

Azure Active Directory **Migration from ADFS to** **Pass-Though Authentication** Deployment Plan

**How to use this guide**

This step-by-step guide walks through the implementation of Pass Through

Authentication in a four-step process. The links below take you to each of those steps.

**3**

**[Implement](#_Implementing_Your_Solution)**

[Your solution](#_Implementing_Your_Solution)



**1**

**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_your_Deployment)**

[Your project](#_Planning_your_Deployment)



**4**

**[Manage](#_Manage_your_solution)**

[Your implementation](#_Manage_your_solution)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

These are general recommendations, and you should only implement if they apply to your specific enterprise needs.

Table of Contents

Contents

[Introduction 4](#_Toc517175267)

[Purpose of document 4](#_Toc517175268)

[What is Managed Authentication? 4](#_Toc517175269)

[What is Managed Authentication with Pass-Through Authentication? 4](#_Toc517175270)

[What is Seamless Single Sign-on? 4](#_Toc517175271)

[Current state of Authentication 4](#_Toc517175272)

[Goals for Pass-through Authentication with Seamless Single Sign-on 5](#_Toc517175273)

[Stakeholders and Sign-off 6](#_Toc517175274)

[Project Scope 7](#_Toc517175275)

[Prerequisites 7](#_Toc517175276)

[In scope 7](#_Toc517175277)

[Out of scope 7](#_Toc517175278)

[Unsupported Scenarios 8](#_Toc517175279)

[Planning your Deployment 9](#_Toc517175280)

[General Planning 9](#_Toc517175281)

[Environments and project stages 9](#_Toc517175282)

[Licensing Considerations 9](#_Toc517175283)

[Understanding Pass-through Authentication 9](#_Toc517175284)

[Planning for Pass-through Authentication 10](#_Toc517175285)

[Update Azure AD Connect 11](#_Toc517175286)

[Plan Authentication Agent Number and Placement 11](#_Toc517175287)

[Plan Migration Method 12](#_Toc517175288)

[Document Current Federation Settings 14](#_Toc517175289)

[Deployment Considerations and AD FS Usage 16](#_Toc517175290)

[Validate Your Current AD FS Usage 16](#_Toc517175291)

[Considerations for Common AD FS Customizations 16](#_Toc517175292)

[Planning for Smart Lockout 17](#_Toc517175293)

[Plan for Modern Authentication 18](#_Toc517175294)

[Plan Seamless SSO 18](#_Toc517175295)

[Plan Logging and Auditing 19](#_Toc517175296)

[Planning Deployment and Support 20](#_Toc517175297)

[Plan the Maintenance Window 20](#_Toc517175298)

[Plan for Rollback 20](#_Toc517175299)

[Plan Change Communications 20](#_Toc517175300)

[Test Planning 22](#_Toc517175301)

[Implementing Your Solution 22](#_Toc517175302)

[Solution Components 22](#_Toc517175303)

[Step 1 – Prepare for Seamless SSO 22](#_Toc517175304)

[Step 2 – Change sign-in method to Pass-Through Authentication and enable Seamless SSO 23](#_Toc517175305)

[Option A: Configuring Pass-through Authentication by using Azure AD Connect 23](#_Toc517175306)

[Option B - Switch from Federation to PTA using Azure AD Connect and PowerShell 27](#_Toc517175307)

[Testing and Next Steps 33](#_Toc517175308)

[Test Pass-through Authentication 33](#_Toc517175309)

[Test Seamless single sign on 35](#_Toc517175310)

[Removal of the Relying Party Trust 36](#_Toc517175311)

[Rollback 36](#_Toc517175312)

[Support Planning 36](#_Toc517175313)

[Manage your solution 36](#_Toc517175314)

[Roll over the Seamless SSO Kerberos decryption 36](#_Toc517175315)

[Monitoring and logging 37](#_Toc517175316)

# 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?

Managed Authentication describes a system in which authentication is driven by Azure Active Directory, with a minimal on-premises footprint, as opposed to Federated authentication, where an on-premises Identity Provider manages authentication. There are two options for a Managed Authentication Model: This document addresses Managed Authentication with Pass-Through Authentication (PTA). Managed Authentication with Password Hash Synchronization (PHS) is addressed in a separate deployment guide.

While PHS is not addressed in this document, it can be combined with PTA to obtain specific benefits.

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

## What is Managed 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.

For a deeper technical and security explanation, 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.

## What is Seamless Single Sign-on?

With Azure Active Directory Single Sign-On (Azure AD Seamless SSO), once users log on to their domain joined computer connected to your corporate network, they are seamlessly authenticated to Azure AD and able to access cloud-based applications without typing their passwords, and typically do not need to enter their user names. This feature provides your users easy access to your cloud-based applications without the need for any additional on-premises components.

## Current state of Authentication

Replacing our current federated authentication infrastructure and migrating to Microsoft Azure Active Directory to manage our authentication with PTA and Seamless SSO will …

<<this is an optional section in which you can detail your current state to help your stakeholders and decision makers understand the benefits specific to your enterprise of moving to PTA. >>

<< Insert your summary text here. Eg: By moving to PTA, we will save XX dollars in Federation running costs.>>

## Goals for Pass-through Authentication with Seamless Single Sign-on

Moving from federation to PTA and Seamless Single Sign-on will benefit our business in the following ways:

|  |  |
| --- | --- |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Within_Your_Reach.png | **MANAGE COST**  Enabling PTA with Seamless SSO removes the requirement to maintain an on-premises highly available and redundant AD FS farm, including the servers and internal/external load balancers. It also removes certificate management administration and overhead costs, while simplifying monitoring, administration, and ongoing maintenance costs of the AD FS Solution. |
| C:\Users\mitchellg\Desktop\Simple_Licensing.png | **REDUCE COMPLEXITY AND RISK**  Moving to PTA with Seamless SSO enables us to take advantage of user authentication at cloud scale. Using Azure AD Conditional Access policies reduces the need for complex custom claims issuance rules in AD FS, simplifying access and authorization control to cloud services. Risk is reduced by reducing susceptibility to authentication outages caused by configuration, certificate expiration and rollover, performance issues, and other on-premises dependencies required by AD FS. |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Confidentiality.png | **FLEXIBILITY AND SECURITY**  Moving to PTA and Seamless SSO enables enterprises to access the security and flexibility that a cloud platform provides. With these solutions, there is no need to open inbound ports for user authentication requests, a common attack vector. Azure AD can protect user accounts from brute force, password spray, and other malicious attacks with its unique Smart Lockout and Identity Protection services. |
| Magnifying glass | **ROBUST AUDITING AND USAGE TRACKING**  The auditing and usage tracking capabilities in Azure AD make it easy to gain 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. |
|  |  |

## Stakeholders and Sign-off

The following roles will be involved in delivering this project. To see a full list of responsibilities and delivery items, see [Implementation Steps and Stakeholders](#_Implementation_Steps_and).

* Action Required:
  + SO = Sign-off on this project
  + R = Review this project and provide input
  + I = Informed of this project

|  |  |  |
| --- | --- | --- |
| Name | Area | Action |
| Enter name and email | IT Support Manager  A representative from the IT support organization who can provide input on the supportability of this change from a helpdesk perspective. | SO |
| Enter name and email | Identity Architect or Azure Global Administrator  A representative from the identity management team in charge of defining how this change is aligned with the core identity management infrastructure in the customer’s organization. | SO |
| Enter name and email | Business Owner  A representative colleague who can provide input on the user experience and usefulness of this change from an end-user’s perspective and owns the overall business aspect of the application, which may include managing access. | SO/I |

# Project Scope

## Prerequisites

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

* The latest build of AAD Connect is installed. For more information see the [Update Azure AD Connect](#_Update_Azure_AD) section.
* Port 80/443 outbound is allowed from the AAD Connect server and any other servers where you plan to install the PTA agent.
* 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).
* The servers where you will install the PTA agents on are running Windows Server 2012R2 or Windows Server 2016.
* An Azure Global Administrator account is available to configure PTA in your tenant and migrate from federated to managed.
* A Domain Administrator account is available to configure Seamless SSO in the on-premises Active Directory.
* 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 enabling Modern Authentication.
* Modern Authentication is enabled for any Office 2013 clients.

## 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
* 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
* Configuring Hybrid Azure AD join

### Unsupported Scenarios

* Access to calendar sharing and free/busy information in Exchange hybrid environments in Office 2010.
* The Apple Device Enrollment Program (Apple DEP) using the iOS Setup Assistant does not support modern authentication. This will fail to enroll Apple DEP devices into Intune for managed domains using Pass-through Authentication. Consider using the [Company Portal](https://docs.microsoft.com/en-us/intune/device-enrollment-program-enroll-ios) app as an alternative.

For an updated list of unsupported scenarios refer to this article:

[Azure Active Directory Pass-through Authentication: Current limitations](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-current-limitations)

# Planning your Deployment

## General Planning

### Environments and project stages

Project stages are dependent on the environments that you have available. If you have a non-production Azure tenant, you can complete a proof of concept (POC) outside of your production environment if desired.

In the table below, document the Azure AD and AD environments and stages of your project.

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Deployment | / |

### Licensing Considerations

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 require a license assigned to be compliant, or to gain access to the feature.

