Deploy Seamless Single Sign on 18](#_Toc509221669)

[Option 1 - Switch from Federation to PTA using Azure AD Connect 18](#_Toc509221670)

[Convert users 21](#_Toc509221671)

[Complete the process 22](#_Toc509221672)

[Option 2 - Switch from Federation to PTA using Azure AD Connect and PowerShell 23](#_Toc509221673)

[Change User Sign-in method in Azure AD Connect 23](#_Toc509221674)

[Verify configuration settings 25](#_Toc509221675)

[Convert Domains from Federated to Managed 26](#_Toc509221676)

[Convert users 27](#_Toc509221677)

[Next Steps and Testing 28](#_Toc509221678)

[Deploy Additional Authentication Agents 28](#_Toc509221679)

[Removal of the Relying Party Trust 29](#_Toc509221680)

[Rollback 30](#_Toc509221681)

[Test Pass-through Authentication 30](#_Toc509221682)

[Operations 31](#_Toc509221683)

[Roll over the Seamless SSO Kerberos decryption 31](#_Toc509221684)

[Monitoring and logging 32](#_Toc509221685)

# Introduction

## Purpose of document

This document describes the key considerations and processes involved to deploy Pass-Through Authentication and Seamless Single Sign-On as a replacement of Federated Authentication with Azure Active Directory.

## What is managed authentication

In a federated authentication model, authentication is delegated to another Identity Provider, typically an on-premises system. In the Managed Authentication model, authentication is driven by Azure Active Directory with a minimal on-premises footprint. There are two options when it comes to selecting a Managed Authentication Model, Cloud Authentication with Password Hash Synchronization and Cloud Authentication with Pass-Through Authentication.

For more information on selecting an authentication model, refer to the following document: <https://aka.ms/auth-options>.

## What is Cloud Authentication with Pass-Through Authentication

With pass-through authentication, user’s passwords are validated against on-premises Active Directory. This allows for on-premises policies, such as sign-in hour restrictions or account expiration, to be evaluated during authentication to cloud services.

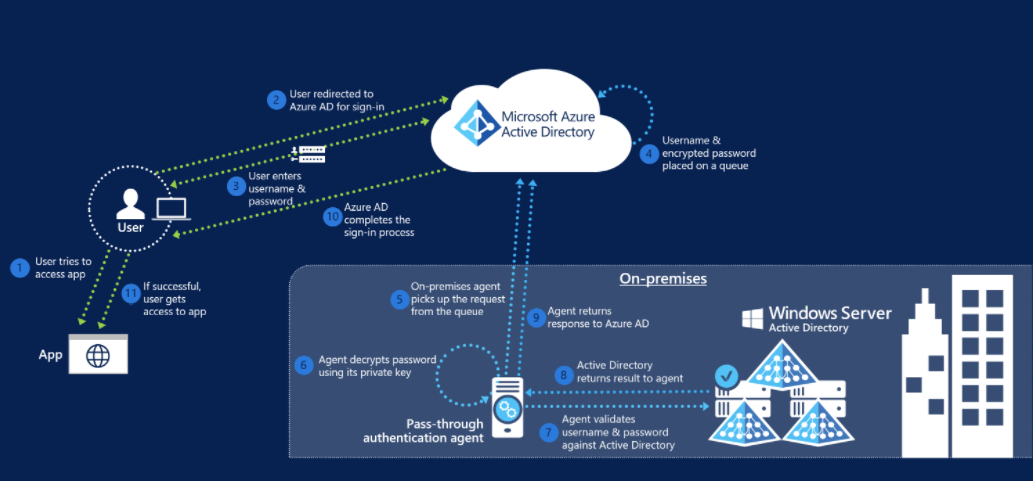
Pass-through authentication uses lightweight agents deployed in the on-premises environment. The agents listen for password validation requests sent from Azure AD and don’t require any inbound ports to be open to the Internet to function. Passwords don’t need to be present in Azure AD in any form.

Password Hash Synchronization can be combined with Pass-Through Authentication to obtain the following benefits:

* As a Disaster Recovery option in case the on-premises Active Directory infrastructure is unavailable or compromised.
* To leverage the Leaked Credentials security report in Azure AD.

This is an overview of how Azure Active directory (Azure AD) Pass-through Authentication works. For deep technical and security information, see the [Security deep dive](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-security-deep-dive) article.

The following diagram illustrates all the components and the steps involved:



When a user tries to sign in to an application secured by Azure AD, and if Pass-through Authentication is enabled on the tenant, the following steps occur:

1. The user tries to access an application, for example, Outlook Web App.
2. If the user is not already signed in, the user is redirected to the Azure AD User Sign-in page.
3. The user enters their username and password into the Azure AD sign in page, and then selects the Sign in button.
4. Azure AD, on receiving the request to sign in, places the username and password (encrypted by using a public key) in a queue.
5. An on-premises Authentication Agent retrieves the username and encrypted password from the queue. Note that the Agent doesn't frequently poll for requests from the queue but retrieves requests over a pre-established persistent connection.
6. The agent decrypts the password by using its private key.
7. The agent validates the username and password against Active Directory by using standard Windows APIs, which is a similar mechanism to what Active Directory Federation Services (AD FS) uses. The username can be either the on-premises default username, usually userPrincipalName, or another attribute configured in Azure AD Connect (known as Alternate ID).
8. The on-premises Active Directory domain controller (DC) evaluates the request and returns the appropriate response (success, failure, password expired, or user locked out) to the agent.
9. The Authentication Agent, in turn, returns this response back to Azure AD.
10. Azure AD evaluates the response and responds to the user as appropriate. For example, Azure AD either signs the user in immediately or requests for Azure Multi-Factor Authentication.
11. If the user sign-in is successful, the user can access the application.

## What is Seamless Single Sign-on

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their domain joined devices connected to your corporate network. Seamless SSO leverages native Kerberos to provide the improved sign-in experience to the user. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless Single Sign-on can be combined with Password Hash Synchronization or Pass-Through Authentication.

* **Microsoft recommends** always combining Seamless SSO with either Password Hash Synchronization or Pass-Through Authentication as it will always substantially improve the end user authentication experience for those users who can leverage it (i.e. domain joined/corporate connected).

## Benefits of moving to Pass-through Authentication & Seamless SSO

1. Reduction in costs by:
   1. Removing the on-premises footprint required to maintain a highly available and redundant AD FS farm, including servers and internal/external load balancers.
   2. Removing certificate management administration overhead and costs
   3. Simplifying monitoring, administration, and ongoing maintenance.
2. Reduced risk by:
   1. Not being susceptible to any authentication outages caused by configuration, certificate expiration/rollover, or performance issues, as well as other on-premises dependencies required by AD FS.
   2. Now being able to take advantage of user authentication at cloud scale.
3. Reduced complexity by:
   1. Using Azure AD Conditional Access policies over complex custom claims issuance rules in AD FS to restrict access and/or control authorization to cloud services.
   2. No longer requiring split DNS to be configured.
4. Improve security:
   1. By no longer requiring any inbound ports to be open to your network for user authentication requests. This allows you to close a common attack vector.
   2. By letting Azure AD protect users accounts from brute force and password spray attacks (and other malicious activity) with its unique Smart Lockout capability and Identity Protection service.
   3. By gaining deeper insights into user authentication sign-in activity, such as where users are signing-in from and from what clients and devices, using the rich reporting capabilities of the Azure AD sign-in logs.

# Licensing

## Azure Active Directory Licensing

While many features are included with Azure AD Free and Azure AD Basic, some features require Azure AD Premium (P1 or P2). Both Pass-through authentication and Seamless SSO do not require Azure AD Premium and are free to use and deploy, however, there may be associated Azure AD Premium features that you need to use that do require a license assigned to be compliant, or to gain access to the particular feature. Common Azure AD Premium scenarios include the following recommended security features:

* [Conditional Access (CA)](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal) (P1 Required)
* [Azure Multi-Factor Authentication (MFA) (P1 Required)](https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-how-it-works)
* [Group based membership](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups) (P1 required)
* [Identity Protection](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection) (P2 Required)

For a full list of license requirements, click [here](https://azure.microsoft.com/en-us/pricing/details/active-directory/).

# Project Scope

## Prerequisites

The following are presumed to be in place prior to the beginning of this project.

* That the latest build of AAD Connect is installed. You can download the latest version [here](https://www.microsoft.com/en-us/download/details.aspx?id=47594).
* That the required network connectivity is in place (port 80/443 outbound only), and the specific public target FQDN’s are whitelisted on your firewall/proxy, and are resolvable for the PTA agents to install, register, and communicate successfully with Azure AD. Specific network requirements for the PTA agents are detailed [here](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-quick-start#in-your-on-premises-environment).
* That the servers where you will install the PTA agents on are running the correct version of Windows (2012R2 or 2016).
* That you have access to a Global Administrator account to be able to configure PTA in your tenant and run through the conversion process of the domains from federated to managed.
* That you have access to a Domain Administrator account to be able to configure Seamless SSO in the On-Premises Active Directory.
* Confirmed that Modern Authentication is enabled in your Office 365 tenant for both Exchange Online and Skype For Business Online. Please refer to [this](https://support.office.com/en-us/article/Enable-or-disable-modern-authentication-in-Exchange-Online-58018196-f918-49cd-8238-56f57f38d662) article for steps on checking or enabling Modern Authentication.
* Enabled Modern Authentication for any Office 2013 clients.
* That you have [rolled out](#_Deploy_Seamless_Single) the required “Intranet Zone” settings via GPO to all domain joined machines so that they can leverage Seamless SSO once it has been enabled.
* If you have an Account Lockout Threshold GPO set on-premises that locks the account out after less than 10 failed password attempts then you will also need to make sure that you have an Azure AD P2 license available and assigned for a single Global Administrator so you can edit the Smart Lockout settings in Azure AD to [tune it](#_Smart_Lockout) to your environment to prevent accounts being locked out through failed password attempts coming through pass-through authentication requests.

