

Azure Active Directory **Migration from ADFS to** **Password Hash Synchronization** Deployment Plan

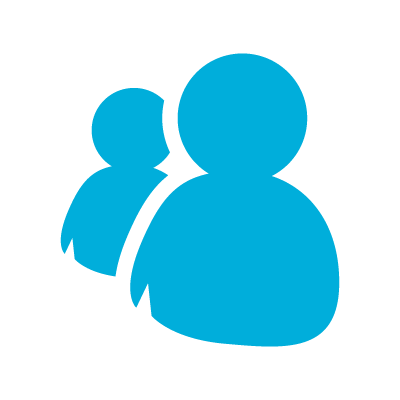
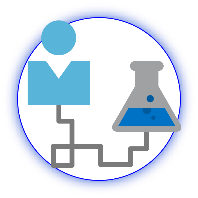
**How to use this guide**

This step-by-step guide walks through the implementation of Password Hash Synchronization 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**

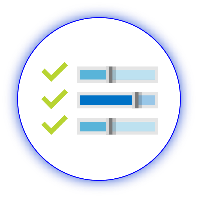
**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_your_Deployment)**

[Your project](#_Planning_your_Deployment)



**4**

**[Manage](#_Operations)**

[Your implementation](#_Operations)

**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.

© 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

Contents

[Introduction 5](#_Toc514420710)

[Purpose of document 5](#_Toc514420711)

[What is Managed Authentication? 5](#_Toc514420712)

[What is Managed Authentication with Password Hash Synchronization? 5](#_Toc514420713)

[What is Seamless Single Sign-on? 5](#_Toc514420714)

[Current state of Authentication 5](#_Toc514420715)

[Goals for Password Hash Synchronization with Seamless Single Sign-on 6](#_Toc514420716)

[Stakeholders and Sign-off 7](#_Toc514420717)

[Project Scope 8](#_Toc514420718)

[Prerequisites 8](#_Toc514420719)

[In scope 8](#_Toc514420720)

[Out of scope 8](#_Toc514420721)

[Planning your Deployment 9](#_Toc514420722)

[General Planning 9](#_Toc514420723)

[Environments and project stages 9](#_Toc514420724)

[Licensing Considerations 9](#_Toc514420725)

[Planning for Password Hash Synchronization 10](#_Toc514420726)

[Understanding Password Hash Synchronization 10](#_Toc514420727)

[Password Hash Synchronization Considerations 12](#_Toc514420728)

[Update Azure AD Connect 13](#_Toc514420729)

[Password Hash Synchronization required permissions 13](#_Toc514420730)

[Plan Migration Method 13](#_Toc514420731)

[Document Current Federation Settings 16](#_Toc514420732)

[Deployment Considerations and AD FS Usage 18](#_Toc514420733)

[Validate Your Current AD FS Usage 18](#_Toc514420734)

[Considerations for Common AD FS Customizations 18](#_Toc514420735)

[Plan Seamless SSO 19](#_Toc514420736)

[Plan Logging and Auditing 20](#_Toc514420737)

[Planning Deployment and Support 20](#_Toc514420738)

[Plan the Maintenance Window 20](#_Toc514420739)

[Plan for Rollback 21](#_Toc514420740)

[Plan Change Communications 21](#_Toc514420741)

[Test Planning 23](#_Toc514420742)

[Implementing Your Solution 23](#_Toc514420743)

[Solution Components 23](#_Toc514420744)

[Step 1 – Enable Password Hash Synchronization 23](#_Toc514420745)

[Validate Password Hash Synchronization has completed successfully 24](#_Toc514420746)

[Step 2 – Prepare for Seamless SSO 25](#_Toc514420747)

[Step 3 – Change sign-in method to Password Hash Synchronization and enable Seamless SSO 25](#_Toc514420748)

[Option A - Switch from Federation to Password Hash Synchronization by using Azure AD Connect 25](#_Toc514420749)

[Option B - Switch from Federation to Password Hash Synchronization using Azure AD Connect and PowerShell 29](#_Toc514420750)

[Testing and Next Steps 35](#_Toc514420751)

[Test Authentication with Password Hash Synchronization 35](#_Toc514420752)

[Test Seamless single sign on 37](#_Toc514420753)

[Removal of the Relying Party Trust 38](#_Toc514420754)

[Rollback 38](#_Toc514420755)

[Troubleshooting 38](#_Toc514420756)

[Operations 39](#_Toc514420757)

[Roll over the Seamless SSO Kerberos decryption 39](#_Toc514420758)

# Introduction

## Purpose of document

This document describes the key considerations and processes involved to deploy Password Hash Synchronization 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 Password Hash Synchronization (Password Hash Synchronization). Managed Authentication with Pass-Through Authentication (PTA) is addressed in a separate deployment guide.

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

## What is Managed Authentication with Password Hash Synchronization?

With Password Hash Synchronization, hashes of user passwords are synchronized from on-premises Active Directory to Azure AD, allowing Azure AD to authenticate users with no interaction with the on-premises Active Directory. When passwords are changed or reset on-premises, the new password hashes are synchronized to Azure AD in near real-time so that your users can always use the same password for cloud resources and on-premises resources. The clear-text passwords are never sent to Azure AD or stored in Azure AD.

## 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 Password Hash Synchronization 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 Password Hash Synchronization. >>

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

## Goals for Password Hash Synchronization with Seamless Single Sign-on

Moving from Federation to Password Hash Synchronization and Seamless SSO will benefit our business in the following ways:

|  |  |
| --- | --- |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Within_Your_Reach.png | **MANAGE COST**  Enabling Password Hash Synchronization 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 | **MANAGE COMPLEXITY AND RISK**  Moving to Password Hash Synchronization 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 Password Hash Synchronization 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.

* 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 solution, which may include managing access. | SO/I |
| Enter group alias for pilot group | End Users  The group of users for which the solution will be implemented. They will be receiving communications about changes in the user experience. | 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.
* An Azure Global Administrator account is available to configure Password Hash Synchronization and Seamless SSO 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.

## In scope

The following are in scope for this project:

**Enabling Password Hash Synchronization**

* Enabling the Password Hash Synchronization feature.
* Changing the user sign-in method from federated to managed.

**Enabling Seamless SSO**

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

**Deployment and Support**

* Rollback scenario.
* 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

# 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 | / |
|  | Pilot | / |
|  | General Availability | / |

### 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 Password Hash Synchronization 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

## Planning for Password Hash Synchronization

### Understanding Password Hash Synchronization

The Active Directory domain service stores passwords in the form of a hash value representation of the actual user password. A hash value is a result of a one-way mathematical function (the hashing algorithm). There is no method to revert the result of a one-way function to the plain text version of a password. You cannot use a password hash to sign in to your on-premises network.

To synchronize your password, Azure AD Connect sync extracts your password hash from the on-premises Active Directory instance. Extra security processing is applied to the password hash before it is synchronized to the Azure Active Directory authentication service. Passwords are synchronized on a per-user basis and in chronological order.

The actual data flow of the password hash synchronization process is similar to the synchronization of user data such as DisplayName or Email Addresses. However, passwords are synchronized more frequently than the standard directory synchronization window for other attributes. The password hash synchronization process runs every 2 minutes. You cannot modify the frequency of this process. When you synchronize a password, it overwrites the existing cloud password.

The first time you enable the password hash synchronization feature, it performs an initial synchronization of the passwords of all in-scope users. You cannot explicitly define a subset of user passwords that you want to synchronize.