The following table describes common Azure AD scenarios and recommended security features. For a full list of license options and features, see [here](https://azure.microsoft.com/en-us/pricing/details/active-directory/).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Azure AD License Type | | |
|  | **FREE/BASIC** | **PREMIUM P1** | **PREMIUM P2** |
| Password Hash Sync | Available | | |
| Pass-through Authentication | Available | | |
| Seamless SSO | Available | | |
| Conditional Access | NOT Available | Requires minimum of P1 | |
| Multi-factor Authentication | NOT Available | Requires minimum of P1 | |
| Group-based membership | NOT Available | Requires minimum of P1 | |
| Identity Protection |  | Requires minimum of P2 | |
| Smart Lockout | Available | | |

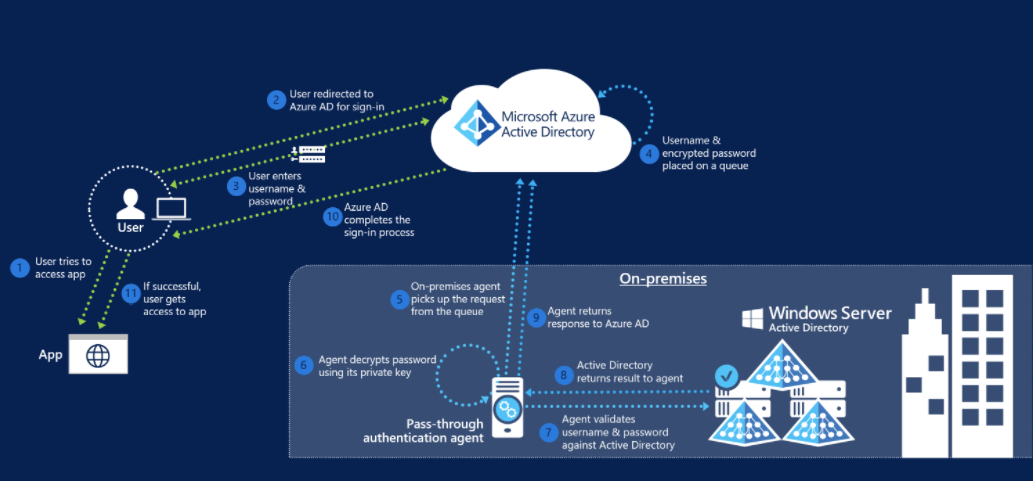
**Enterprise Mobility and Security (EMS) subscriptions:**

If you have an existing Enterprise Agreement or Server and Cloud Enrollment, you may already have Azure Premium. Check the details of your agreement.

* EMS E3 includes P1
* EMS E5 includes P2

## Understanding Pass-through Authentication

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 credentials 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 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 on-premises 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.

## Planning for Pass-through Authentication

### Update Azure AD Connect

Azure AD Connect is the tool to integrate your on-premises directories with Azure AD. In addition to directory synchronization, Azure AD Connect provides a wizard-driven experience for configuring your Azure AD authentication settings and other features.

Microsoft **strongly recommends** updating Azure AD Connect to the latest version as part of this implementation project. The deployment steps and captured screens on this deployment guide were developed using the latest available version of Azure AD Connect.

As a minimum to successfully perform the steps on this document, you should have Azure AD connect **1.1.819.0**. This version contains significative changes to the way sign-in conversion is performed and reduces the overall time to migrate from Federation to Cloud Authentication from potentially hours to minutes.

**Important!** Outdated documentation, tools and blogs indicate that user conversion is a required step when converting domains from Federated to Managed. Note that **converting users is not required anymore** and Microsoft is working on updating documentation and tools to reflect this.

Download the latest version of Azure AD Connect here <https://www.microsoft.com/en-us/download/details.aspx?id=47594>.

To understand how to update Azure AD Connect to the latest version, see the following article.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-upgrade-previous-version>

### Plan Authentication Agent Number and Placement

Pass-through Authentication is accomplished by deploying light-weight agents on the Azure AD Connect Server, and on your on-premises Windows Servers. Install the agents as close as possible to your Active Directory Domain Controllers to reduce latency.

For most customers two or three authentication agents are sufficient for high availability and capacity, and a tenant can have no more than 12 agents registered. The first agent is always installed on the AAD Connect server itself.

For more information on network traffic estimations and performance guidance refer to the [document](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-current-limitations) on limitations.

Once you have determined the number of agents, record the servers on which you will install the agents in the following table.

|  |  |
| --- | --- |
| Agent number | Server name |
| 1 | (must be AAD Connect Server) |
| 2 |  |
| 3 |  |
| 4 |  |

If performance is a concern for your Azure AD 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. Record your plan below.

|  |  |
| --- | --- |
| Agent Service on Azure AD Connect Server | State |
| Microsoft Azure AD Connect Authentication Agent | (Enabled or Disabled) |
| Microsoft Azure AD Connect Agent Updater | (Enabled or Disabled) |

**Important!** The servers where the Authentication Agents are deployed should be considered a Tier 0 system according to the [Active Directory administrative tier model](https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material).

### Plan Migration Method

There are two methods to migrate from federated authentication to PTA and Seamless SSO. The method you use will depend on how your AD FS was originally configured.

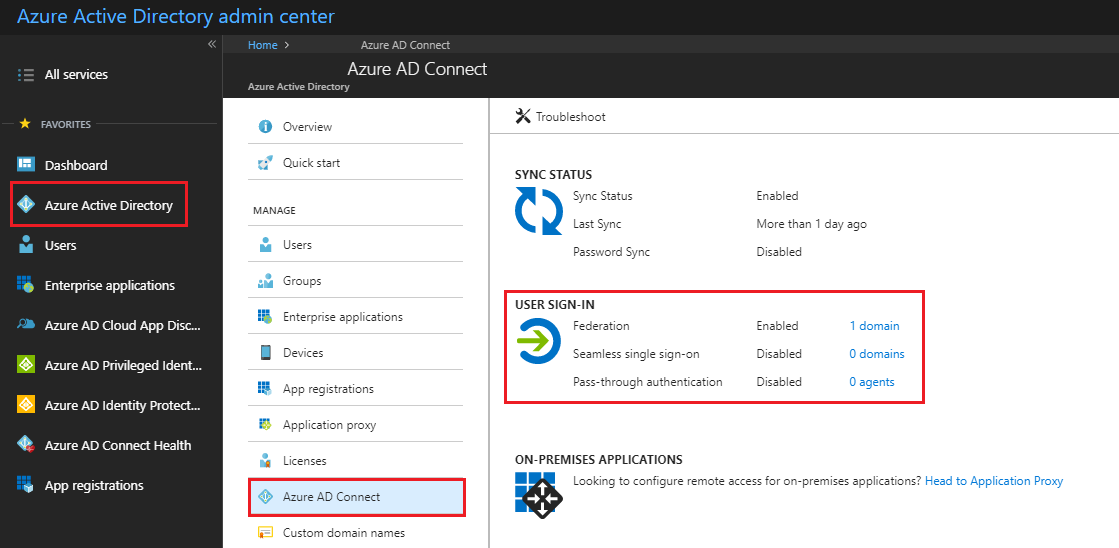
1. **Using Azure AD Connect**. If AD FS was originally configured using Azure AD Connect, then the change to pass-through Authentication ***must*** be performed through the Azure AD Connect wizard.   
   When using Azure AD Connect, it runs the Set-MsolDomainAuthentication cmdlet for you automatically when you change the user sign-in method, and hence you have no control over it un-federating ***all of*** the verified federated ***domains*** in your Azure AD tenant.  
     
   ***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.
2. **Using Azure AD Connect with PowerShell.** This method may be used only when AD FS was *not* originally configured with Azure AD Connect.You still need to change the user sign-in method via the Azure AD Connect wizard, but the core difference is that it will not automatically run the Set-MsolDomainAuthentication cmdlet for you as it has no awareness of your AD FS farm, and hence you have full control over which domains are converted and in which order.

To understand what method you should use, perform the steps on the following section.

#### Verify Current User Sign-in settings

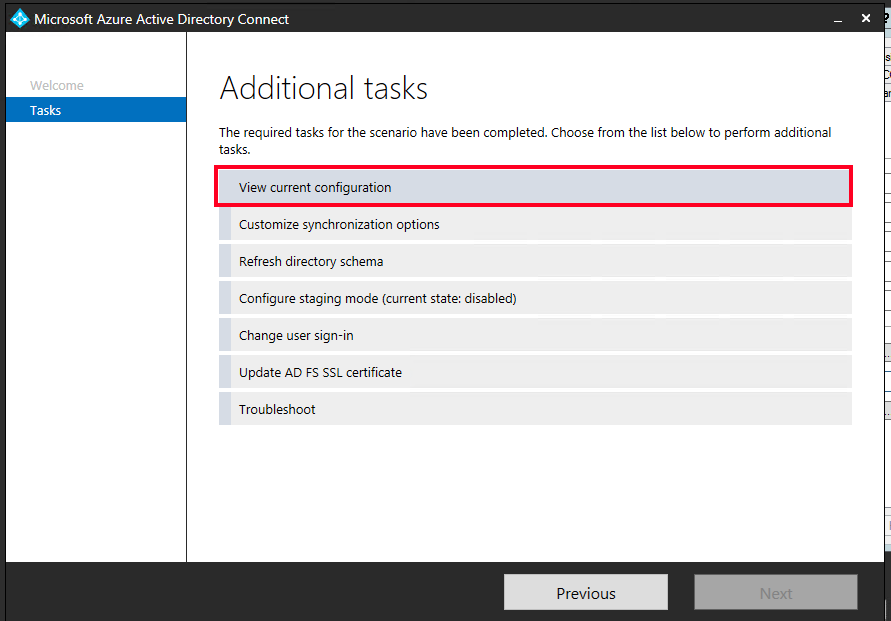
Verify your current user sign-in settings by logging into the Azure AD portal <https://aad.portal.azure.com> with a **Global Administrator** account.

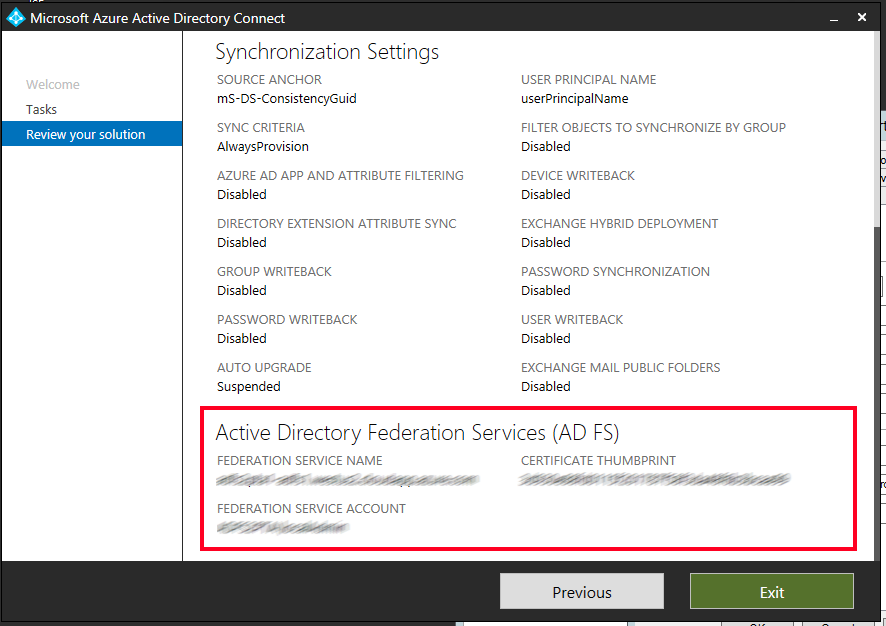
In the **User Sign In** section, verify that **Federation** is **Enabled** and that **Seamless Single Sign-on** and **Pass-through authentication** are **Disabled.**

****

#### Verify How Federation was Configured

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



1. In the **Review Your Solution** screen scroll down to **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: Configuring Pass-through Authentication by using Azure AD Connect](#_Option_1:_Configuring)”.
2. 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_-).