## In scope

The following are in scope for this project:

**Enabling Pass-through Authentication**

* Changing the user sign-in method from federated to managed through Azure AD Connect
* Converting federated domains to managed
* Converting federated users
* Installing the pass-through authentication agent(s)

**Enabling Seamless SSO**

* Configuring the required GPO
* Enabling the Seamless SSO feature via Azure AD connect

**Deployment and Support**

* Rollback scenarios
* Testing and validation steps
* Troubleshooting

## Out of scope

The following are out of scope of this project:

* Deployment of Azure AD Connect
* Migrating any AD FS custom claims authorization rules to conditional access policies
* Configuring Multi-factor authentication (Azure MFA)
* Assigning licenses to users
* Providing detailed backup and restoration steps for AD FS
* Configurating Hybrid Azure AD join

# Project Steps

We present two options in this document for moving from a federated to a managed domain.

[Option 1 - Switch from Federation to PTA using Azure AD Connect](#_Option_1_-)

or

[Option 2 - Switch from Federation to PTA using Azure AD Connect and PowerShell](#_Option_2_-)

Which option you choose ultimately depends on whether AD FS was originally configured by AAD Connect or not. For customers who configured AD FS through AAD Connect, then changing the user sign-in experience to use pass-through authentication must be performed through the AAD Connect wizard.

***Note:*** Regardless of which option you need to take (option 1 or 2) the underlying conversion process is the same for each and involves two steps.

1. The domain(s) are set to “Managed” using the Set-MsolDomainAuthentication cmdlet
2. The users are converted using the Convert-MsolFederatedUser cmdlet

The only difference between option 1 and option 2 is that AAD Connect runs the Set-MsolDomainAuthentication cmdlet for you automatically when you change the user sign-in method, and hence you have no control over it un-federating ***all of the domains***. Whereas option 2 is completely under your control as you run the same cmdlet manually. The user conversion process is required and are manual tasks for both options. AAD Connect ***will not*** convert the users for you.

To determine if AD FS was originally configured by AAD Connect refer to the [Verify how Federation was configured](#_Verify_how_Federation) section of this document.

# Planning for Pass-Through Authentication and Seamless SSO

## Review supported scenarios and limitations

As part of the planning process, it is a good idea to review the supported scenarios and the current limitations of Pass-Through Authentication and Seamless SSO. Please refer to the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-current-limitations>

## Authentication Agent placement

Installing multiple Authentication Agents will provide high availability to the solution. Try to deploy agents as close as possible to Active Directory Domain Controllers and in different datacentres to ensure authentication traffic can still be served in case of a datacentre failure.

For most customers two or three authentication agents are sufficient for high availability and capacity. It is important to note that the first agent is always installed on the AAD Connect server itself when the pass-through authentication feature is enabled. If performance is a concern for your AAD Connect server, or if you wish to prevent the agent installed on it from servicing any authentication requests then the agent services, “Microsoft Azure AD Connect Authentication Agent” and “Microsoft Azure AD Connect Agent Updater”, can be safely disabled provided you have successfully installed at least another agent on a server elsewhere in your environment.

For more information on network traffic estimations and performance guidance refer to the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-faq#how-many-pass-through-authentication-agents-do-i-need-to-install>

## Smart Lockout

Azure AD Smart Lockout protects against brute-force password attacks and prevents the on-premises Active Directory account from being locked out when pass-through authentication is being used and an account lockout group policy is set in Active Directory. The Smart Lockout behaviour is as follows:

Lockout Threshold – default 10 failed attempts  
Lockout Duration – default 60 seconds

Lockout Duration automatically increases with a continuing attack. Machine intelligence algorithms attempt to distinguish between genuine users and attackers. Factors include past sign-in behaviour, user’s devices and browsers. The Smart Lockout settings can be adjusted via Graph API but requires an Azure AD P2 license to do so. It is recommended to configure the Smart Lockout threshold to a number lower than your current on-premises account lockout threshold to invoke Smart Lockout before allowing the failed password attempts to traverse on-premises and trip the lockout threshold group policy.

For more information on Smart Lockout feature and how to edit its configuration please refer to the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-smart-lockout>

If you don’t have an [account lockout threshold](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold) group policy set today in Active Directory, then there is no requirement for you to edit the Smart Lockout behavior and you can safely go with the default settings and still stay protected.

## Change Communications

After both pass-through authentication and Seamless SSO are deployed the end user sign-in experience will change slightly when accessing Office 365 and other associated resources underpinned by Azure AD. For users external to the network they will now see the Azure AD logon page only as opposed to being redirected to the forms-based page presented by the external facing Web Application Proxy servers.

[Branding](#_AD_FS_Branding) can be used to customise the Azure AD logon screen, however visual changes are to be expected.

* **Microsoft recommends** communicating to end users about these changes to reduce help desk calls and drive positive adoption.

## Maintenance window

The conversion process for moving from federated to managed involves not only converting the domain(s), but also the users. The domain conversion process itself is relatively quick, however Exchange Online can hold a cache for a period that can still end up sending Exchange ActiveSync clients to your AD FS environment even after the domain is no longer federated. Exchange Active Sync can take up to 4 hours until users will no longer get redirected to AD FS. During this time users might not be able to download email on EAS clients (native mail client on iOS / Android). It is recommended to ***not*** shut down your AD FS environment or remove the Office 365 relying party trust until after 12 hours from successful domain conversion has transpired, at which point you can safely shutdown and start to dismantle your AD FS farm.

Aside from Exchange ActiveSync clients, it is important to note that the process of converting a domain from federated to managed and converting users should not cause any authentication outage for users using a browser, or modern authentication client. Uses will still be able to authenticate to Azure AD with these clients during the changes, but some users may still be redirected to AD FS for a period of time during the maintenance window.

Whilst the conversion of the domain is near instant, the user conversion process is slightly more nuanced, and the length of time this will take is ultimately dictated by how many users you have in your tenant that you need to convert. The PowerShell cmdlet to convert users can process (on average) 2 users per second.

As an example, if you needed to convert 5,000 users then this would take roughly 41 minutes to complete. 5,000/2 = 2,500 /60 = 41.6667

The length of your maintenance window will largely be dictated by how long you calculate the user conversion process to take.

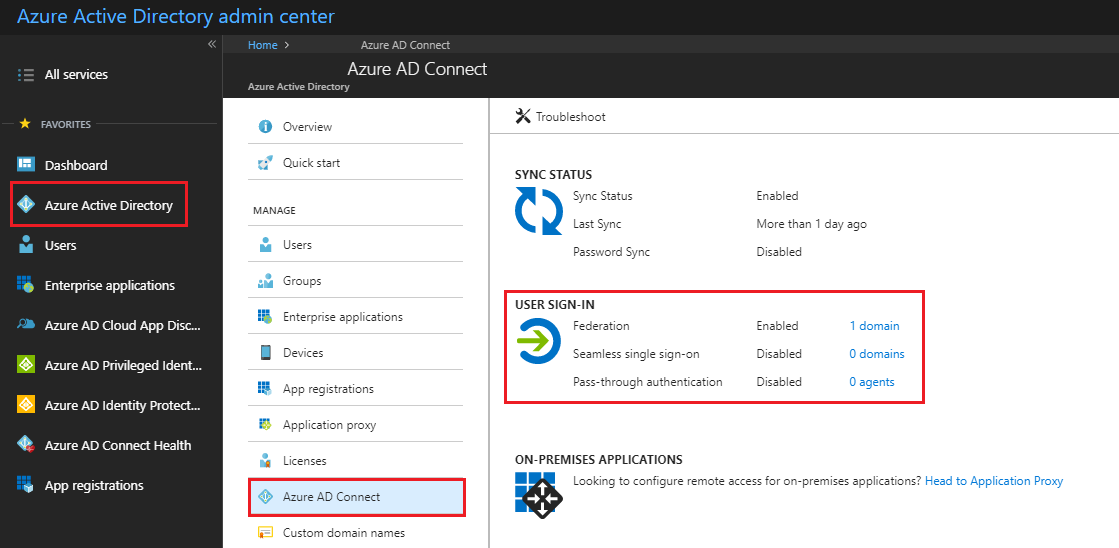
# Converting from Federation to PTA and Seamless SSO

This section describes the steps required to convert a deployment currently using Federation to Cloud Authentication with Pass-Through Authentication and Seamless Single Sign-On.

## Verify Current User Sign-in settings

Verify your current User Sign-in settings by logging into the Azure AD portal <https://aad.portal.azure.com> with a **Global Administrator** account.

In the **User Sign In** section, verify that **Federation** is **Enabled** while **Seamless Single Sign-on** and **Pass-through authentication** should show as **Disabled.**

****

### Verify how Federation was configured

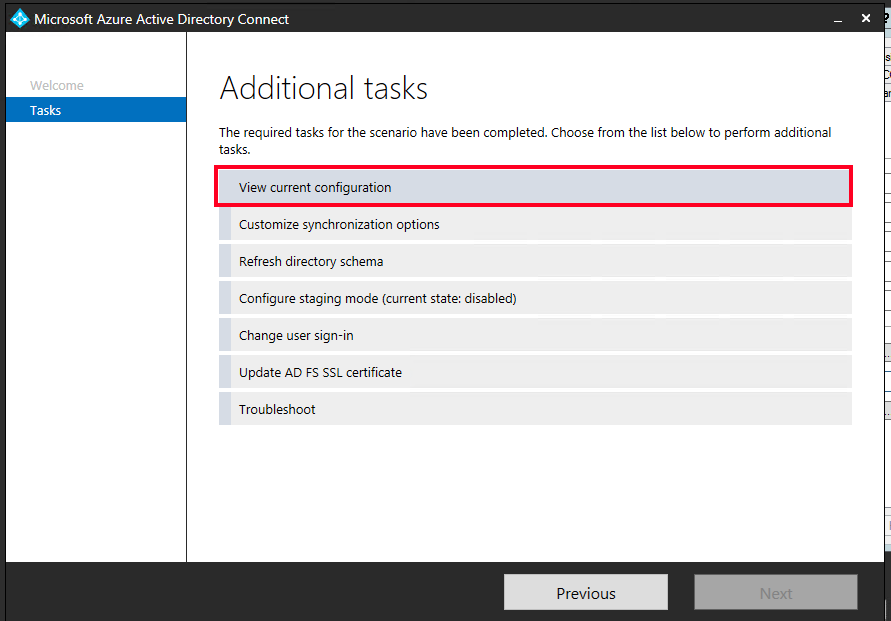
Federating domains with Azure AD can be configured either through Azure AD Connect or through PowerShell. In this step we will understand how federation was originally configured to guide you through the appropriate steps to convert your domain(s) from federated to managed.

This is important because if Federation was configured through Azure AD Connect, changing the authentication mode from Federation to Pass-Through Authentication will convert ***all*** federated domains in the tenant to managed.