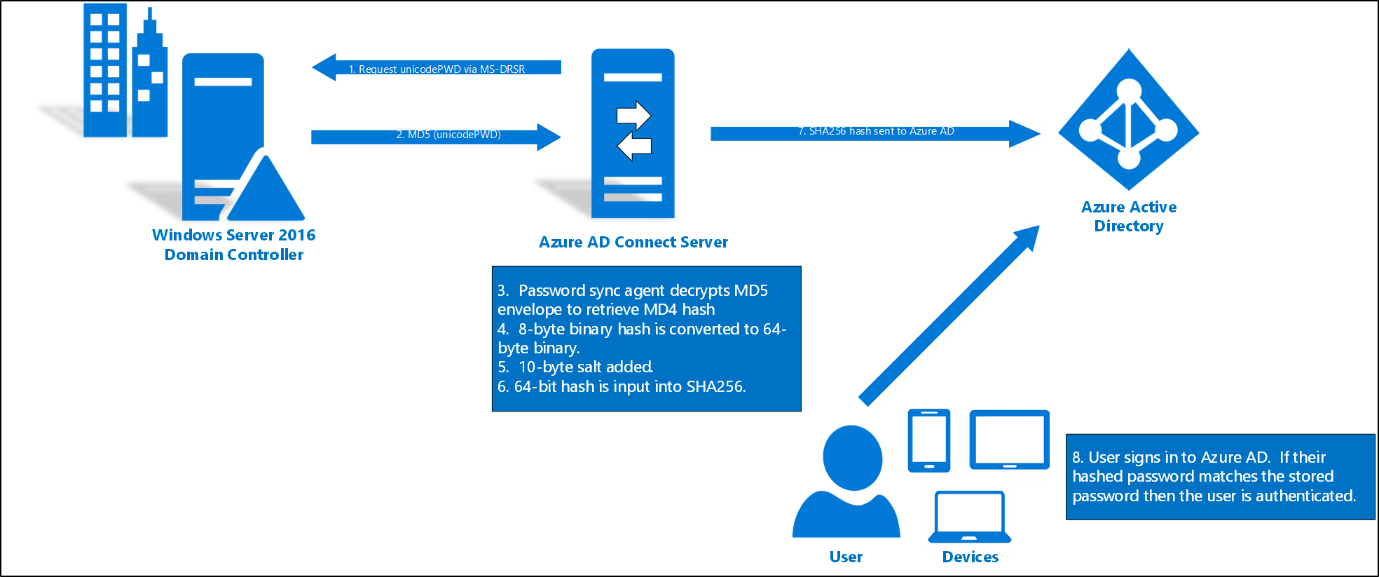
When you change an on-premises password, the updated password is synchronized, most often in a matter of minutes. The password hash synchronization feature automatically retries failed synchronization attempts. If an error occurs during an attempt to synchronize a password, an error is logged in your event viewer.

The synchronization of a password has no impact on the user who is currently signed in. Your current cloud service session is not immediately affected by a synchronized password change that occurs while you are signed in to a cloud service. However, when the cloud service requires you to authenticate again, you need to provide your new password.

A user must enter their corporate credentials a second time to authenticate to Azure AD, regardless of whether they're signed in to their corporate network. These patterns can be minimized, however, if the user selects the Keep me signed in (KMSI) check box at sign in. This selection sets a session cookie that bypasses authentication for a short period. KMSI behaviour can be enabled or disabled by the Azure AD administrator.

#### Detailed description of how password hash synchronization works

The following describes in-depth how password hash synchronization works between Active Directory and Azure AD.



1. Every two minutes, the password hash synchronization agent on the AD Connect server requests stored password hashes (the unicodePwd attribute) from a DC via the standard MS-DRSR replication protocol used to synchronize data between DCs. The service account must have Replicate Directory Changes and Replicate Directory Changes All AD permissions (granted by default on installation) to obtain the password hashes.
2. Before sending, the DC encrypts the MD4 password hash by using a key that is a MD5 hash of the RPC session key and a salt. It then sends the result to the password hash synchronization agent over RPC. The DC also passes the salt to the synchronization agent by using the DC replication protocol, so the agent will be able to decrypt the envelope.
3. After the password hash synchronization agent has the encrypted envelope, it uses MD5CryptoServiceProvider and the salt to generate a key to decrypt the received data back to its original MD4 format. At no point does the password hash synchronization agent have access to the clear text password. The password hash synchronization agent’s use of MD5 is strictly for replication protocol compatibility with the DC, and it is only used on premises between the DC and the password hash synchronization agent.
4. The password hash synchronization agent expands the binary password hash to 64 bytes by first converting the hash to a 32-byte hexadecimal string, then converting this string back into binary with UTF-16 encoding.
5. The password hash synchronization agent adds a salt, consisting of a 10-byte length salt, to the 64-byte binary to further protect the original hash.
6. The password hash synchronization agent then combines the MD4 hash plus salt, and inputs it into the PBKDF2 function. 1000 iterations of the HMAC-SHA256 keyed hashing algorithm is used.
7. The password hash synchronization agent takes the resulting 32-byte hash, concatenates both the salt and the number of SHA256 iterations to it (for use by Azure AD), then transmits the string from Azure AD Connect to Azure AD over SSL.
8. When a user attempts to sign in to Azure AD and enters their password, the password is run through the same MD4+salt+PBKDF2+HMAC-SHA256 process. If the resulting hash matches the hash stored in Azure AD, the user has entered the correct password and is authenticated.

Note: The original MD4 hash is not transmitted to Azure AD. Instead, the SHA256 hash of the original MD4 hash is transmitted. As a result, if the hash stored in Azure AD is obtained, it cannot be used in an on-premises pass-the-hash attack.

### Password Hash Synchronization Considerations

Before starting the deployment, the following considerations should be reviewed to understand how they will impact your deployment and operations.

**Password complexity**

When password synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use any password considered valid in your environment to access Azure AD services.

Passwords for users that are created directly in the cloud are still subject to password policies as defined in the cloud.

**Password expiration policy**

If a user is in the scope of password synchronization, the cloud account password is set to Never Expire. Users can continue to sign in to cloud services by using a synchronized password that is expired in the on-premises environment. The cloud password is updated the next time the password is changed on-premises.

**Account expiration**

If your organization uses the accountExpires attribute as part of user account management, be aware that this attribute is not synchronized to Azure AD. As a result, an expired Active Directory account in an environment configured for password synchronization will still be active in Azure AD. We recommend that if the account is expired, a workflow action should trigger a PowerShell script that disables the user's Azure AD account. Conversely, when the account is turned on, the Azure AD instance should be turned on

**User must change password at next logon**

When the option “User must change password at next logon” is selected for an account, the password is not synchronized to Azure AD. In this case, the user needs to change the password on-premises to allow the new password to be synchronized. This can be done directly on a domain-joined device, or via Azure AD Self-Service Password Reset/Change.

**Account Lockout**

The account locked status is not synchronized to Azure AD. If an account is locked out on-premises, authentication to Azure AD won’t be affected and will continue working.

Account lockout in Azure AD is provided by the [Smart Lockout](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-smart-lockout) feature, that can be configured to match your on-premises Active Directory account lockout settings.

### 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**.

**Important!** While changing the user sign in settings in Azure AD Connect, you might be presented with warnings indicating that user conversion and full password hash synchronization are required steps for converting from federation to cloud authentication. Additionally, outdated documentation, tools and blogs indicate these steps are required. Please note that **these steps are not required anymore**. Microsoft is working on updating documentation and tools to reflect this. Future versions of Azure AD Connect will not have an option to convert users. If you still see these warnings, check that you are running the latest version of Azure AD Connect and that you are using the latest version of this guide.

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>

### Password Hash Synchronization required permissions

Azure AD Connect can be configured using Express Settings or Custom Installation. If you used the Custom Installation option, the required permissions for Password Hash Synchronization might not be in place.

The Azure AD Connect AD DS service account needs the following permissions to be able to synchronize password hashes.

* Replicate Directory Changes
* Replicate Directory Changes All

Now is a good time to validate these permissions are in place for all domains in the forest.