### Document Current Federation Settings

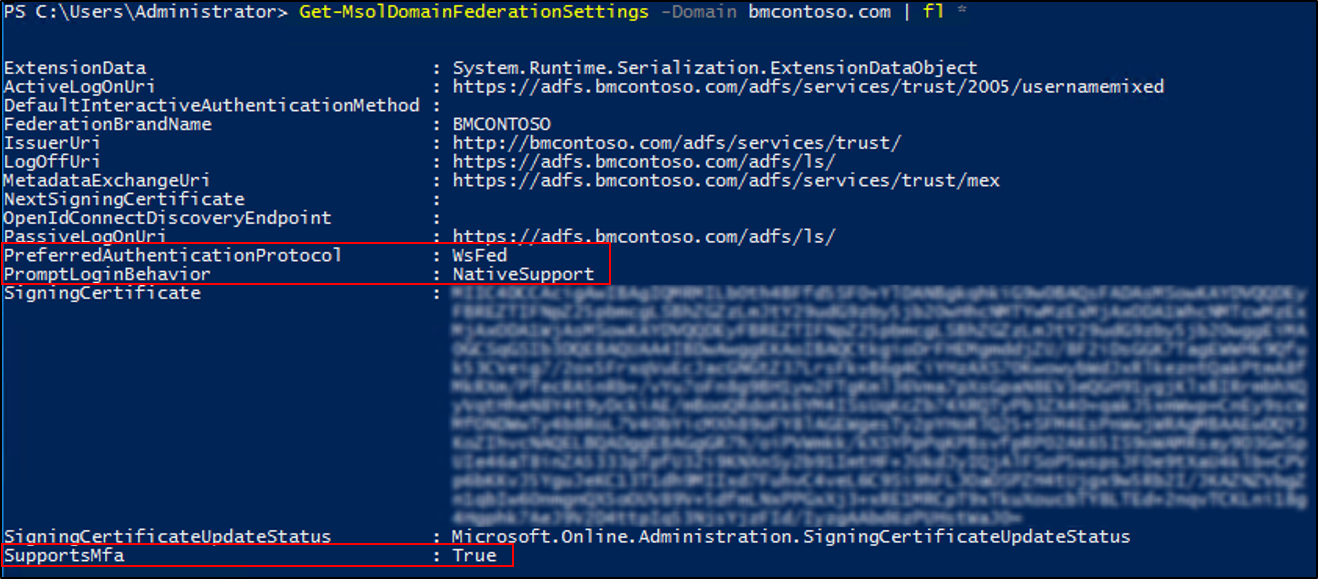
You can find the current federation setting by running the Get-MsolDomainFederationSettings cmdlet.

The command is:

Get-MsolDomainFederationSettings -DomainName YourDomain.extention | fl \*

For example:

Get-MsolDomainFederationSettings -DomainName Contoso.com | fl \*



Validate any settings that might have been customized to your Federation design and deployment documentation, specifically the following, in the event that you need to roll back:

|  |  |
| --- | --- |
| Settings | Values |
| PreferredAuthenticationProtocol |  |
| SupportsMfa |  |
| PromptLoginBehavior |  |

More information on what these settings do can be found below.

[Active Directory Federation Services prompt=login parameter support](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-prompt-login)  
[Set-MsolDomainAuthentication](https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoldomainauthentication?view=azureadps-1.0)

**Note**: If the SupportsMfa value is currently set to “True” then this means you are using an On-Premises MFA solution to inject a 2nd factor challenge into the user authentication flow. This will no longer work for Azure AD authentication scenarios, and instead you will have to leverage the Azure MFA (cloud-based) service to perform the same function. Carefully evaluate your MFA requirements before moving forward and make sure you understand how to leverage Azure MFA, the licensing implications, and the end user registration process before converting your domains.

#### Backup Federation Settings

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 Microsoft [AD FS Rapid Restore Tool](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-quick-start#in-your-on-premises-environmenthttps://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-rapid-restore-tool). This tool can be used to backup and restore AD FS, either to an existing farm, or a new farm.

If you choose not to use the AD FS Rapid Restore Tool, then at a minimum, you should export the "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"

## Deployment Considerations and AD FS Usage

### Validate Your 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:

| If | Then |
| --- | --- |
| You are going to retain AD FS for those other applications. | You will be using both 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. |
| AD FS is heavily customized and reliant on specific customization settings in the onload.js file that cannot be duplicated in Azure AD  (for example, you have changed the sign-in experience so that users only enter a SamAccountName format for their username as opposed to a UPN, or have a heavily branded the login experience) | You will need to verify that your current customization 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. |
| You are blocking legacy authentication clients via AD FS. | This is the only way to effectively 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 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. |
| You require 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. |
| You use Access Control Policies (AuthZ rules) today in AD FS to control access to Office 365. | 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). |

### Considerations for Common AD FS Customizations

#### Inside Corporate Network claim

The InsideCorporateNetwork claim is issued by AD FS if the user authenticating is inside the corporate network. This claim can then be passed on to Azure AD and used to bypass Multi-Factor authentication based on the users’ network location. See [Trusted IPs for Federated Users](https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-get-started-adfs-cloud#trusted-ips-for-federated-users) for information on how to determine if you have this currently enabled in AD FS.

The InsideCorporateNetwork claim won’t be available anymore once your domains are converted to Pass-Through Authentication. [Named Locations in Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-named-locations) can be used to replace this functionality.

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.

See [Active Directory Conditional Access Locations](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-locations) for more information on the Location condition in Conditional Access.

#### Hybrid Azure AD Joined Devices

Joining a device to Azure AD enables you to create conditional access rules that enforce devices meeting your access standards for security and compliance and allows users to sign-in to a device using an organizational work or school account instead of a personal account. Hybrid Azure AD Joined Devices enables you to join your AD domain-joined devices to Azure AD. Your federated environment may have been configured with this feature.

To ensure 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 synchronize Active Directory computer accounts for Windows 10 clients to Azure AD. For Windows 7 and Windows 8 computer accounts, Hybrid Join will use Seamless SSO to register the computer in Azure AD and you do not have to sync them as you do for Windows 10 devices. 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. [Download the .msi](https://www.microsoft.com/en-us/download/details.aspx?id=53554).

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

[How to configure hybrid Azure Active Directory joined devices](https://docs.microsoft.com/en-us/azure/active-directory/device-management-hybrid-azuread-joined-devices-setup)

#### Branding

Your organization may have [customized your ADFS sign-in pages](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-user-sign-in-customization) to display information more pertinent to the organization. If so, consider making similar [customizations to the Azure AD sign-in page](https://docs.microsoft.com/en-us/azure/active-directory/customize-branding).

While similar customizations are available, some visual changes should be expected. You may want to include expected changes in your communications to end users.

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

## Planning for 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 behavior 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 behavior, and user’s devices and browsers. The Smart Lockout settings can be adjusted via Graph API but require 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 [this 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. If you have an on-premises Group Policy object that locks accounts after fewer than 10 failed password attempts, an Azure AD P2 license is required for a single Global Administrator account so that they can edit Smart Lockout settings in Azure AD to tune it to your environment and prevent unintended lockouts resulting from pass-through authentication requests.

## Plan for Modern Authentication

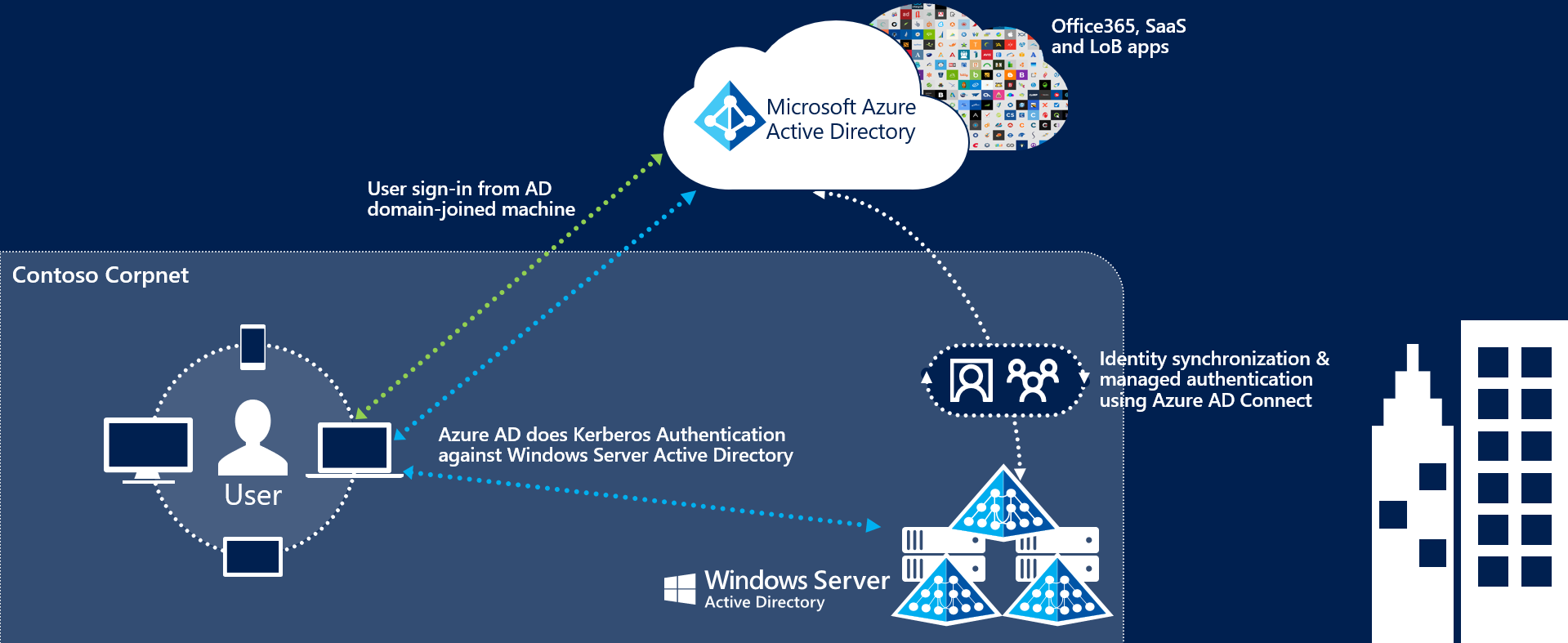
While pass-through authentication does support authenticating certain legacy clients (Exchange ActiveSync, Outlook 2010/2013 etc.) organizations are encouraged to switch to modern authentication, if possible. Modern authentication brings Active Directory Authentication Library (ADAL)-based sign-in to Office client apps across platforms. This enables sign-in features such as Multi-Factor Authentication (MFA), smart card and certificate-based authentication, and it removes the need for Outlook to use the basic authentication protocol. Modern authentication allows for Pass-through Authentication support. It also helps you secure your user accounts by using conditional access features. 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)

* **Microsoft Recommends** enabling Modern Authentication

## Plan Seamless SSO

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. 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.