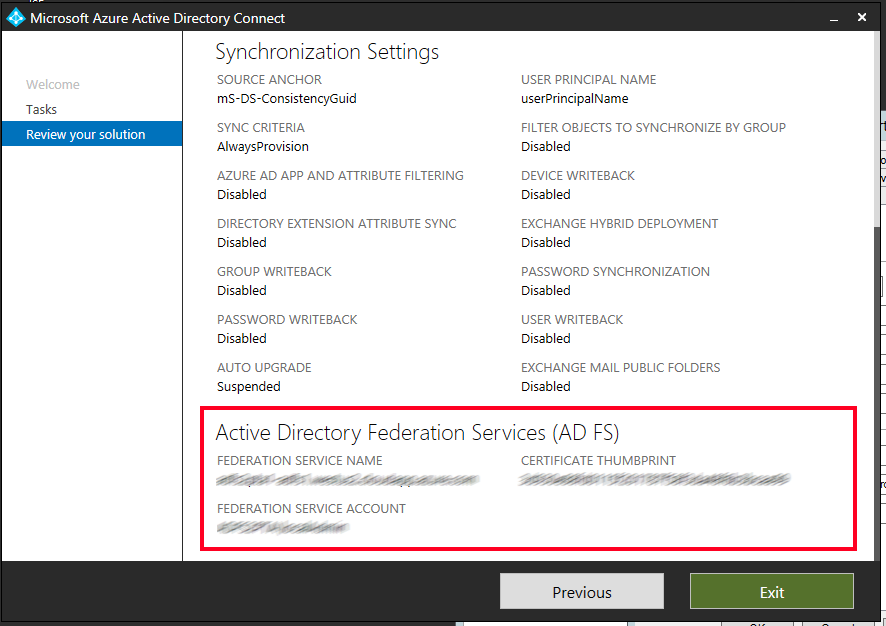
***Note:*** At this time, you cannot avoid un-federating all domains in your tenant when you change the user sign-in to pass-through authentication when AAD Connect was originally used to configure AD FS for you. If you require that some domains still remain as federated, then you should consider enabling Password Hash Sync instead of Pass-through Authentication, which will allow you to control what domains can be converted manually via PowerShell.

#### Verify Azure AD Connect settings

Go to your Azure AD Connect server and launch Azure AD Connect, then click on **Configure.** On the **Additional Tasks** screen, click on **View Current Configuration** and then click on **Next.**



In the **Review Your Solution** screen scroll down to the **Active Directory Federation Services (AD FS).**   
If you see that the AD FS configuration is in this section then you can safely assume AD FS was originally configured through Azure AD Connect and hence the conversion of your domain(s) from federated to managed can be driven through the Azure AD Connect **“Change user sign-in”** option, this process is detailed in the section “[Option 1- Switch from Federation to PTA using Azure AD Connect](#_Option_1_-)”.

****

If you can’t see Active Directory Federation Services listed in the current settings, then you will need to manually convert the domains from federated to managed via PowerShell which is detailed in the section “[Option 2 - Switch from Federation to PTA using Azure AD Connect and PowerShell](#_Option_2_-)”.

## Preparation steps

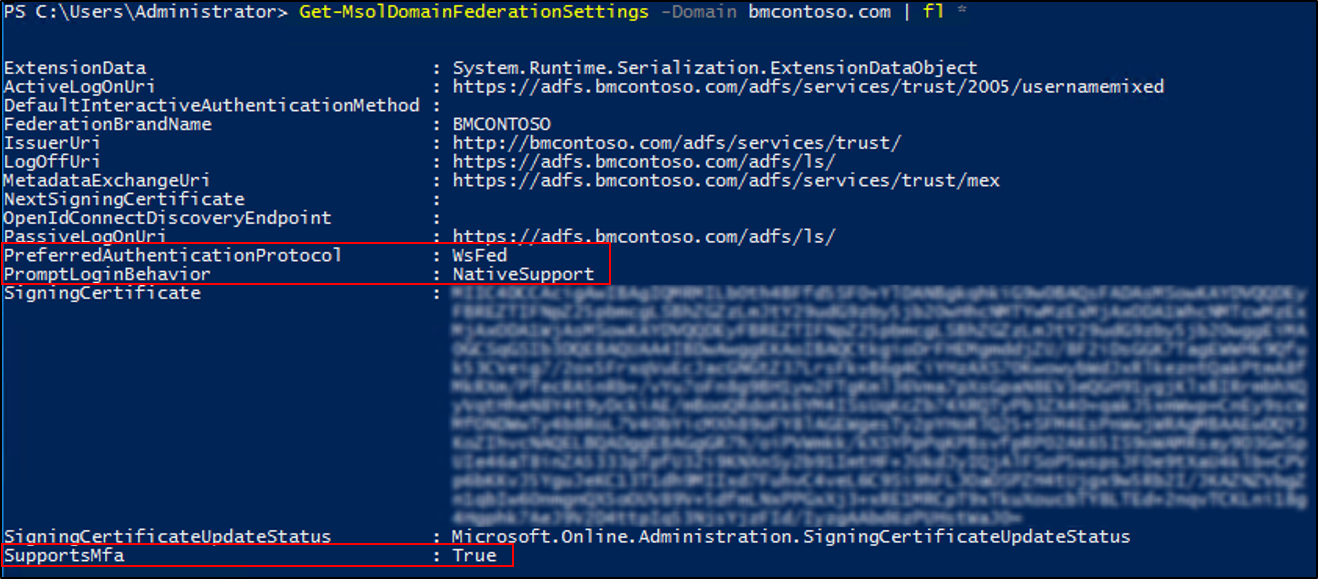
Complete the following steps in preparation for the conversion of your authentication model from Federated to Managed using Pass-Through Authentication.

### Validate current AD FS usage

Before converting from Federated to Managed you should look closely at how you are using AD FS today for Azure AD/Office 365 and other applications (relying party trusts). Specifically, you should consider the following:

1. Are you going to retain AD FS for those other applications? If so you will end up using two IdP's (AD FS and Azure AD) and will need to consider the end user experience as a result. Users may need to authenticate twice in some scenarios, once to Azure AD (where they will get SSO onwards to other applications like Office 365) and again for any applications still bound to AD FS as a relying party trust.
2. Is AD FS heavily customised today and reliant on specific customisation settings in the onload.js file that cannot be duplicated in Azure AD? For example, have you changed the sign-in experience where users only need to enter in a SamAccountName format for their username as opposed to a UPN, or heavily branded the login experience? You will need to verify that your current customisation requirements can be met by Azure AD before proceeding. Refer to the [AD FS Branding](#_AD_FS_Branding) and [AD FS Customization](#_Other_ADFS_customisations) sections of this document for further information and guidance.
3. Are you blocking legacy authentication clients via AD FS? Today this is the only way to effectively truly block all legacy authentication client scenarios and you will not be able to prevent all legacy authentication clients from connecting to services when you move to a managed domain. The only mechanism available today to block these clients with a managed domain is via by disabling certain protocols against the mailbox in Exchange Online, such as POP/IMAP, or by using the new Exchange Online Client Access rules capabilities.
4. Are you requiring users to perform MFA against an on-premises MFA server solution when authenticating to AD FS? You won't be able to inject an MFA challenge via the on-premises MFA solution into the authentication flow for a managed domain, however you can use the Azure MFA service to do so going forward once the domain is converted. If users are not using Azure MFA today, then this will involve a onetime end user registration step that you will have to prepare for and communicate to your end users.
5. Do you use Access Control Policies (AuthZ rules) today in AD FS to control access to Office 365? If so, consider replacing these with the equivalent Azure AD [Conditional Access Policies](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal) and [Exchange Online Client Access Rules](http://aka.ms/EXOCAR).
6. Document the current federation settings in Azure AD via the Get-MsolDomainFederationSettings cmdlet.  
     
   Get-MsolDomainFederationSettings -DomainName contoso.com | fl \*

Validate any settings that might have been customised to your Federation design and deployment documentation, specifically the PreferredAuthenticationProtocol, SupportsMfa, and PromptLoginBehavior property values.



### Backup federation settings

It’s important to plan what to do if your deployment doesn’t go as planned. If the conversion of the domain or users fails during the deployment, or you need to rollback to federation, then you must understand how to mitigate any outage and reduce the impact to your users. Although no changes will be made to other Relying Parties on your AD FS farm during this process, it is recommended to make sure you have a current valid backup of your AD FS farm that can be restored. You can do this using the free AD FS Rapid Restore Tool available from here. This tool can be used to backup and restore AD FS, either to an existing farm, or a new farm.

At a minimum, you should export "Microsoft Office 365 Identity Platform" relying party trust and any associated custom claim rules you may have added. You can do this via the following PowerShell example

(Get-AdfsRelyingPartyTrust -Name "Microsoft Office 365 Identity Platform") | Export-CliXML "C:\temp\O365-RelyingPartyTrust.xml"

### AD FS Branding

ADFS sign-in pages can be customised to display information more pertinent to the organisation. If you have made customisations to ADFS, consider making similar changes to the Azure AD sign-in page.

Check the following document for a reference on the customisations available for ADFS.

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-user-sign-in-customization>

Check the following document for a reference on the customisations available for the Azure AD sign-in page.

<https://docs.microsoft.com/en-us/azure/active-directory/customize-branding>

***Note:*** Company branding is available only if you purchased the Premium or Basic license for Azure AD or have an Office 365 license.

### Other ADFS customisations

The following items are common customisations made on ADFS deployments and should be carefully considered before converting your domains to Pass-Through Authentication.

#### Inside Corporate Network claim

The InsideCorporateNetwork claim in ADFS is present when users authenticate from inside the corporate network using Windows Integrated Authentication. This claim is then passed onto Azure AD and is commonly used to bypass Multi-Factor authentication based on the users’ network location.

Refer to the following document for more information about this claim and how to check if your ADFS farm has been configured to leverage it.

<https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-get-started-adfs-cloud>

The InsideCorporateNetwork claim won’t be available anymore once your domains are converted to Pass-Through Authentication. Named Locations in Azure AD can be used to replace this functionality.

Refer to the following document for Named Locations configuration.

<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-named-locations>

Once Named Locations have been configured, all Conditional Access policies configured to include or exclude the network locations “All trusted locations” or “MFA Trusted IPs” must be updated to reflect the newly created Named Locations.