For more information review the following article:

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions#create-the-ad-ds-account>

### Plan Migration Method

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

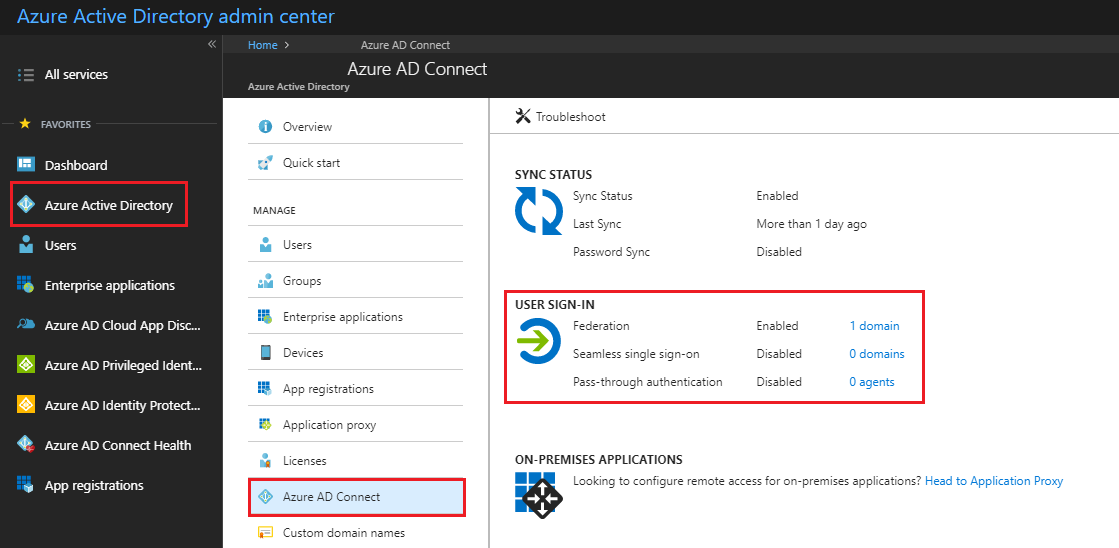
1. **Using Azure AD Connect**. If AD FS was originally configured using Azure AD Connect, then the change to Password Hash Sync as the user sign-in method ***must*** be performed through the Azure AD Connect wizard.   
   When using Azure AD Connect, it runs the Set-MsolDomainAuthentication cmdlet for 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 Password Hash Synchronization 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

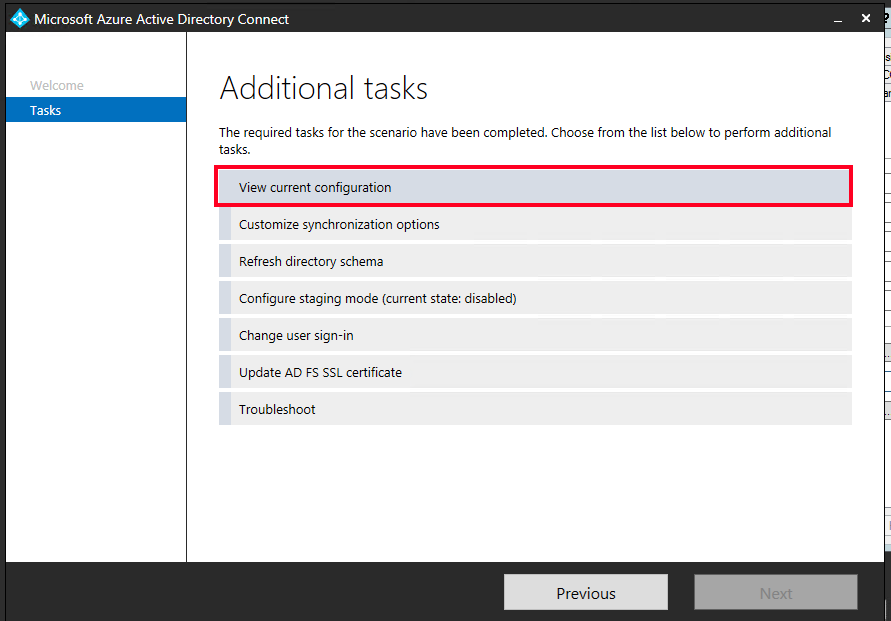
Verify your current user sign-in settings by logging into the Azure AD portal <https://aad.portal.azure.com> with a **Global Administrator** account.

In the **User Sign In** section, verify that **Federation** is **Enabled** and that **Seamless Single Sign-on** and **Pass-through authentication** are **Disabled.** Also verify that state of **Password Sync** which should show as **Disabled** unless this has previously been turned on.

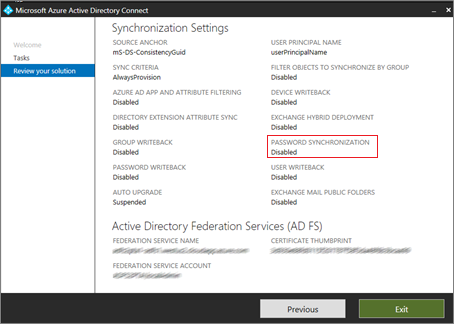
****

#### Verify Azure AD Connect configuration

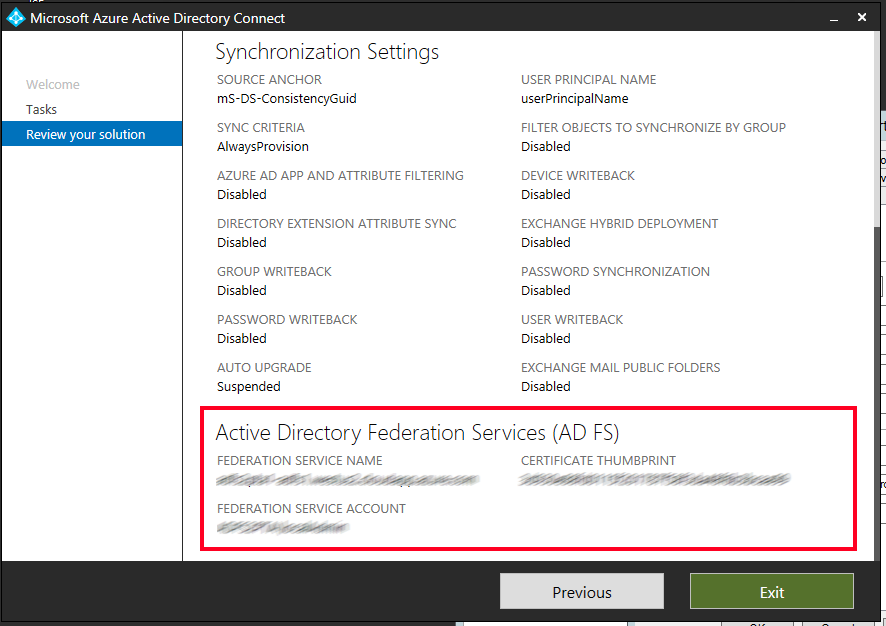
1. Go to your Azure AD Connect server and launch Azure AD Connect, then select **Configure.**
2. On the **Additional Tasks** screen, select **View Current Configuration** and then select **Next.**



1. In the **Review Your Solution** screen take note of the **Password Synchronization** status.



If Password Hash Synchronization is currently set to Disabled, you will need to follow the steps in this guide to enable it. If Password Hash Synchronization is currently set to Enabled, you can safely skip the section [Step 1 – Enable Password Hash Synchronization](#_Step_1_–) in this guide.

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 A - Switch from Federation to Password Hash Synchronization by using Azure AD Connect](#_Option_A_-).
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 B - Switch from Federation to Password Hash Synchronization using Azure AD Connect and PowerShell](#_Option_B_-).