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

* Enabling client devices to utilize Seamless SSO by modifying the users “Intranet Zone” settings through Active Directory Group Policies.
* Enable the Seamless SSO feature in AAD Connect which creates a special computer account in the On-Premises Active Directory called AZUREADSSOACC

Client devices can be enabled for Seamless SSO using a group policy. We recommend performing this step before enabling the Seamless SSO feature and converting your domains to Managed to minimize the time in which your users might be prompted for a username and password.

For more information on the changes required, refer to the section [Step 1 – Prepare for Seamless SSO](#_Step_1_–).

## Plan Logging and Auditing

Sign-ins and Auditing logs are available for 30 days in Azure AD. If security auditing within your corporation requires longer retention, the logs need to be exported and stored or ingested into a Security Information and Event Management (SIEM) solution.

In the table below, document the backup schedule, the system, and the responsible parties. You may not need separate auditing and reporting backups, but you should have a separate backup from which you can recover from an issue.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Frequency of download | Target system | Responsible party |
| Auditing backup |  |  |  |
| Reporting backup |  |  |  |
| Disaster recovery backup |  |  |  |

## Planning Deployment and Support

### Plan the Maintenance Window

While the domain conversion process itself is relatively quick, Azure AD and Exchange Online might still send some authentication requests to your AD FS servers for a period of up to 4 hours after domain conversion. During this 4-hour window and depending on various caches in the service, these authentications might not be accepted by Azure AD and users will receive an error.

* **Microsoft recommends:** don’t shut down your AD FS environment or remove the Office 365 relying party trust until you have verified all users are successfully authenticating using cloud authentication.

### Plan for Rollback

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

#### Rolling back

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.

In the following table, record your documentation and backup settings, and additional information.

|  |  |
| --- | --- |
| Resource | Location / Name |
| AD FS backup |  |
| AD FS Design and Deployment documentation |  |
|  |  |

### Plan Change Communications

An important part of planning deployment and support is ensuring that your end users are proactively informed about the changes and what they may experience or must do.

After both pass-through authentication and Seamless SSO are deployed, the end user sign-in experience will change when accessing Office 365 and other associated resources authenticated through Azure AD. Users external to the network 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.

There are multiple elements to planning your communication strategy. These include:

* Notifying users of upcoming and released functionality via
  + Email and other internal communication channels
  + Visuals such as posters
  + Executive live or other communications
* Determining who will customize and who will send the communications, and when.

Use the following table to plan your communications strategies. In the channels column, record the channels you will use for communications, including email, Yammer, Slack, intranet sites, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Communication | Channels | Person customizing content | Person communicating | Date of communication |
| Creation of end-user emails |  |  |  |  |
| Initial communication to all users for launch |  |  |  |  |
| Posters up for Launch |  |  |  |  |
| Exec. Comms. For launch |  |  |  |  |
| Maintenance window starting |  |  |  |  |
| Maintenance window complete |  |  |  |  |
| Post-launch follow-up communications |  |  |  |  |

### Test Planning

In this section, document how you will test during the pre-production phases of your roll-out, as well as post-launch. Testing should ensure that your business use cases are covered. You can then use this table to record results. We have added a few cases based on the sample business requirements in this document, and on typical technical scenarios. You should add others specific to your needs.

|  |  |  |
| --- | --- | --- |
| Use Case | Condition | Expected Result |
| Verify Seamless SSO with a domain hint | From a domain joined machine connected to the corporate network navigate to myapps.microsoft.com/contoso.com | When providing a domain hint the user should be silently signed in with no username or password prompt. |
| Verify Seamless SSO without a domain hint | From a domain joined machine connected to the corporate network navigate to myapps.microsoft.com | When no domain hint is provided the user will need to enter in their UPN but they will not be challenged for a password. |
| Verify PTA | From a non-domain joined PC or any device connected to an external network, navigate to myapps.microsoft.com/contoso.com | The user should see the Azure AD login page where they will have to enter in both a username and password. They should be successfully signed. |
| Verify Exchange ActiveSync | On a mobile device, configure the ActiveSync client. | The user will need to enter in both a username and password. The ActiveSync client will be using the PTA flow. |

# Implementing Your Solution

Now that you have planned your solution, you are ready to implement it.

## Solution Components

Implementation includes the following components:

1. Preparing for Seamless Single Sign on
2. Changing sign-in method Pass-Through Authentication and enabling Seamless SSO

## Step 1 – Prepare for Seamless SSO

To your devices to use Seamless SSO, you need to add an Azure AD URL to the users' Intranet zone settings by using Group Policy in Active Directory.

By default, the browser automatically calculates the correct zone, either Internet or Intranet, from a specific URL. For example, "http://contoso/" maps to the Intranet zone, whereas "http://intranet.contoso.com/" maps to the Internet zone (because the URL contains a period). Browsers will not send Kerberos tickets to a cloud endpoint, like the Azure AD URL, unless you explicitly add the URL to the browser's Intranet zone.

Follow the steps on the following article to make the required changes to your devices.

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

**Important!** Making this change won’t modify the way your users sign in to Azure AD. However, it’s important this configuration is applied to all your devices before you continue with the Step 3. Also note that users signing in on devices that have not received this configuration will simply need to enter username and password to sign in to Azure AD.

## Step 2 – Change sign-in method to Pass-Through Authentication and enable Seamless SSO

### Option A: Configuring Pass-through Authentication by using Azure AD Connect

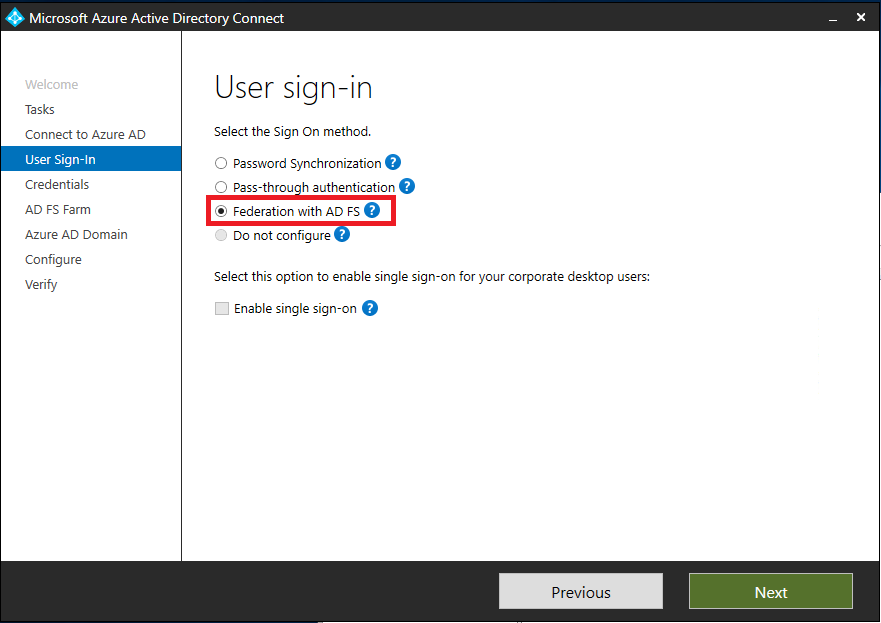
Use this method when your AD FS was initially configured using Azure AD Connect. You cannot use this method if your AD FS was not originally configured using Azure AD Connect.

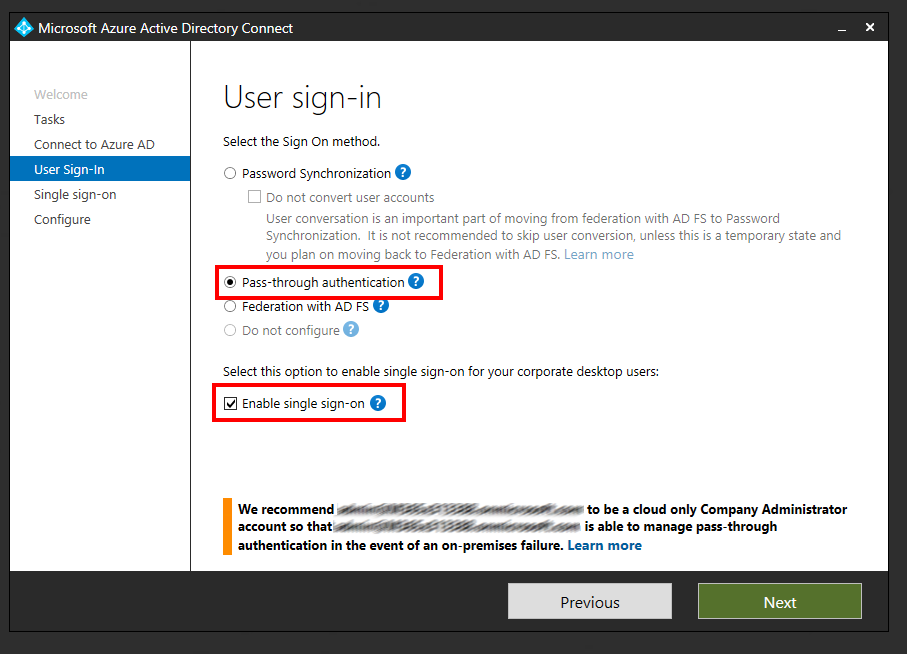
**Important!** Remember that by following the steps below all your domains will be converted from Federated to Managed. Review the section [Plan Migration Method](#_Plan_Migration_Method) for more information.