For more information on the Location condition in Conditional Access refer to the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-locations>

### Azure AD Hybrid Join

Azure AD Hybrid Join for environments that are federated requires adding at least three additional Claim Issuance Rules to the Azure AD Relying Party Trust in your AD FS deployment. To make sure Hybrid Join continues working for any new devices joined to the domain once your domains have been converted to Pass-Through Authentication, Azure AD Connect must be configured to synchronise Active Directory computer accounts to Azure AD for Windows 10 clients. For down-level operating systems, namely Windows 7 and Windows 8, Hybrid Join will use Seamless SSO to register the computer in Azure AD and you do not have to sync these down-level computer accounts unlike Windows 10. You will however have to deploy an updated workplacejoin.exe file (via an .msi) to these down-level clients so they can register themselves using Seamless SSO. This .msi is available for download from [here](https://www.microsoft.com/en-us/download/details.aspx?id=53554).

For more information on this requirement, refer to the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/device-management-hybrid-azuread-joined-devices-setup>

### Enable Modern Authentication for all clients and services

Whilst pass-through authentication does support authenticating certain legacy clients (Exchange ActiveSync, Outlook 2010/2013 etc) organizations are encouraged to switch to modern authentication, if possible. Modern authentication allows for Pass-through Authentication support. It also helps you secure your user accounts by using conditional access features, such as Azure Multi-Factor Authentication. To verify that your Office 365 tenant is configured for modern authentication please refer to this article:

[How modern authentication works for Office 2013 and Office 2016 client apps](https://support.office.com/en-us/article/how-modern-authentication-works-for-office-2013-and-office-2016-client-apps-e4c45989-4b1a-462e-a81b-2a13191cf517?ui=en-US&rs=en-US&ad=US)

### Deploy Seamless Single Sign on

The deployment of Seamless Single Sign-On comprises two main steps:

* Enable client devices to utilise SSSO
* Enable the SSSO feature.

Client devices can be enabled for SSSO using a group policy. We recommend performing this step before enabling the SSSO feature and converting your domains to Pass-Through Authentication to minimise the time in which your users might be prompted for a username and password.

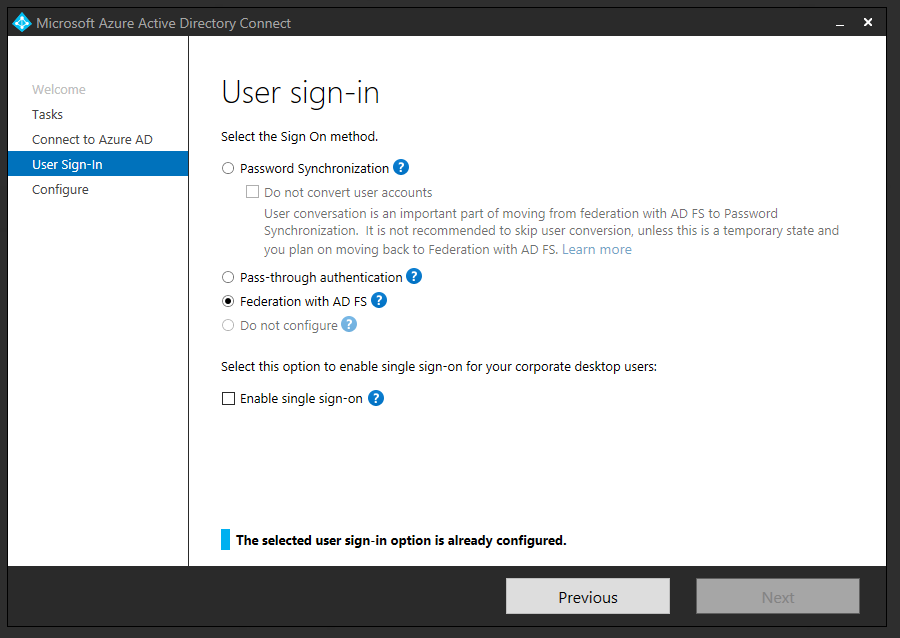
For more information on the changes required, refer to the following document.

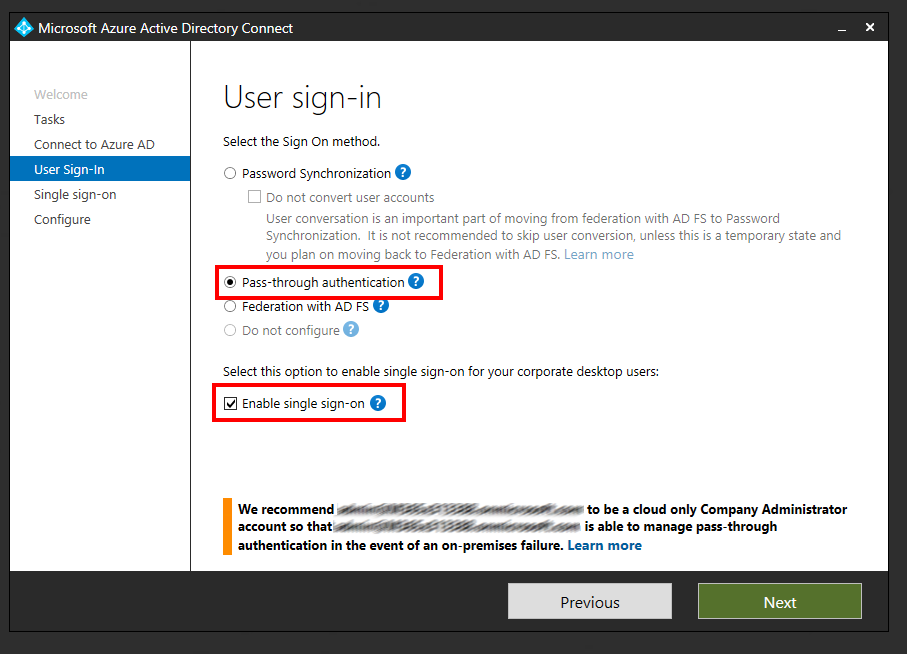
<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-quick-start#step-3-roll-out-the-feature>

## Option 1 - Switch from Federation to PTA using Azure AD Connect

In the Azure AD Connect wizard that you have open from the previous step, click on **Previous** to go back to the **Additional Tasks** screen. Click on **Change User Sign in** and then click **Next**. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.

In the **User Sign-in** Screen, **Select the Sign in method,** itshould be set to **Federation with AD FS**. Change the radio button to select **Pass-through authentication.** In addition, click on the checkbox next to **Enable single sign-on** then click **Next.**



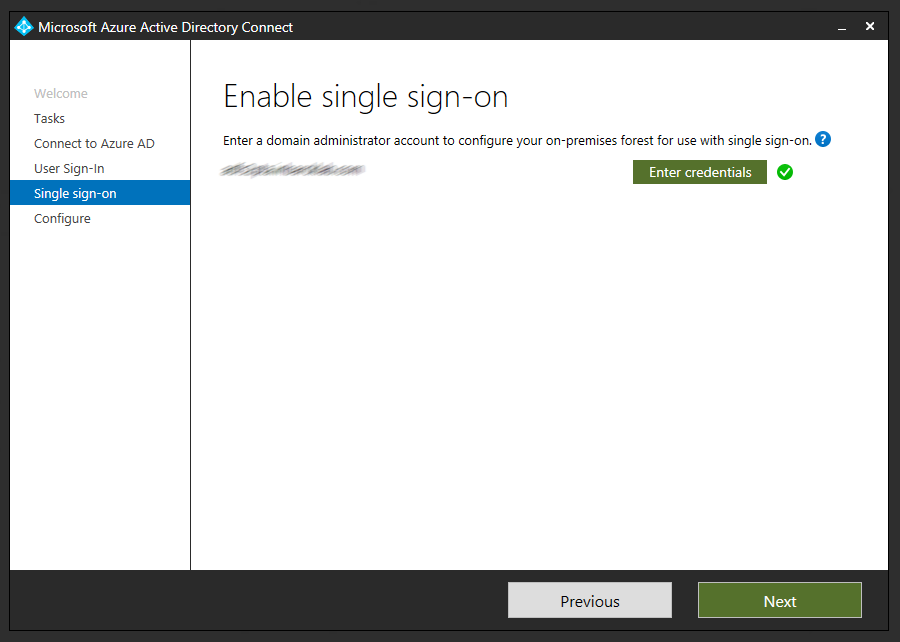


In **Enable Single Sign-on** screen, enter the credentials of Domain Administrator account, then click **Next**.

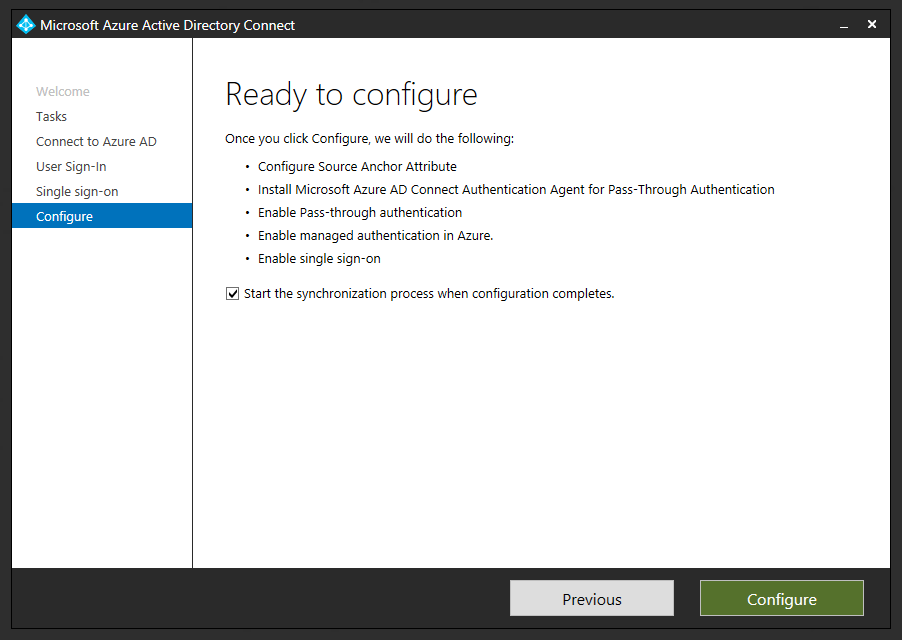
Note: Domain Administrator credentials are required for enabling Seamless Single Sign-on as the process performs the following actions which require these elevated permissions.