### Document Current Federation Settings

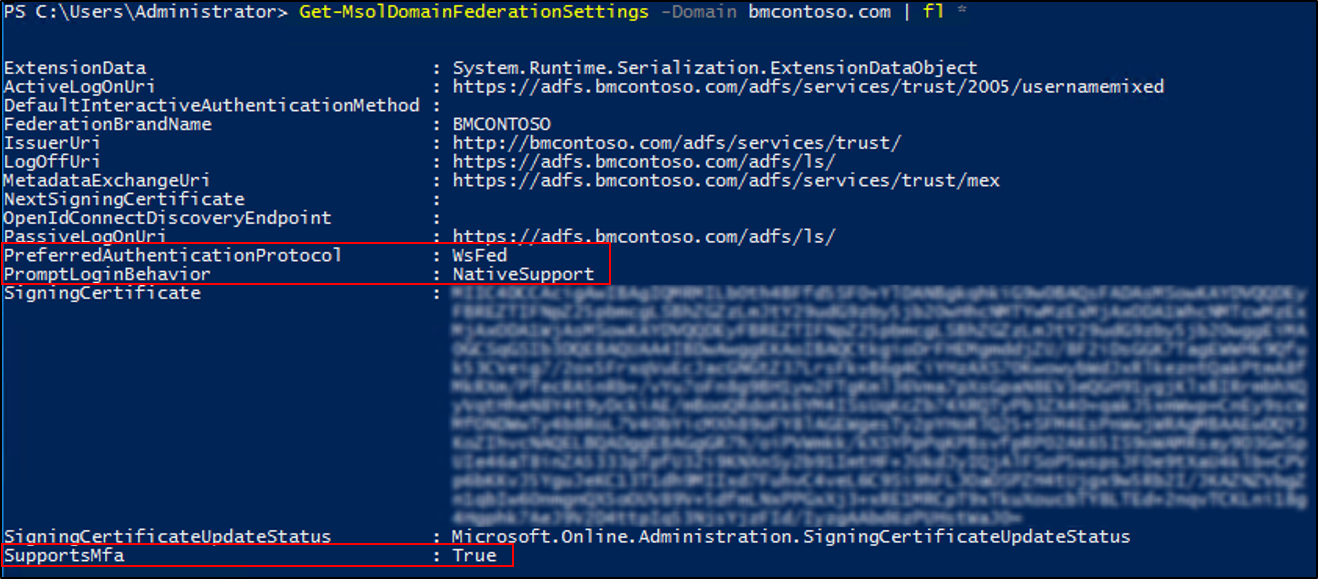
You can find the current federation setting by running the Get-MsolDomainFederationSettings cmdlet.

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 one-time 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 Password Hash Synchronization. [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 Password Hash Synchronization, 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

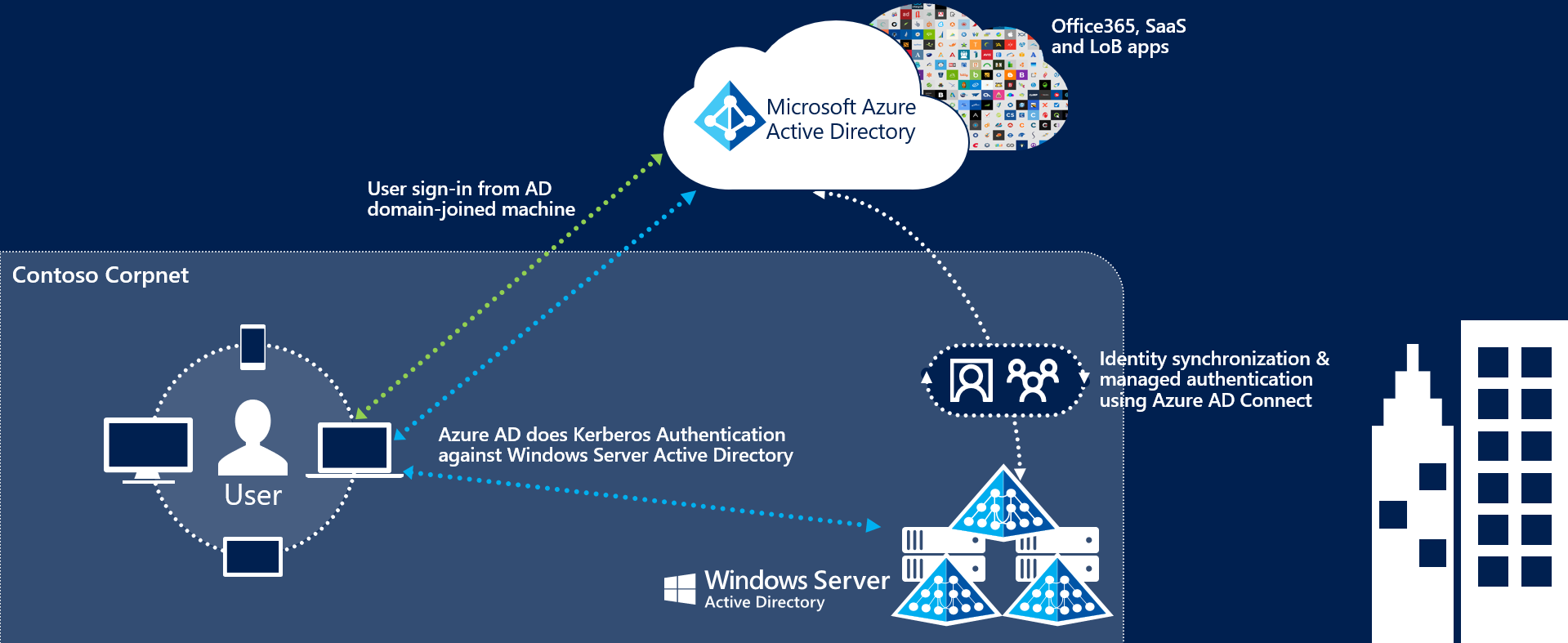
Your organization may have [customized your ADFS sign-in pages](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-user-sign-in-customization) to display information more pertinent to the organization. If so, consider making similar [customizations to the Azure AD sign-in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

## 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 2 – Prepare for Seamless SSO](#_Step_2_–).

## 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 Password Hash Synchronization 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 pilot or other 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 Password Hash Synchronization | 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 synchronized password hash for authentication. |

# Implementing Your Solution

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

## Solution Components

Implementation includes the following components:

1. Enabling Password Hash Synchronization
2. Preparing for Seamless Single Sign on
3. Changing sign-in method to Password Hash Synchronization and enabling Seamless SSO

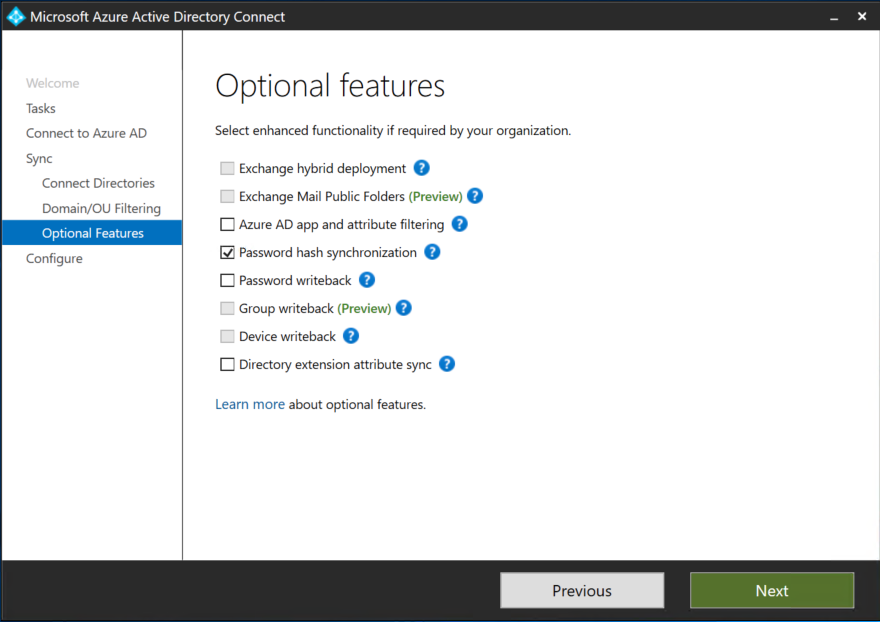
## Step 1 – Enable Password Hash Synchronization

The first step to implement this solution is enabling Password Hash Synchronization on the Azure AD Connect wizard. Password Hash Synchronization is an optional feature that can be enabled on environments using Federation without any impact to the authentication flow. In this case, Azure AD Connect will simply start synchronizing password hashes without affecting users signing-in using federation.

For this reason, we recommend performing this step as a preparation task well before changing your domains sign-in method. This will give you ample time to validate Password Hash Synchronization is correctly working.