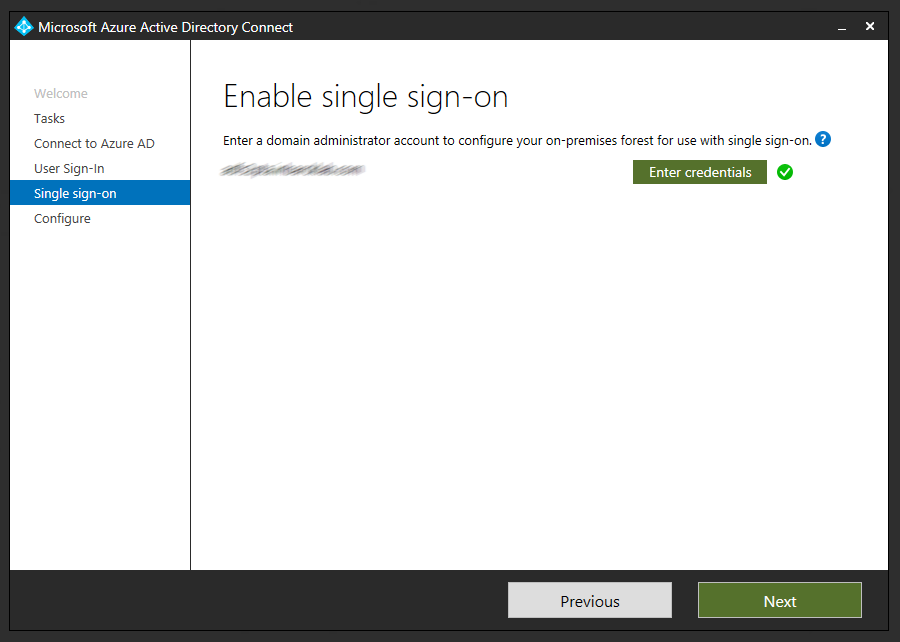
#### Change user Sign in method

1. On the Azure AD Connect Server, open the wizard.
2. Select **Change User Sign in** and then select **Next**.
3. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.
4. The **User Sign-in** screen, change the radio button from **Federation with AD FS** to **Pass-through authentication,** select **Enable single sign-on** then select **Next.**

Before the change:

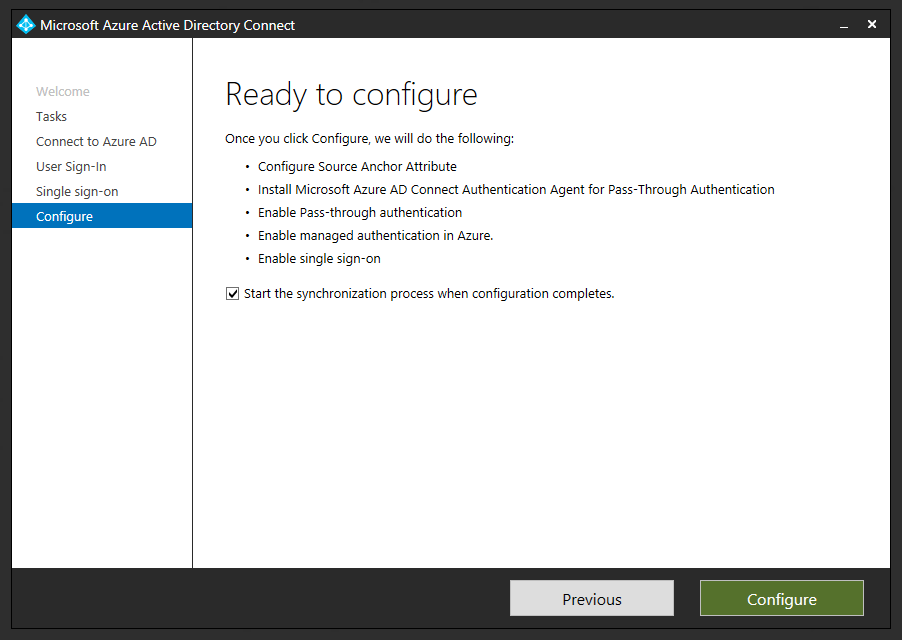
****

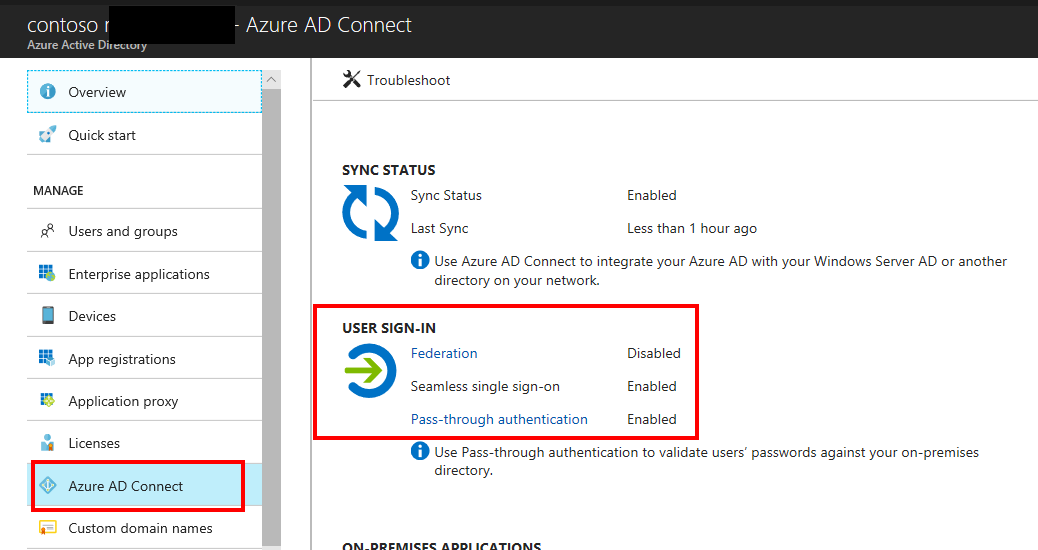
After the change:

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

* A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
* The computer account's Kerberos decryption key is shared securely with Azure AD.
* 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

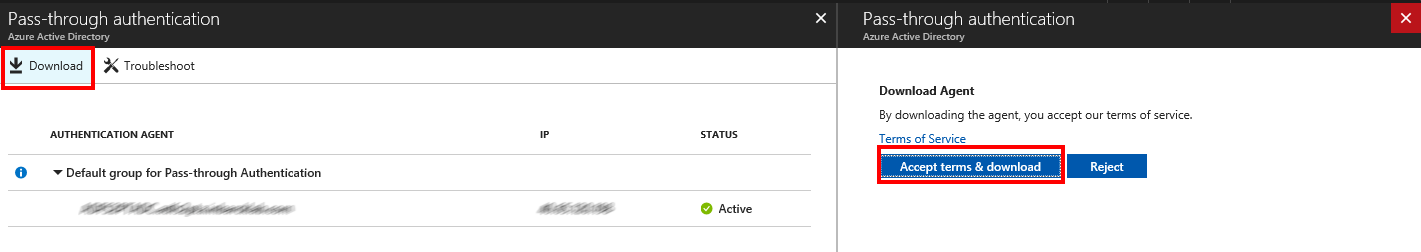
1. In the **Ready to Configure** screen, make sure “**Start Synchronization process when configuration completes**” checkbox is selected. Then select **Configure**.  
   
2. Open the **Azure AD portal**, select **Azure Active Directory**, and then select **Azure AD Connect**.
3. Verify that that **Federation is Disabled** while **Seamless single sign on** and **Pass-thorough authentication** are **Enabled**.



#### Deploy Additional Authentication Agents

Open the **Azure Portal**, browse to **Azure Active Directory**, **Azure AD Connect** and click **Pass-through authentication**.

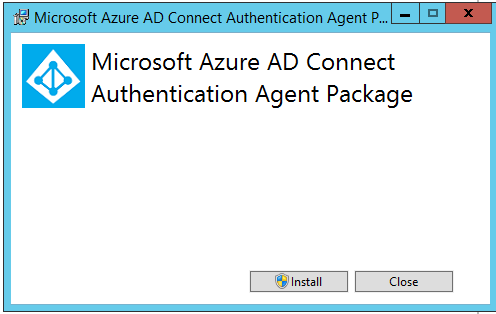
From the **Pass-through authentication** page, click on the **Download** button. From the **Download Agent** screen, click on **Accept terms and download.**

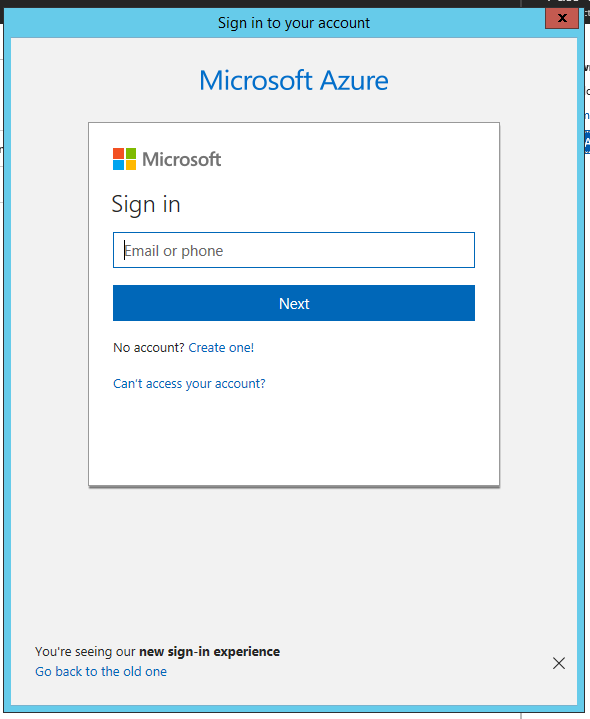


The download of additional authentication agents will begin. Install the secondary Authentication Agent on a domain-joined server.