1. A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
2. The computer account's Kerberos decryption key is shared securely with Azure AD.
3. In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that are used during Azure AD sign-in.

The domain administrator credentials are not stored in Azure AD Connect or in Azure AD. They're used only to enable the feature and then discarded after successful completion.



In the **Ready to Configure** screen, make sure “Start Synchronization process when configuration completes” checkbox is selected. Then click **Configure.**



### Convert users

Once the domains have been converted to Managed by AAD Connect for you, all the users must now be converted in a separate step. This process makes sure all Azure Active Directory sub-systems are updated to reflect the new authentication settings and ***must not be skipped.***

The user conversion process can iterate through two users per second on average, but PowerShell throttling and other factors may ultimately slow this down, so this must be planned accordingly, and an appropriate [maintenance window](#_Maintenance_window) set.

To convert all users in the tenant run the following command:

Get-MsolUser -All | Convert-MsolFederatedUser

To convert all users of a specific domain the following commands can be used:

$users = Get-MsolUser -All | Select UserPrincipalName | Where-Object {$\_.UserPrincipalName -like "\*@domain.com"}

$users | Export-Csv c:\temp\usersToConvert.csv -NoTypeInformation

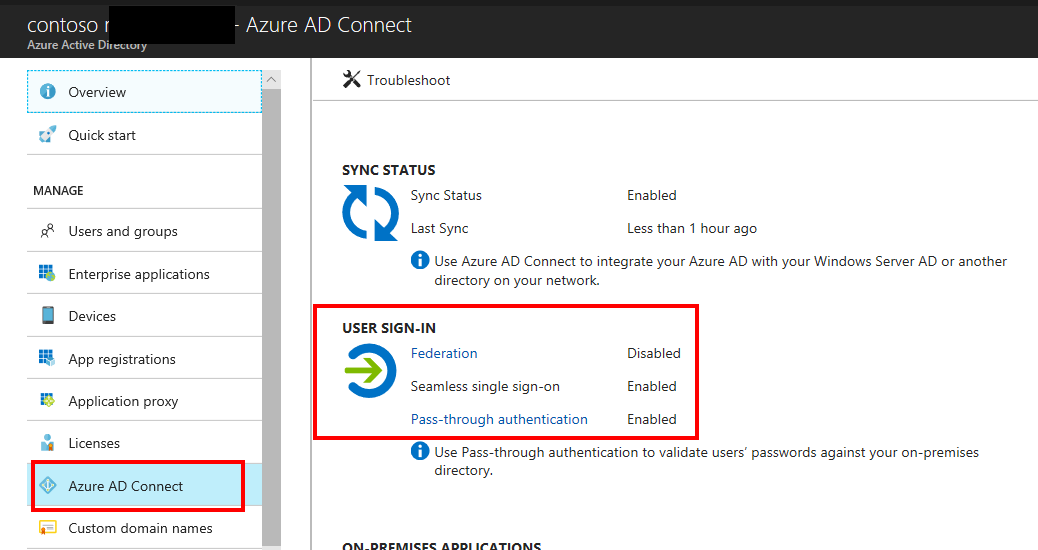
**Note:** to speed up the process, the usersToConvert.csv file can be split in different files, then multiple PowerShell sessions can be opened and run in parallel. We recommend doing this for domains with more than 10,000 users.

To convert the users run:

$users = Import-Csv C:\Temp\usersToConvert.csv

$users | foreach {Convert-MsolFederatedUser -UserPrincipalName $\_.UserPrincipalName}

Once all domains and users have been converted to Managed, you can go back to the Azure AD Connect page in the Azure AD portal and verify that **Federation** is **Disabled** while **Seamless Single Sign on** and **Pass-thought authentication** are **Enabled.**



## Complete the process

Once you have validated that both Pass-through Authentication and Seamless Single Sign both show as enabled in the portal you can proceed straight to the [Next Steps and Testing](#_Next_Steps_and) section of this document where you will be guided through installing more Pass-through Authentication agents, and validating that both Pass-through Authentication and Seamless SSO are working successfully.

***Note:*** As you have chosen and successfully completed “Option 1” it is important that you skip past the next section **“Option 2 - Switch from Federation to PTA using Azure AD Connect and PowerShell”** as the steps in that section do not apply.

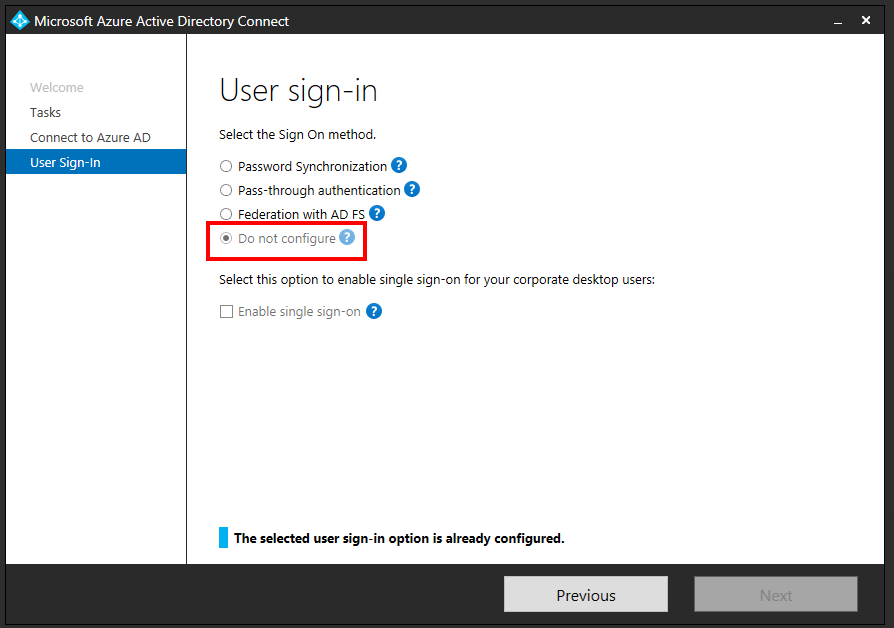
## Option 2 - Switch from Federation to PTA using Azure AD Connect and PowerShell

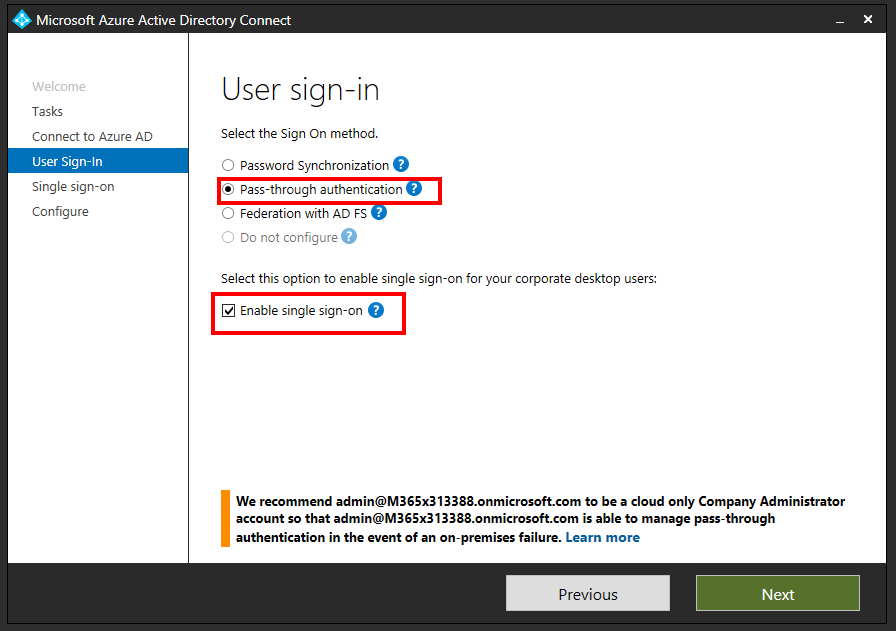
Since Federation was not initially configured using Azure AD Connect, enabling Pass-Through Authentication will not switch Federated domains to Managed. This step will need to be performed manually using PowerShell.

### Change User Sign-in method in Azure AD Connect

In Azure AD Connect click on **Previous** to go back to the **Additional Tasks** screen. Click on **Change User Sign in** and then click **Next**. In the **Connect to Azure AD** screen provide username and password of a Global Administrator.

In the **User Sign-in** Screen, **Select the Sign in method** should be set to **Do Not configure**. Change the radio button to **Pass-through authentication.** In addition, click on the checkbox next to **Enable single sign-on** then, click **Next.**



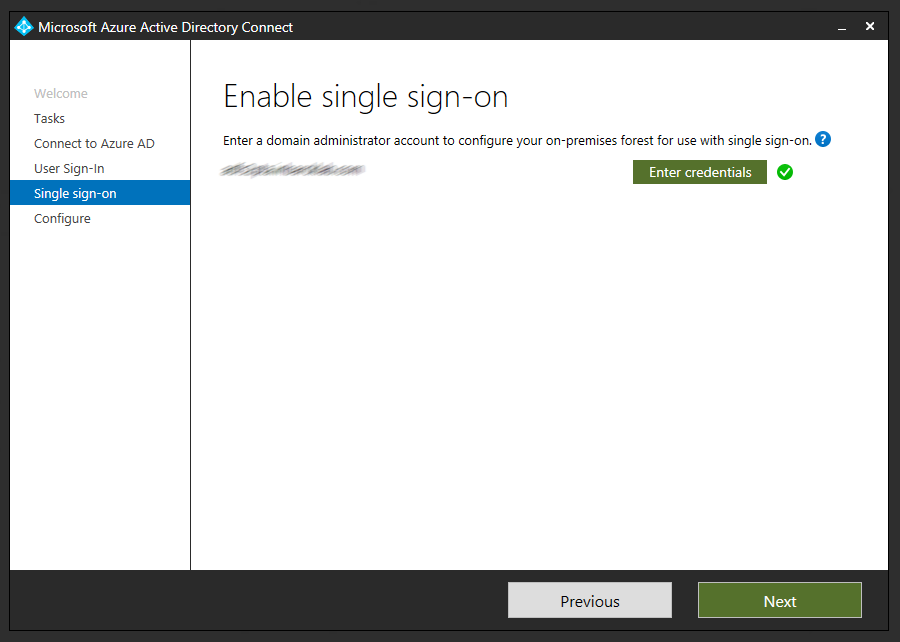


In **Enable Single Sign-on** screen, enter the credentials of Domain Administrator account, then click **Next**.