To enable Password Hash Synchronization:

1. On the Azure AD Connect Server, open the wizard and select **Configure**.
2. Select **Customize synchronization options** and then select **Next**.
3. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.
4. In the **Connect your directories** screen click **Next**.
5. In the **Domain and OU filtering** screen click **Next**.
6. In the **Optional features** screen select **Password synchronization** and select **Next**.



1. Select **Next** on all remaining screens and **Configure** on the last screen.
2. Azure AD Connect will start synchronizing password hashes on the next synchronization.

### Validate Password Hash Synchronization has completed successfully

Once Password Hash Synchronization has been enabled, the password hashes for all users in Azure AD Connect synchronization scope will be re-hashed and written to Azure AD. Depending on the number of users, this operation can take from minutes to several hours.

For planning purposes, you should estimate that approximately 20,000 users can be processed in 1 hour.

To validate Password Hash Synchronization is correctly working, use the Troubleshooting task on the Azure AD Connect wizard.

#### Run the troubleshooting task

1. Open a new Windows PowerShell session on your Azure AD Connect server with the Run as Administrator option.
2. Run *Set-ExecutionPolicy RemoteSigned* or *Set-ExecutionPolicy Unrestricted*.
3. Start the Azure AD Connect wizard.
4. Navigate to the Additional Tasks page, select Troubleshoot, and click Next.
5. On the Troubleshooting page, click Launch to start the troubleshooting menu in PowerShell.
6. In the main menu, select Troubleshoot password hash synchronization.
7. In the sub menu, select Password hash synchronization does not work at all.

If you find issues, use the information on this article to troubleshoot:

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-troubleshoot-password-hash-synchronization>

## Step 2 – 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.

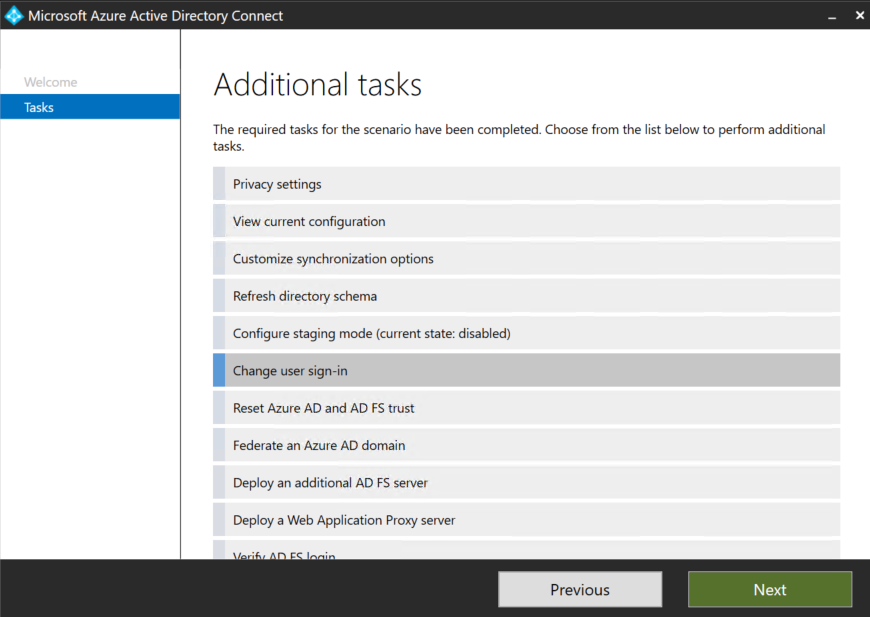
## Step 3 – Change sign-in method to Password Hash Synchronization and enable Seamless SSO

### Option A - Switch from Federation to Password Hash Synchronization by using Azure AD Connect

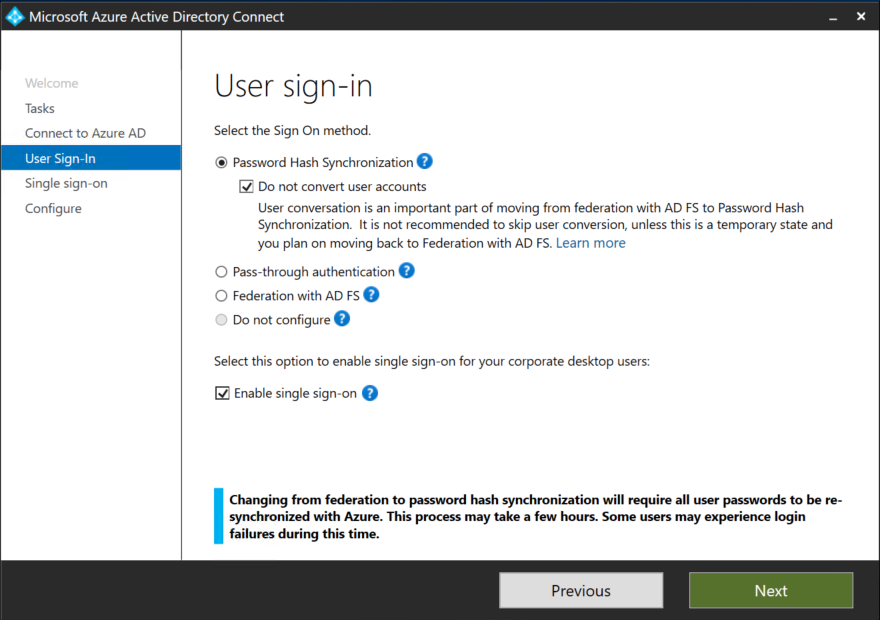
Use this method when your AD FS was initially configured using Azure AD Connect. You cannot use this method if your AD FS was not originally configured using Azure AD Connect.

#### 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**.



1. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.
2. In the **User Sign-in** screen, change the radio button from **Federation with AD FS** to **Pass Hash Synchronization,** and make sure to check the box **Do not convert user accounts** as this is a deprecated step and will be removed from a future version of AAD Connect. Also select **Enable single sign-on** then select **Next.**



**Important!** You can safely ignore the warnings indicating that user conversion and full password hash synchronization are required steps for converting from federation to cloud authentication. Please note that **these steps are not required anymore**, future versions of Azure AD Connect will not have an option to convert users. If you still see these warnings, check that you are running the latest version of Azure AD Connect and that you are using the latest version of this guide. For more information see the [Update Azure AD Connect section](#_Update_Azure_AD).

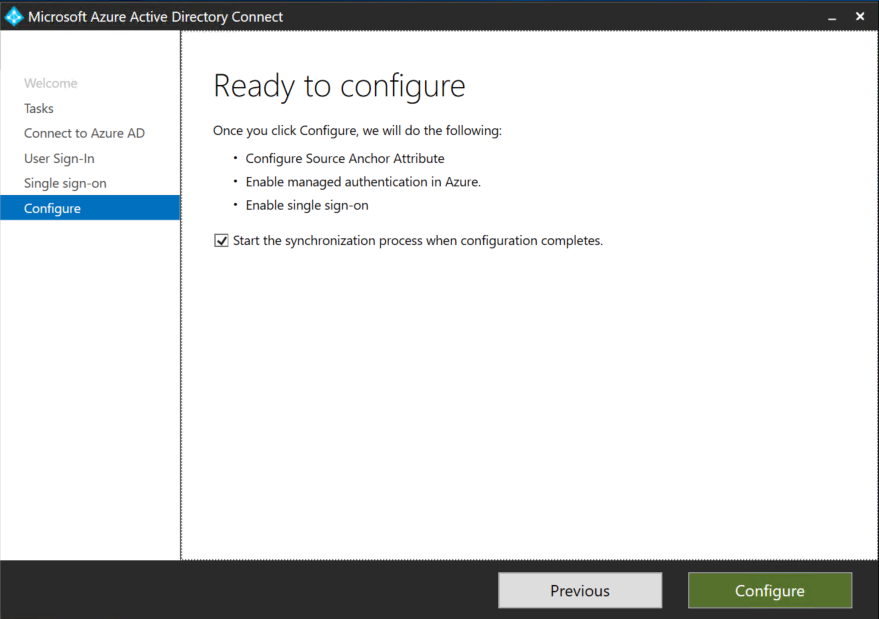
1. In **Enable Single Sign-on** screen, enter the credentials of Domain Administrator account, then select **Next**.