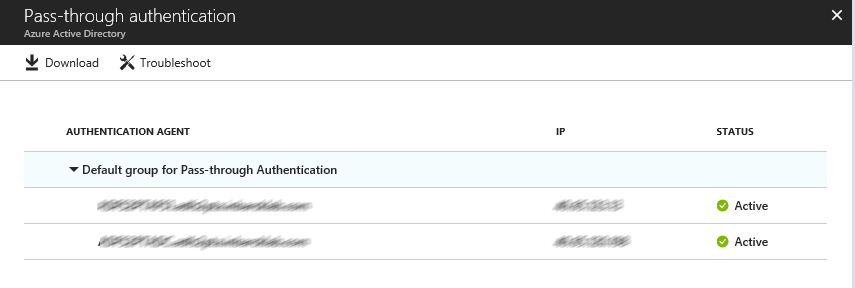
***NOTE:*** the first agent is always installed on the Azure AD Connect server itself as part of the configuration changes made in the User Sign In section of the Azure AD Connect tool. Any additional Authentication Agents should be installed on a separate server. It is recommended to have between 2-3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



Go to [**Testing and Next Steps**](#_Next_Steps_and).

**Important!** Skip the section Option B: Switch from Federation to PTA by using Azure AD Connect and PowerShell as the steps in that section do not apply.

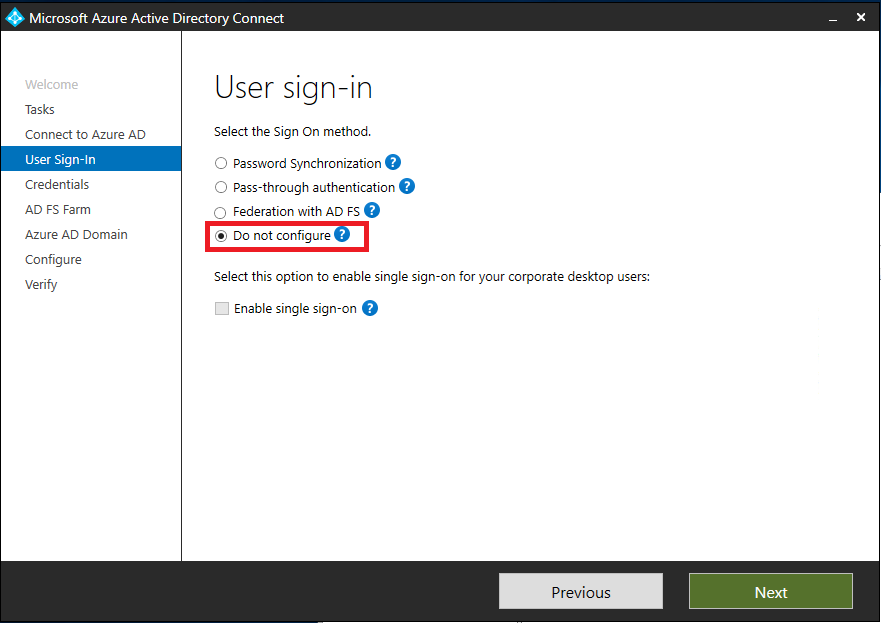
### Option B - Switch from Federation to PTA using Azure AD Connect and PowerShell

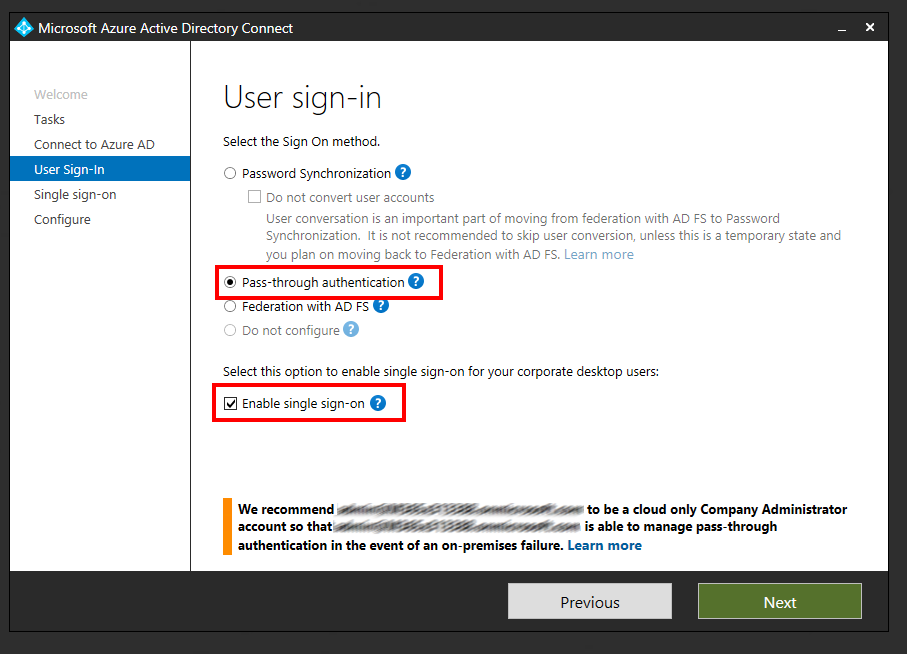
Use this option when your federation was not initially configured by using Azure AD Connect.

#### Enable Pass-through Authentication

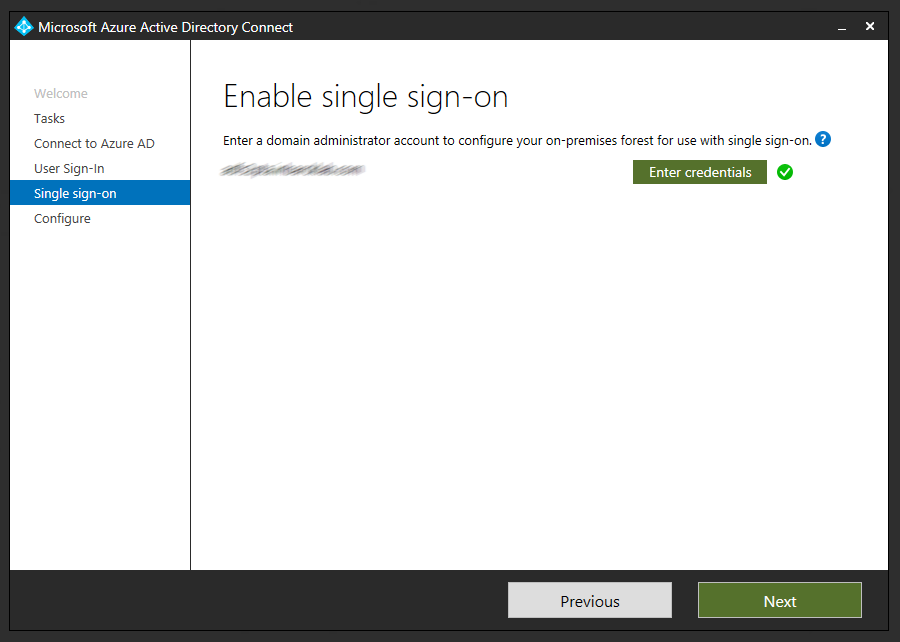
1. On the Azure AD Connect Server, open the wizard.
2. Select **Change User Sign in** and then select **Next**.
3. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.
4. On the **User Sign-in** screen, change the radio button from **Do not configure** to **Pass-through authentication,** select **Enable single sign-on** then select **Next.**

Before the change:

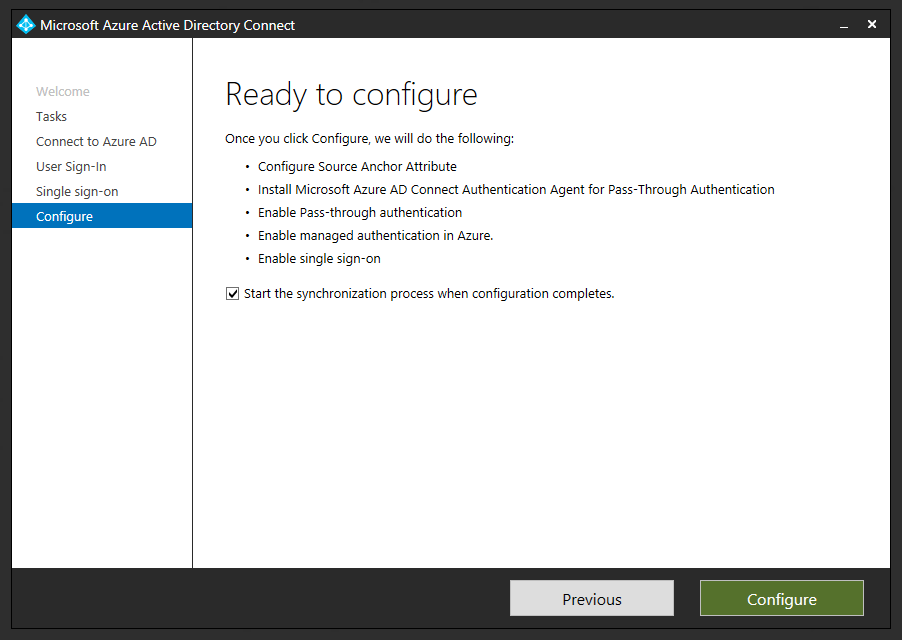
****

After the change:

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

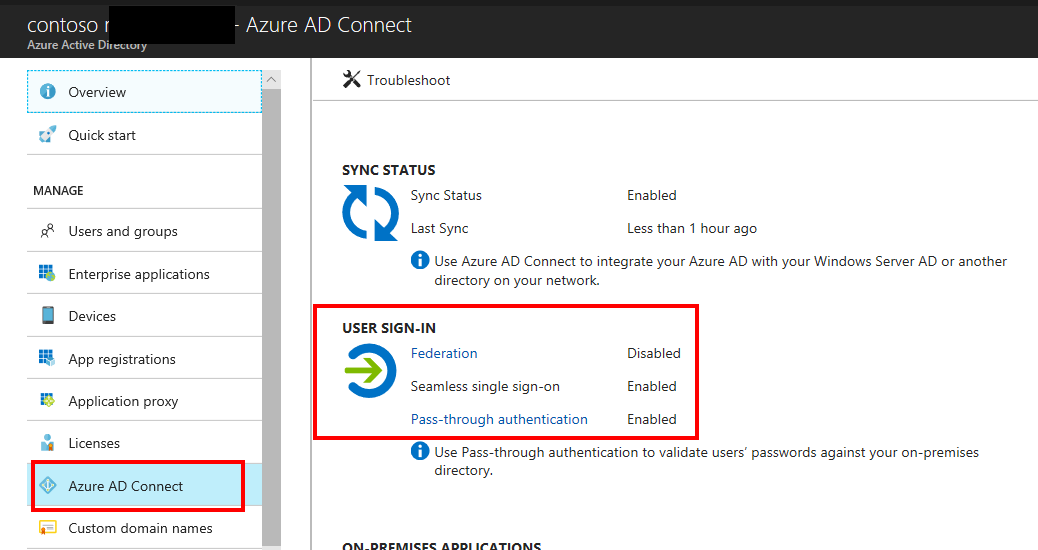
* A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
* The computer account's Kerberos decryption key is shared securely with Azure AD.
* In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that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