Note: Domain Administrator credentials are required for enabling Seamless Single Sign-on as the process performs the following actions which require these elevated permissions.

1. A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
2. The computer account's Kerberos decryption key is shared securely with Azure AD.
3. In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that are used during Azure AD sign-in.

The domain administrator credentials are not stored in Azure AD Connect or in Azure AD. They're used only to enable the feature and then discarded after successful completion.

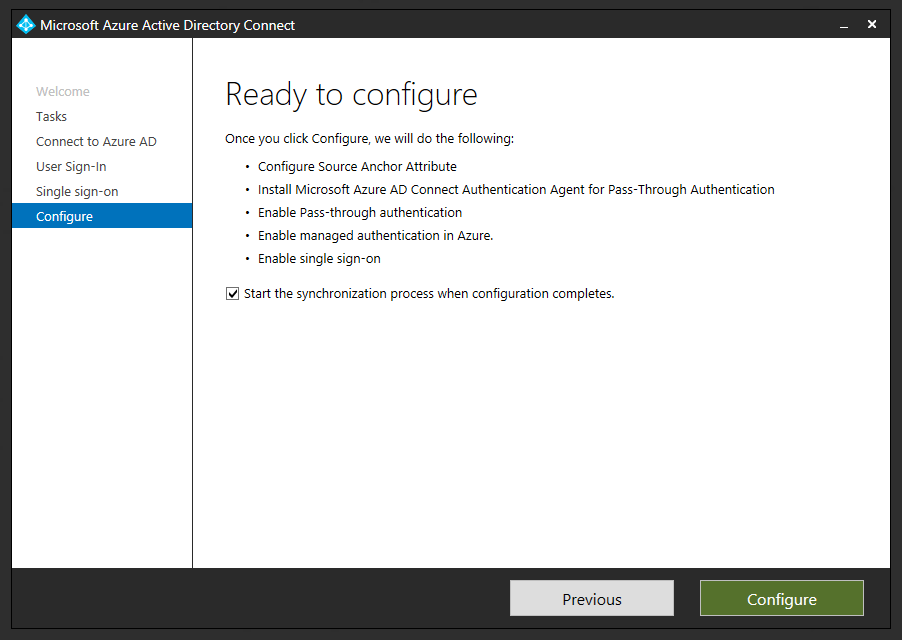


In the **Ready to Configure** screen, make sure “Start Synchronization process when configuration completes” checkbox is selected. Then click **Configure.**

When clicking Configure, the following steps are performed:

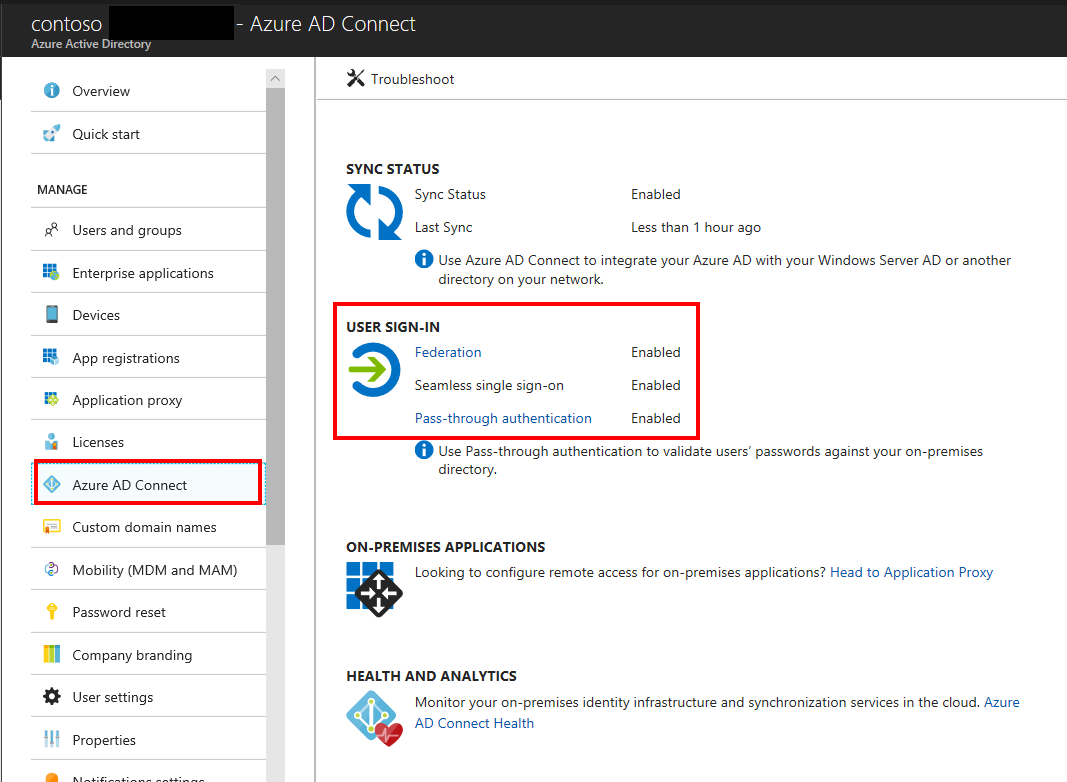
* The first Pass-Through Authentication Agent is installed
* The Pass-Through feature is enabled
* Seamless Single Sign-On is enabled.

Note that none of these changes will impact your users’ sign-in experience. To complete the configuration, your domains need to be converted from Federated to Managed as described later in this document.

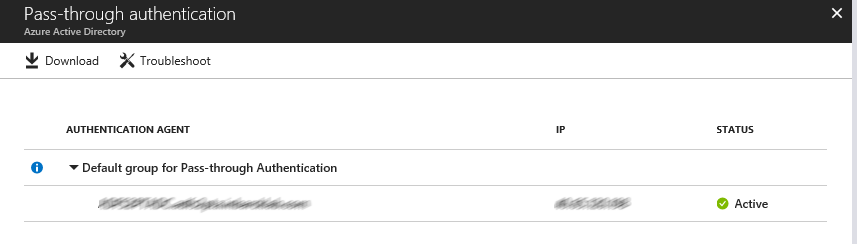


### Verify configuration settings

When Azure AD Connect finished the configuration changes, it is time to check these settings on the Azure AD side. Login to the Azure AD portal (<https://aad.portal.azure.com>) with a **Global Administrator** account. Click on **Azure Active Directory** blade from the left navigation and then click on **Azure AD Connect**. Under **User Sign-in** you should see that **federation**, **Seamless single Sign on** and **Pass-thought authentication** are all **Enabled.**



Click on **Pass-Through authentication** to check the health status of the Authentication Agent.



If the Authentication Agent is not active, follow troubleshooting steps on the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-troubleshoot-pass-through-authentication>

### Convert Domains from Federated to Managed

At this point, Federation is still enabled and operational for your domains. To continue with the deployment, each domain needs to be converted from Federated to Managed so Pass-Through Authentication starts serving authentication requests for the domain.

Not all domains need the be converted at the same time, you might choose to start with a test domain on your production tenant or the domain with the least number of users.

The conversion is performed using the Azure AD PowerShell Module and is a two-step process. First the domain must be converted to Managed authentication, then each user must be updated to reflect this change.

Open **PowerShell** and login to Azure AD using a **Global Administrator**.

Connect-MsolService

To update the domain authentication run:

Set-MsolDomainAuthentication -Authentication Managed -DomainName <domainname>



### Convert users

Once the domain has been converted to Managed, all the users with a matching User Principal Name must now be converted in a separate step. This process makes sure all Azure Active Directory sub-systems are updated to reflect the new authentication settings and should not be skipped.

The user conversion process can iterate through two users per second on average, but PowerShell throttling and other factors may ultimately slow this down, so this must be planned accordingly, and an appropriate [maintenance window](#_Maintenance_window) set.

To convert all users of a specific domain the following commands can be used:

$users = Get-MsolUser -All | Select UserPrincipalName | Where-Object {$\_.UserPrincipalName -like "\*@domain.com"}

$users | Export-Csv c:\temp\usersToConvert.csv -NoTypeInformation

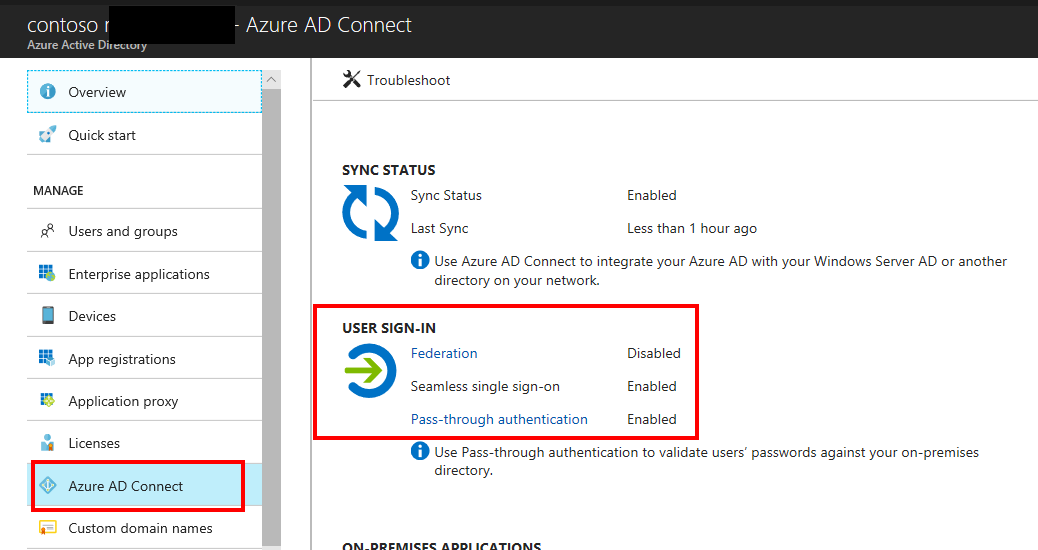
Note: to speed up the process, the usersToConvert.csv file can be split in different files, then multiple PowerShell sessions can be opened and run in parallel. We recommend doing this for domains with more than 10,000 users.