**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

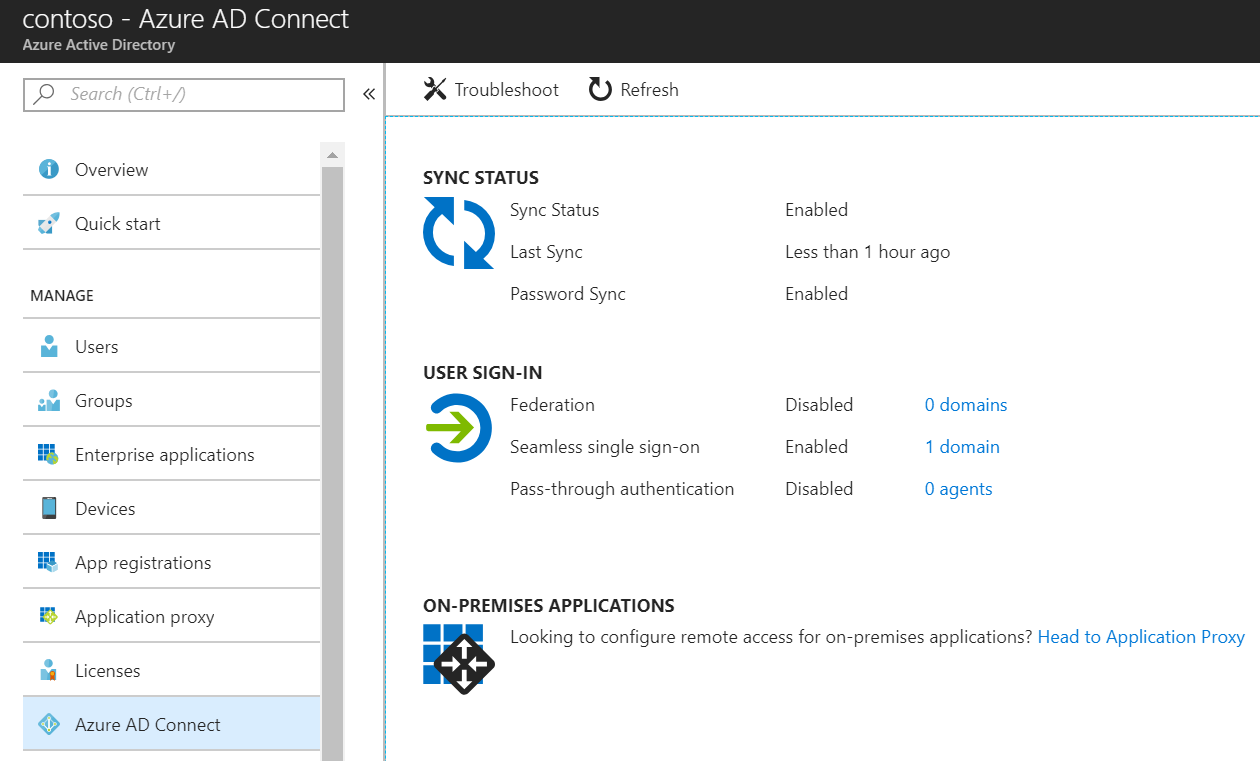
* A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
* The computer account's Kerberos decryption key is shared securely with Azure AD.
* In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that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



**Important!** At this point all your federated domains will be changed to Managed authentication which will now leverage Password Hash Synchronization as the method for authentication.

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 **Password Sync** are **Enabled**.



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

**Important!** Skip the section Option B - Switch from Federation to Password Hash Synchronization using Azure AD Connect and PowerShell as the steps in that section do not apply.

### Option B - Switch from Federation to Password Hash Synchronization using Azure AD Connect and PowerShell

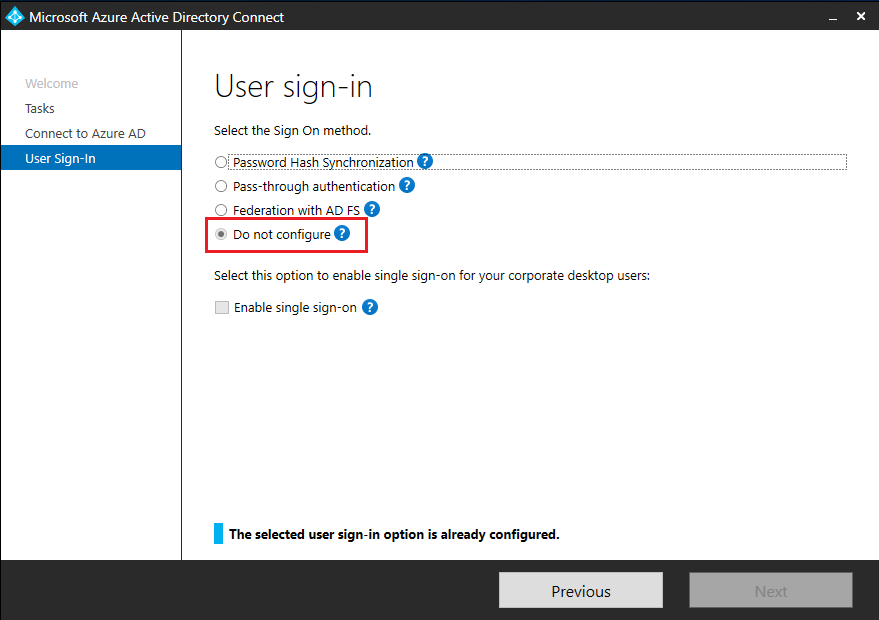
Use this option when your federation was not initially configured by using Azure AD Connect.

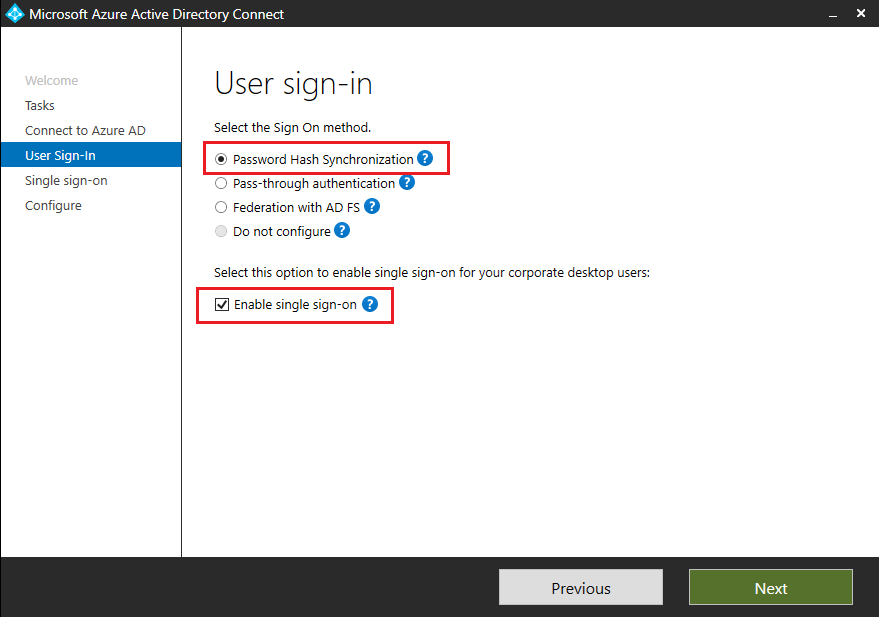
As part of this process you will enable Seamless SSO and switch your domains from Federated to Managed.