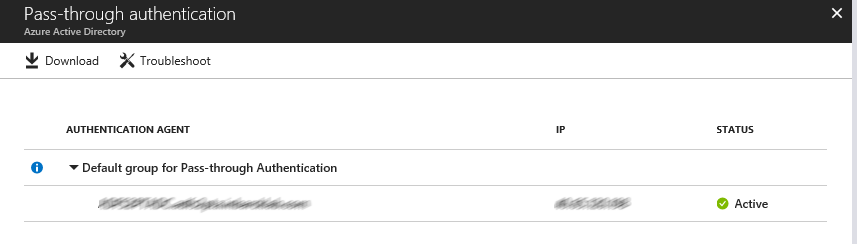
1. In the **Ready to Configure** screen, make sure “**Start Synchronization process when configuration completes**” checkbox is selected. Then select **Configure**.  
   

The following occurs when selecting Configure:

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

1. Verify that that **Federation is Disabled** while **Seamless single sign on** and **Pass-thorough authentication** are **Enabled**.

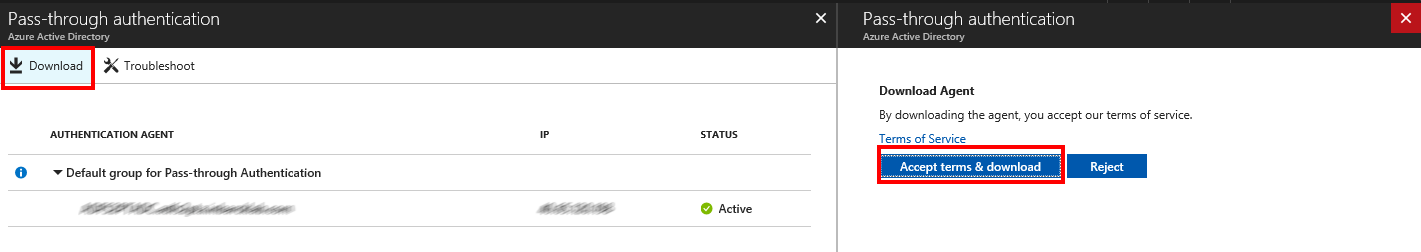


Select **Pass-through authentication** and verify that the status is **Active**.  
  
If the Authentication Agent is not active, follow [these troubleshooting steps](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-troubleshoot-pass-through-authentication) before proceeding with the domain conversation process in the next step. You risk causing an authentication outage if you convert your domains prior to validating that your PTA agents have installed successfully and that their status shows as “Active” in the Azure portal.

#### Deploy Additional Authentication Agents

Open the **Azure Portal**, browse to **Azure Active Directory**, **Azure AD Connect** and click **Pass-through authentication**.

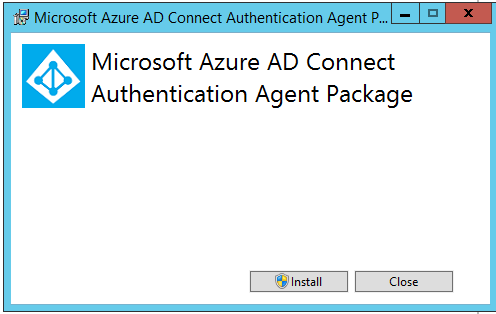
From the **Pass-through authentication** page, click on the **Download** button. From the **Download Agent** screen, click on **Accept terms and download.**

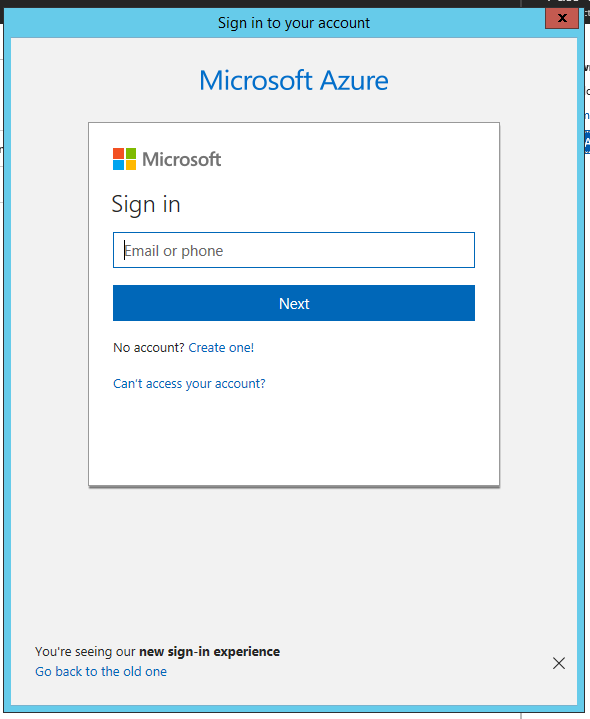


The download of additional authentication agents will begin. Install the secondary Authentication Agent on a domain-joined server.

***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.

#### 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.

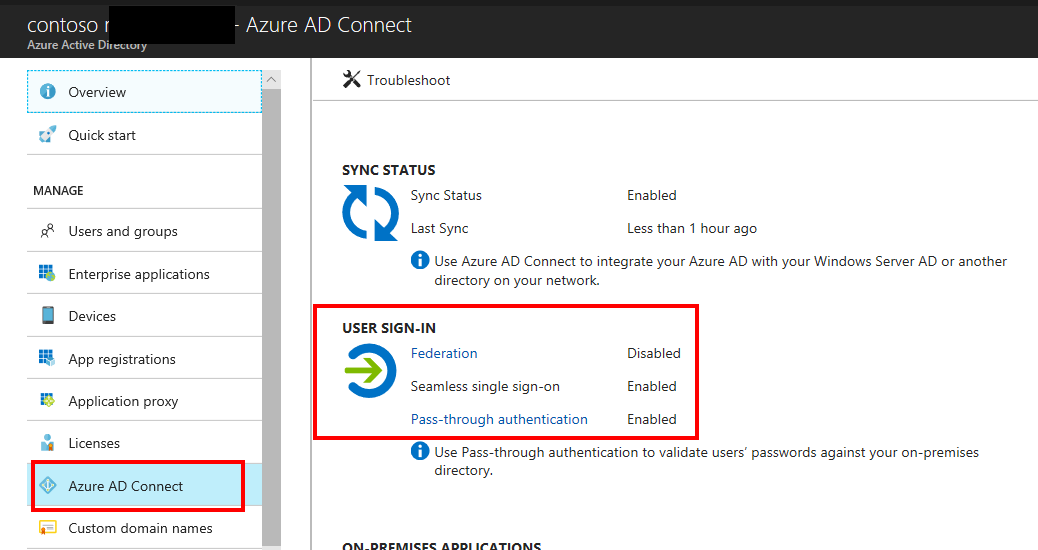
Not all domains need the be converted at the same time, you might choose to start with a test domain on your production tenant or the domain with the least number of users.

The conversion is performed using the Azure AD PowerShell Module.

1. Open **PowerShell** and login to Azure AD using a **Global Administrator** account.
2. To convert the first domain, run the following command:  
   Set-MsolDomainAuthentication -Authentication Managed -DomainName <domainname>



1. Open the **Azure AD portal**, select **Azure Active Directory**, and then select **Azure AD Connect**.
2. Verify that that **Federation is Disabled** while **Seamless single sign on** and **Pass-thorough authentication** are **Enabled**.