To convert the users run:

$users = Import-Csv C:\Temp\usersToConvert.csv

$users | foreach {Convert-MsolFederatedUser -UserPrincipalName $\_.UserPrincipalName}

Once all domains have been converted to Managed, you can go back to the Azure AD Connect page in the Azure AD portal and verify that **Federation** is **Disabled** while **Seamless Single Sign on** and **Pass-thought authentication** are **Enabled.**

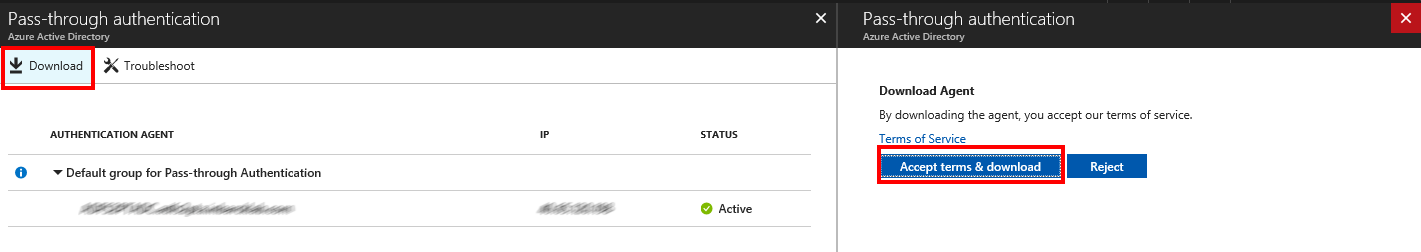


At this point, you are ready to continue the deployment with Next Steps and Testing.

## Next Steps and Testing

### Deploy Additional Authentication Agents

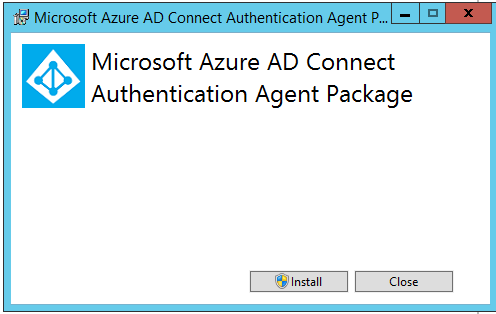
From the **Pass-through authentication** page, click on the **Download** button. From the **Download Agent** screen, click on **Accept terms and download.**

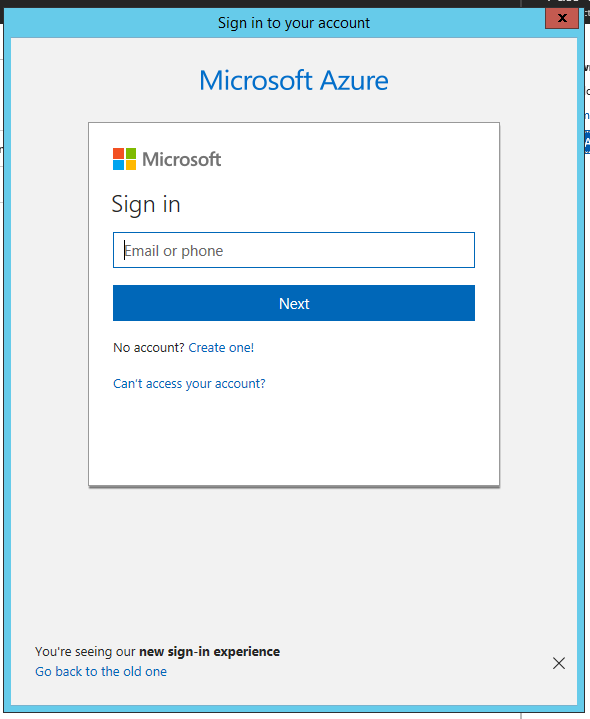


The download of additional authentication agents will begin. Install the secondary Authentication Agent on a domain joined server located close to a DC.

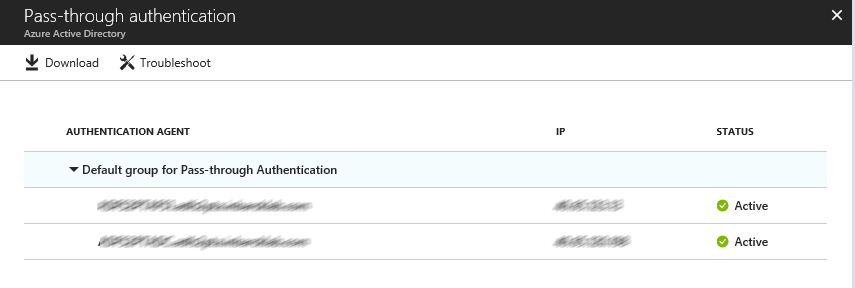
***NOTE:*** the first agent is always installed on the Azure AD Connect server itself as part of the configuration changes made in the User Sign In section of the Azure AD Connect tool. Any additional Authentication Agents should be installed on a separate server. It is recommended to have between 2-3 additional Authentication Agents available.

Run the Authentication Agent installation. During the installation you will need to provide credentials of a **Global Administrator** account.





Once the Authentication Agent is installed you can go back to the Pass-through Authentication Agent health page to check the status of the additional agents.



### Removal of the Relying Party Trust

Once you have validated that all users and Exchange ActiveSync clients are successfully authenticating via Azure AD and no longer being redirected to AD FS (which may take up to 12 hours) it can be considered safe to remove the Office 365 relying party trust.

If AD FS is not being used for other purposes (other Relying Party Trusts have been configured), it is safe to decommission ADFS now.

### Rollback

If a major issue is found and cannot be resolved quickly, you might decide to roll back the solution back to Federation.

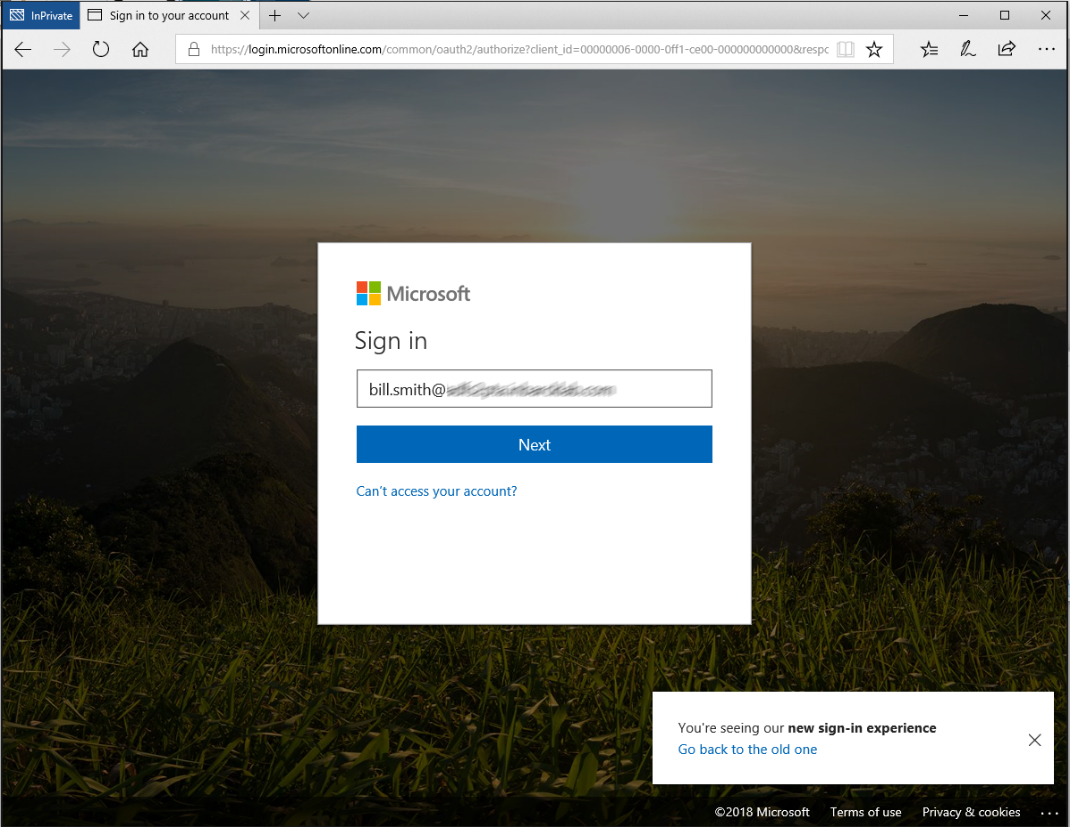
Consult your Federation design and deployment documentation for your particular deployment details. The process should involve:

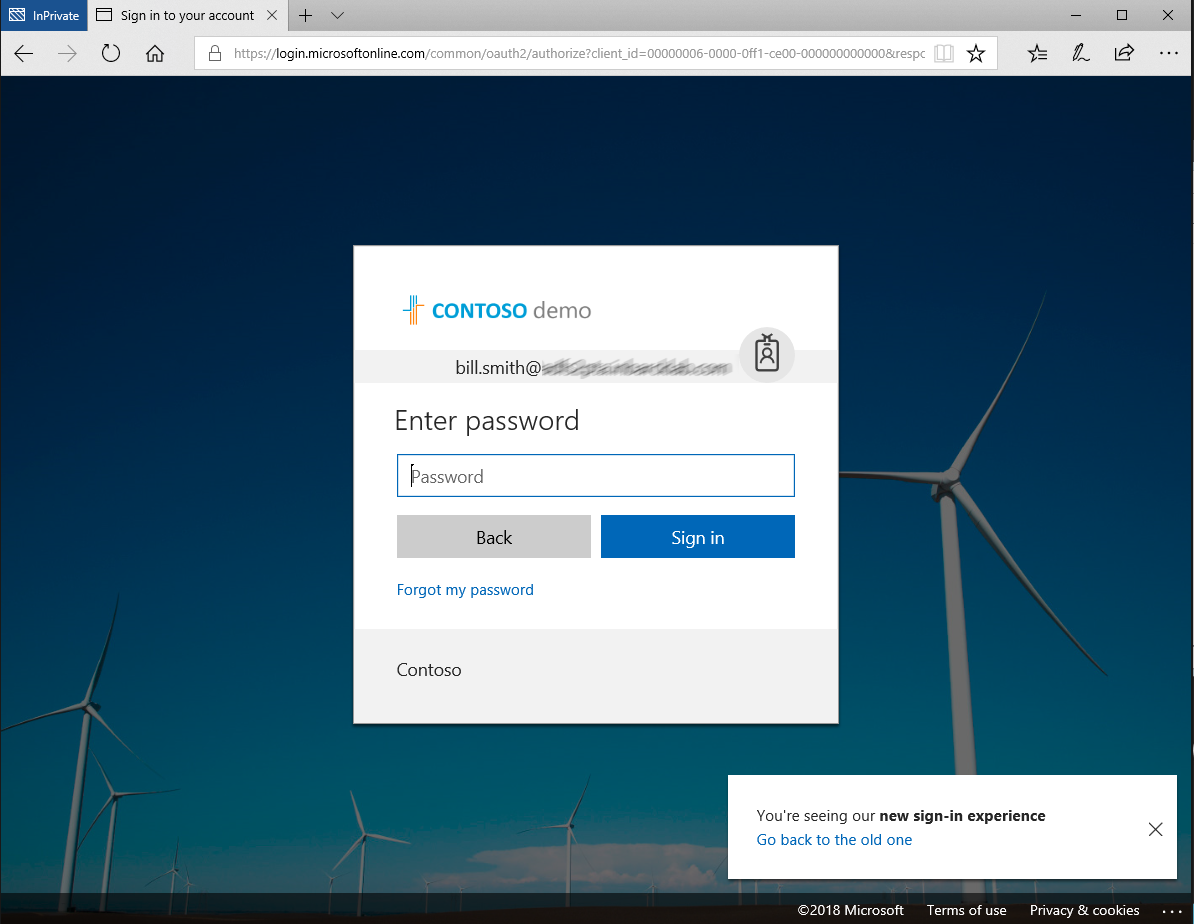
* Convert Managed domains to federated using Convert-MSOLDomainToFederated
* If required, configuring additional claims rules.

### Test Pass-through Authentication

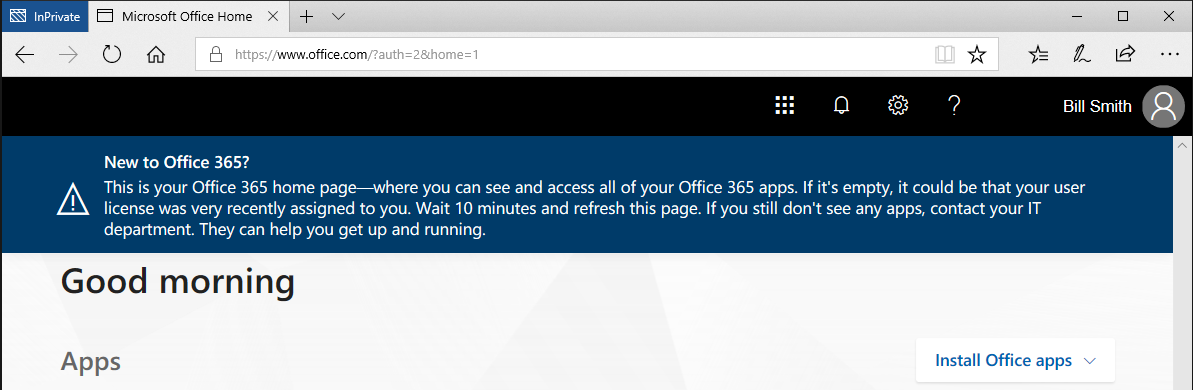
When your tenant was using federation, users were getting redirected from the Azure AD login page to your AD FS environment. Now that the tenant is configured to use Pass-through Authentication instead of federation, users will not get redirected to AD FS and instead will login directly through the Azure AD Login page.

Open Edge in InPrivate mode and go to the Office 365 login page (<http://portal.office.com>). Type the **UPN** of your user and click **Next.** Make sure to type UPN of a hybrid user that was synced from your on-premises Active Directory and who was previously federated. The user will see the screen to type in their username and password.





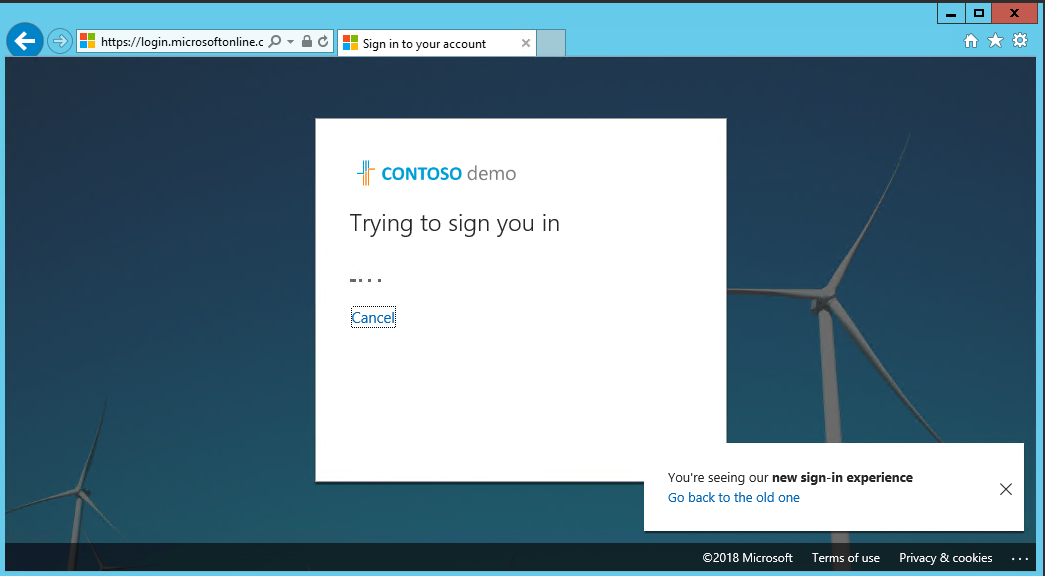
Once you type the password, you should get redirected to the Office 365 portal.



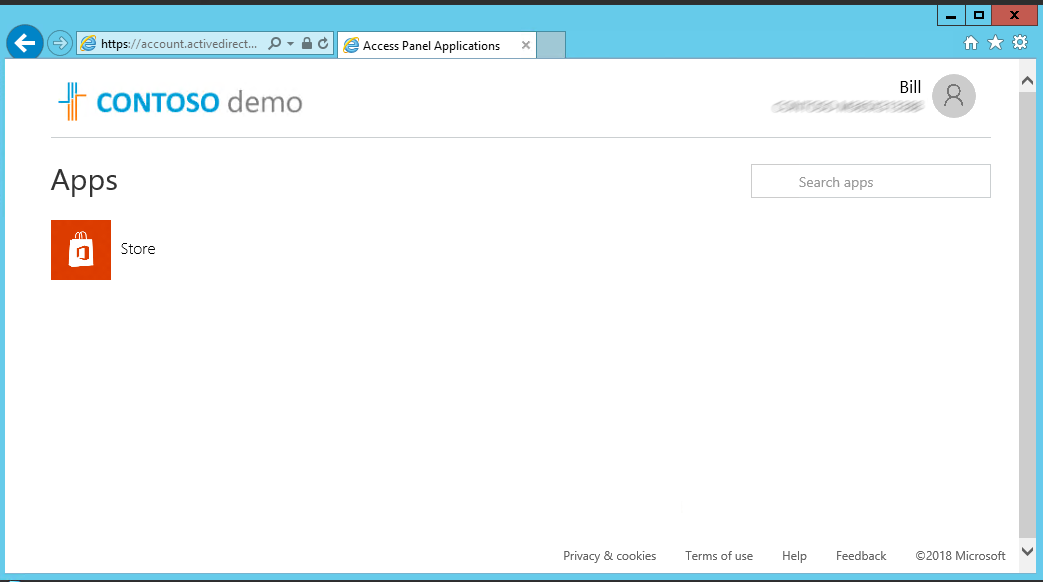
### Test Seamless single sign on

Login to a domain joined machine that is connected to the corporate network. Open **Internet Explorer** or **Chrome** and go to one of the following URLs:   
  
<https://myapps.microsoft.com/contoso.com> <https://myapps.microsoft.com/contoso.onmicrosoft.com> (replace Contoso with your domain).

The user will be briefly redirected to the Azure AD login page and see the message “Trying to sign you in” and should not be prompted for either a username or a password.



Then, the user will get redirected and signed into the Access Panel successfully:



NOTE: Seamless Single Sign-On works on Office 365 services that supports domain hint (for example, myapps.microsoft.com/contoso.com). The Office 365 portal (portal.office.com) currently doesn’t support domain hint and therefore it is expected that users will need to type their UPN. Once a UPN is entered, Seamless single sign on can retrieve the Kerberos ticket on behalf of the user and log them in without typing a password.

* **Microsoft recommends** deploying [Azure AD Hybrid Join on Windows 10](https://docs.microsoft.com/en-us/azure/active-directory/device-management-introduction#hybrid-azure-ad-joined-devices) for an improved single sign-on experience.

# Operations

This section describes the recommended task to be performed regularly on Pass-Through Authentication and Seamless SSO deployments.

## Roll over the Seamless SSO Kerberos decryption

It is important to frequently roll over the Kerberos decryption key of the AZUREADSSOACC computer account (which represents Azure AD) created in your on-premises AD forest. We highly recommend that you roll over the Kerberos decryption key at least every 30 days.

Follow these steps on the on-premises server where you are running Azure AD Connect to initiate the rollover of the Kerberos decryption key.

[How can I roll over the Kerberos decryption key of the AZUREADSSOACC computer account](https://docs.microsoft.com/en-au/azure/active-directory/connect/active-directory-aadconnect-sso-faq#how-can-i-roll-over-the-kerberos-decryption-key-of-the-azureadssoacc-computer-account)?

## Monitoring and logging

The servers running the Authentication Agents should be monitored to maintain the solution availability. In addition to general server performance counters, the Authentication Agents expose performance objects that can be used to understand authentication statistics and errors.

Authentication Agents log operations to Windows event logs under “*Application and Service Logs\Microsoft\AzureAdConnect\AuthenticationAgent\Admin”*

Troubleshooting logs can be enabled if required.

For more information about monitoring and logging refer to the following document.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-troubleshoot-pass-through-authentication#collecting-pass-through-authentication-agent-logs>