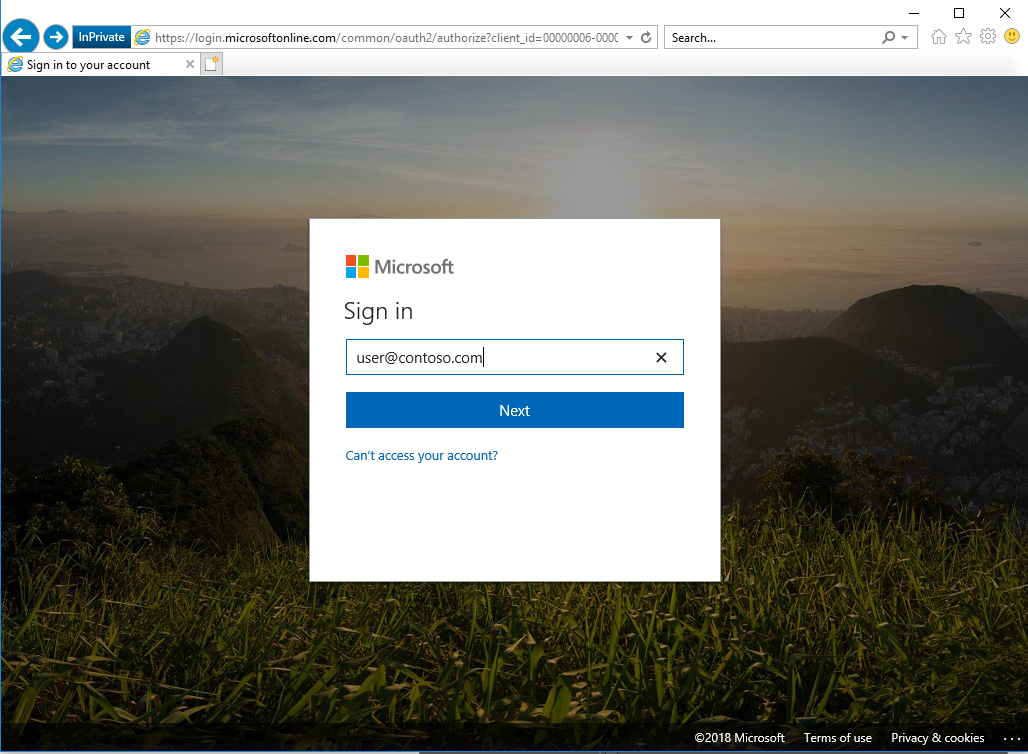


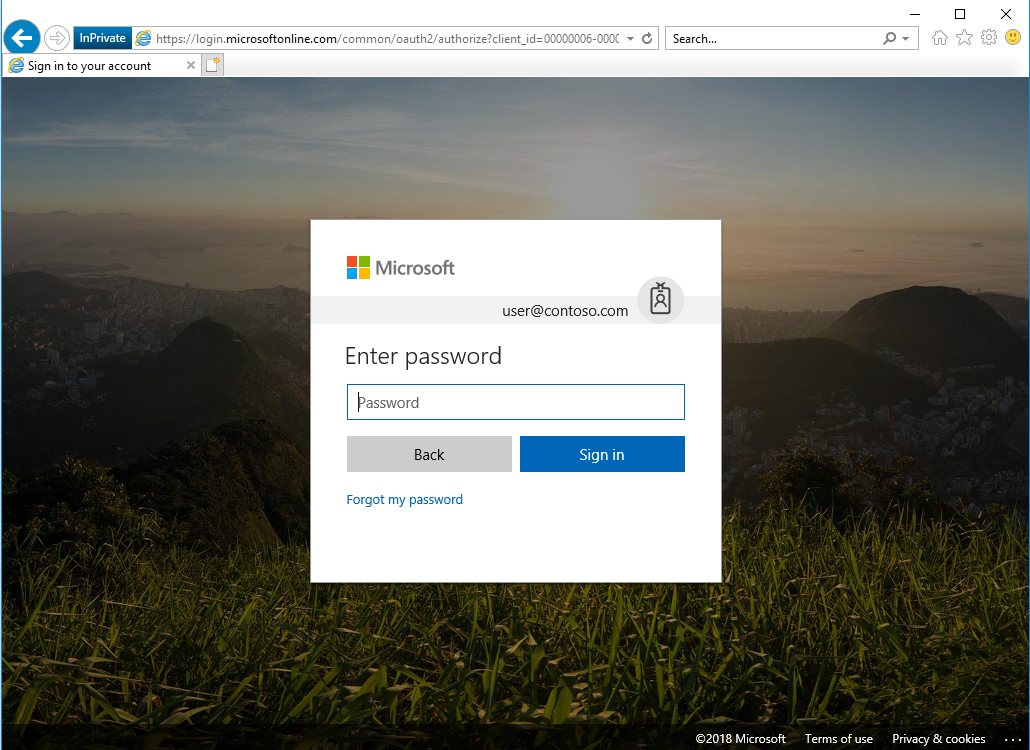
## Testing and Next Steps

### Test Pass-through Authentication

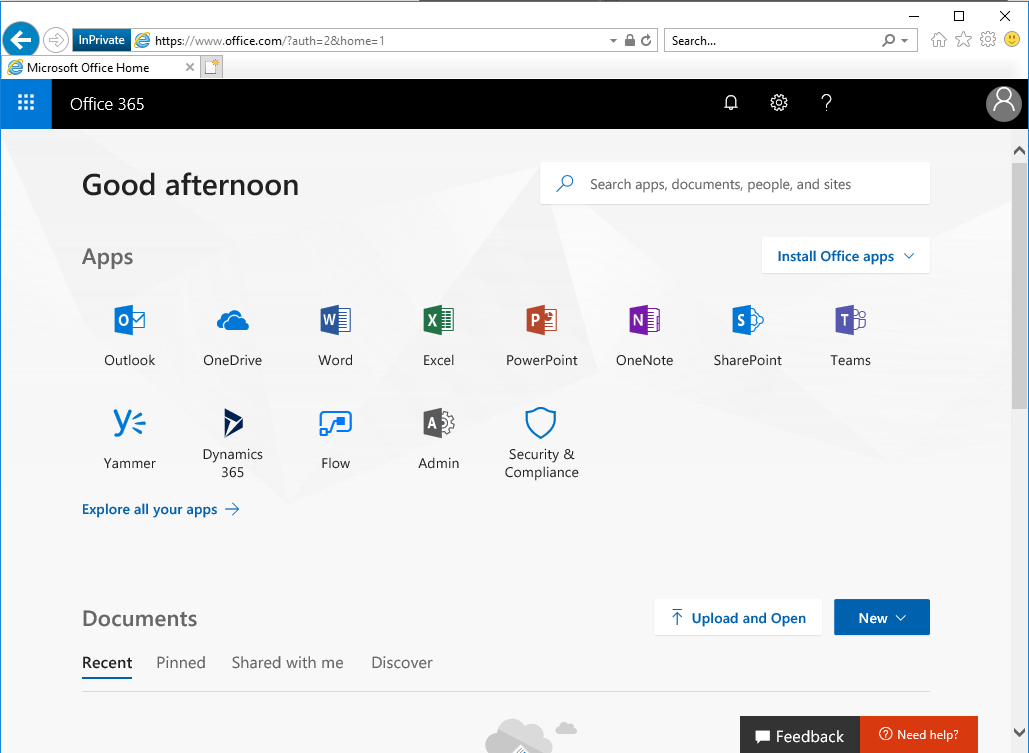
When your tenant was using federation, users were getting redirected from the Azure AD login page to your AD FS environment. Now that the tenant is configured to use Pass-through Authentication instead of federation, users will not get redirected to AD FS and instead will login directly through the Azure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

Open Internet Explorer in InPrivate mode to avoid Seamless SSO signing you in automatically 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.





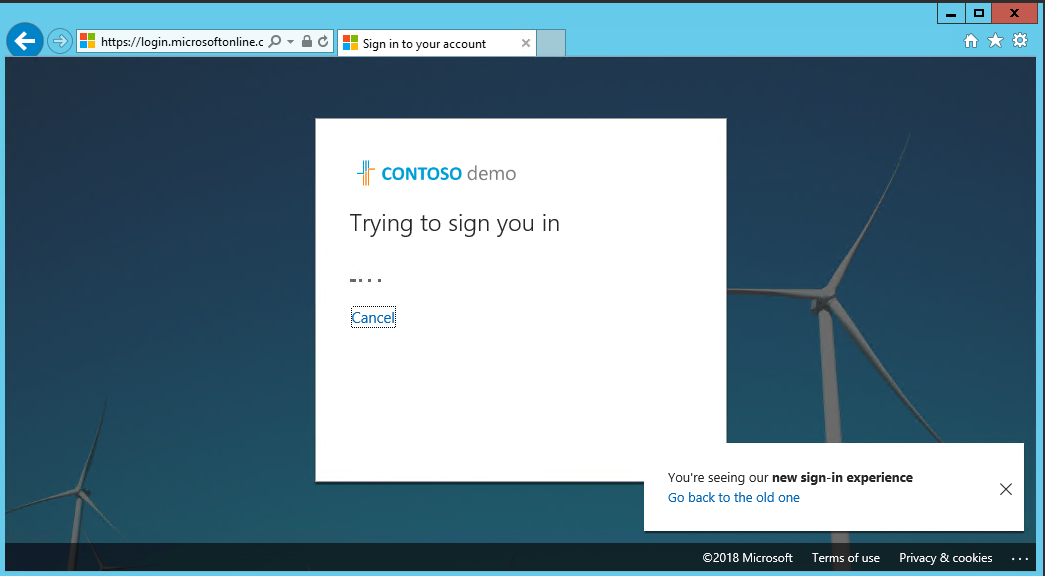
Once you type the password, you should get redirected to the Office 365 portal.



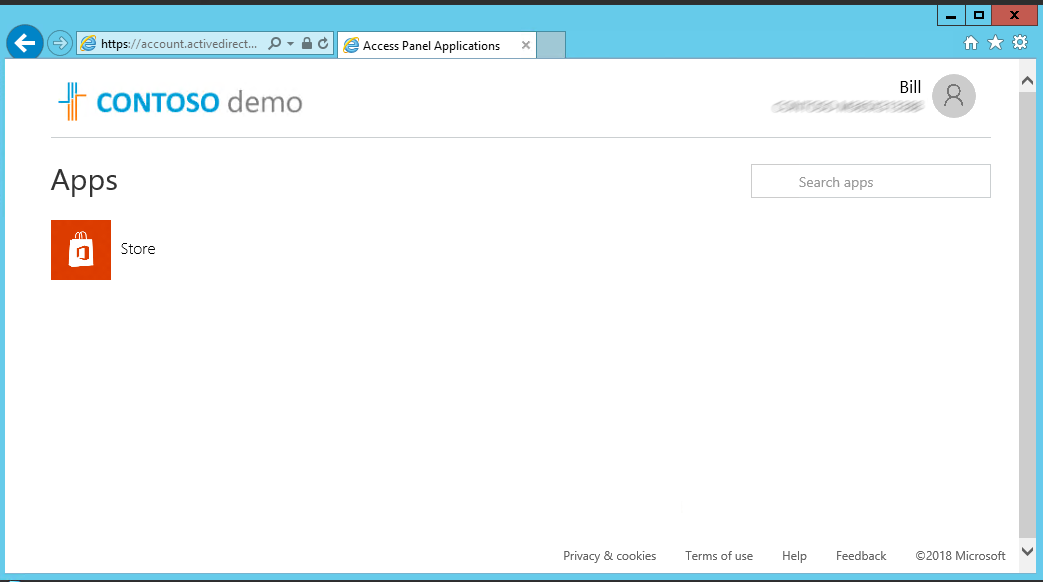
### Test Seamless single sign on

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.

### 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.

### Support Planning

Your support team should understand how to troubleshoot any authentication issues that arise either during, or after the change from federation to managed. Use the following troubleshooting documentation to help your support team familiarize themselves with the common troubleshooting steps and appropriate actions that can help to isolate and resolve the issue.

[Troubleshoot Azure Active Directory Pass-through Authentication](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-troubleshoot-pass-through-authentication)

[Troubleshoot Azure Active Directory Seamless Single Sign-On](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-troubleshoot-sso)

# Manage your solution

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 to align with how Active Directory domain members submit password changes. As there is no associated device attached to the AZUREADSSOACC computer account object the roll over needs to be performed manually.

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>

© 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