#### Enable Seamless SSO

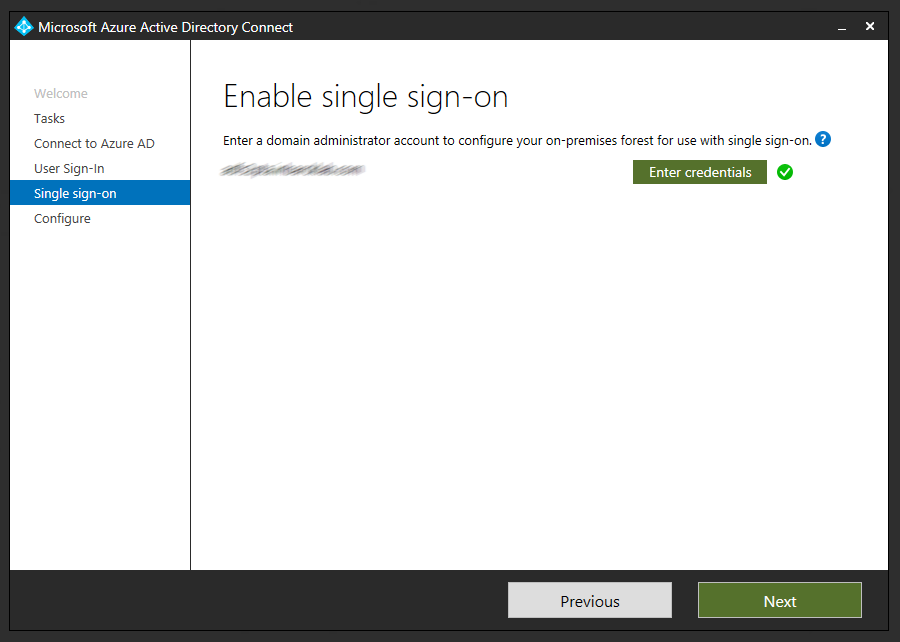
1. On the Azure AD Connect Server, open the wizard.
2. Select **Change User Sign in** and then select **Next**.
3. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.
4. On the **User Sign-in** screen, change the radio button from **Do not configure** to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

Before the change:

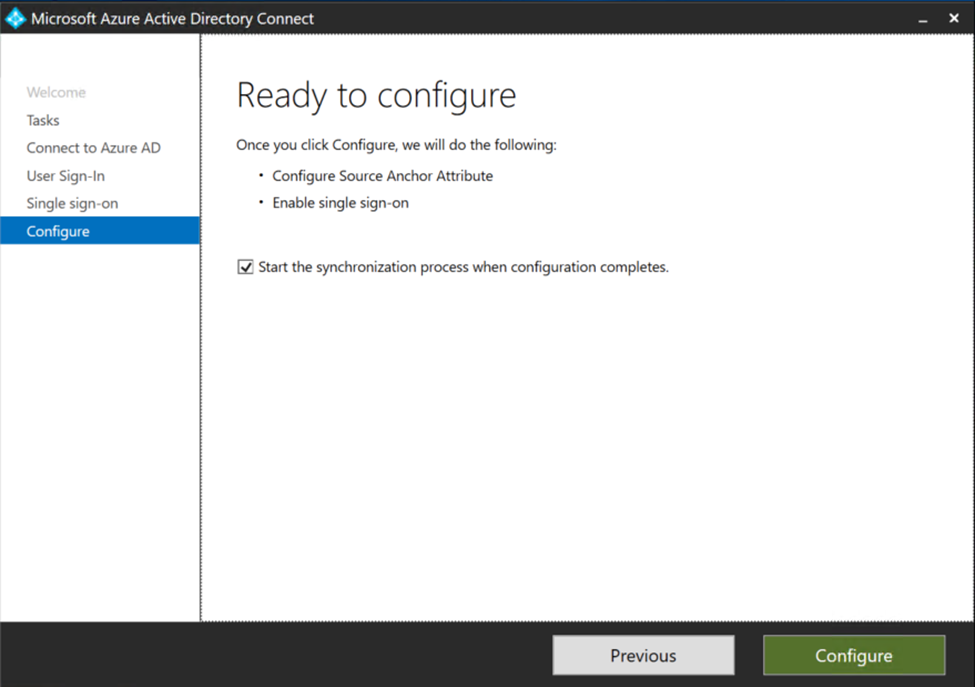
****

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.

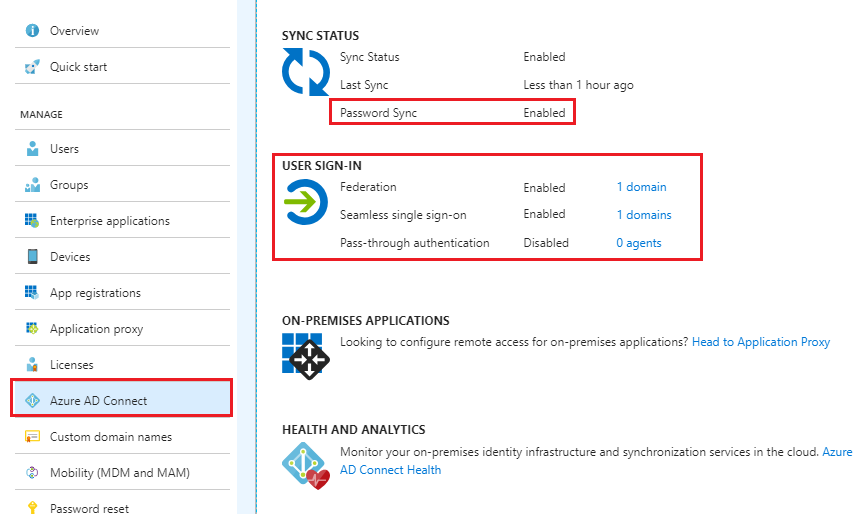
* A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
* The computer account's Kerberos decryption key is shared securely with Azure AD.
* In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that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

When selecting configure, Seamless SSO will be configured as per the previews step. Password Hash Synchronization configuration won’t be modified as it has been previously enabled.

**Important!** **No** changes will be made to the way users sign in at this point.

1. On the Azure AD Portal, verify that that **Federation** continues to be **Enabled** and now **Seamless single sign on** is **Enabled**.



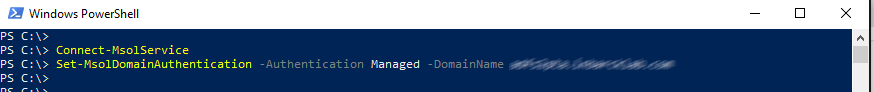
#### Convert Domains from Federated to Managed

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 to force user authentication via Password Hash Synchronization.

**Important!** 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 the domain has been converted to Managed by running the following command:

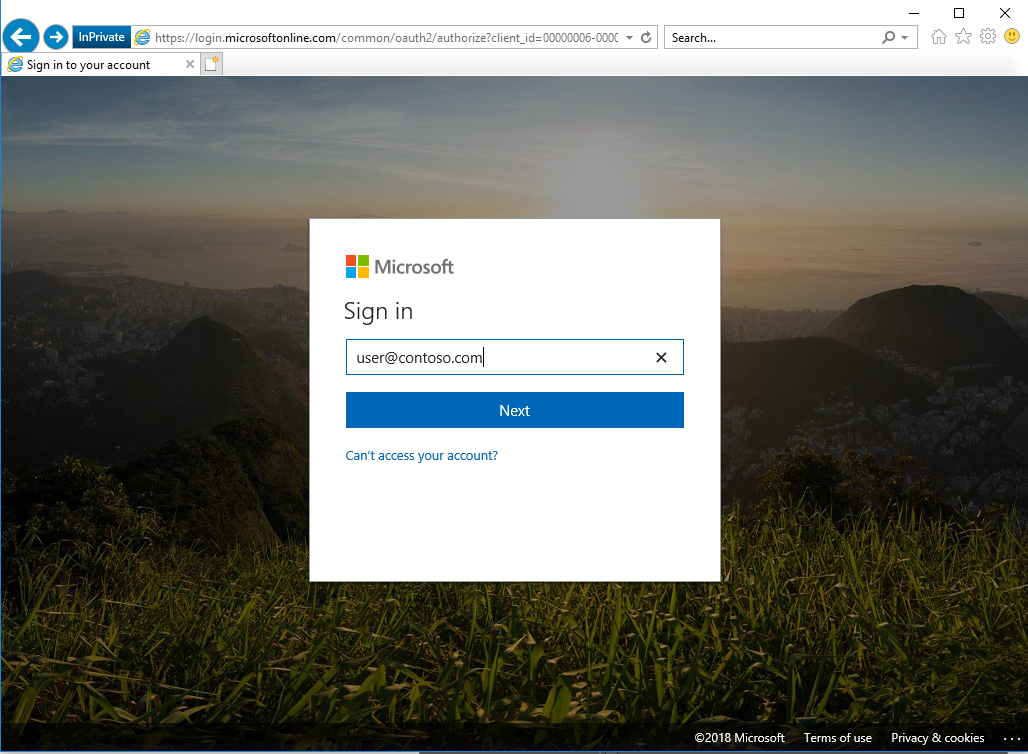
Get-MsolDomain -DomainName <domainname>

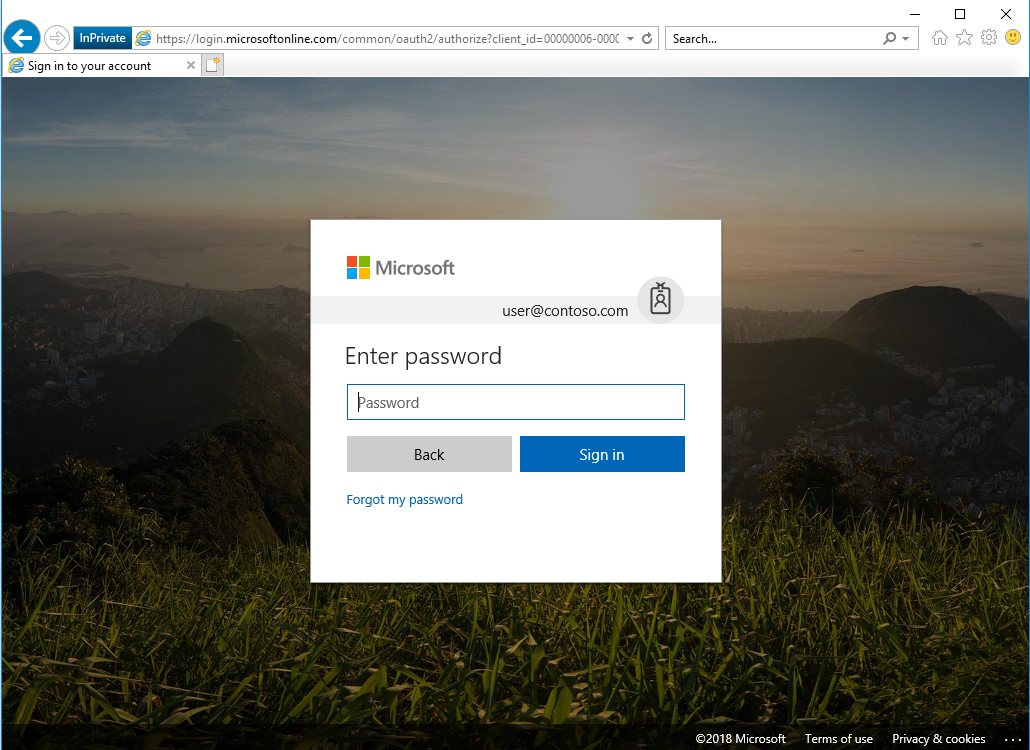
## Testing and Next Steps

### Test Authentication with Password Hash Synchronization

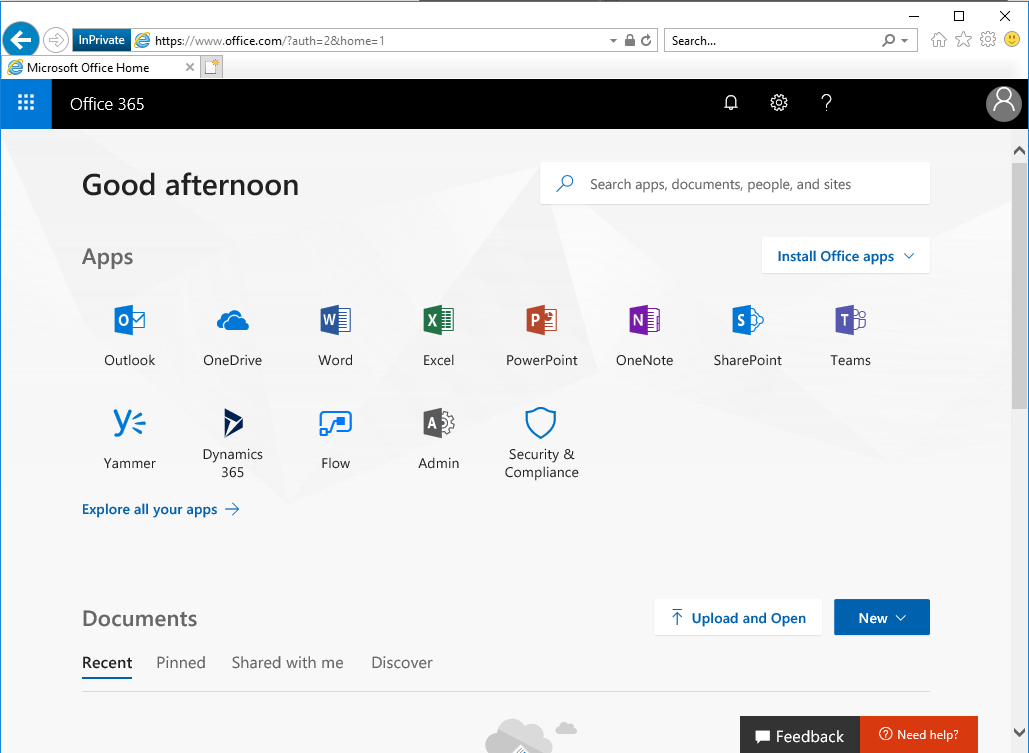
When your tenant was using federation, users were getting redirected from the Azure AD login page to your AD FS environment. Now that the tenant is configured to use Password Hash Synchronization instead of federation, users will not get redirected to AD FS and instead will login directly through the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





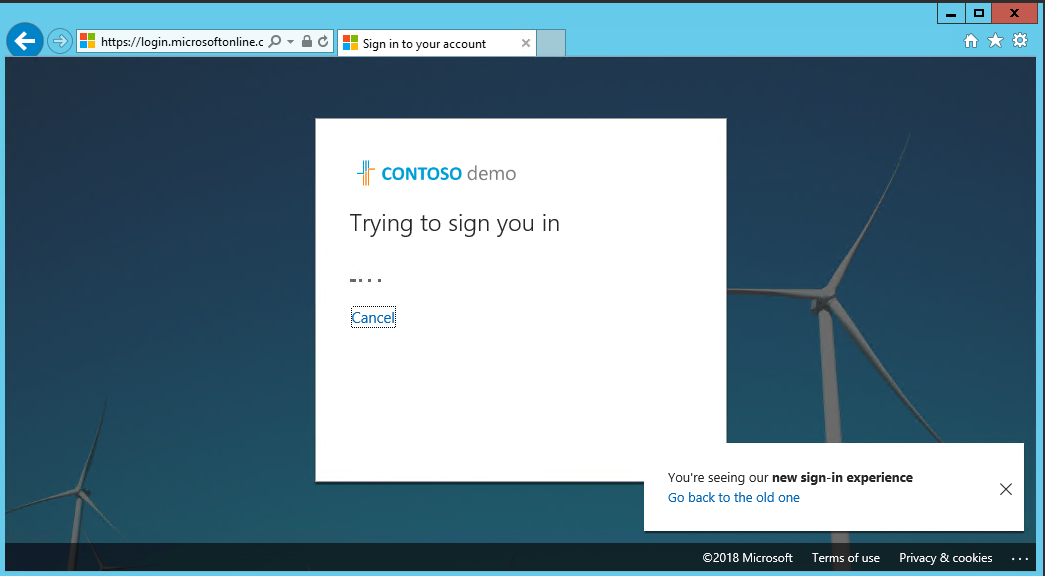
Once you type the password, you should get redirected to the Office 365 portal.



### Test Seamless single sign on

Login to a domain joined machine that is connected to the corporate network. Open **Internet Explorer** 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.

### Troubleshooting

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 Password Hash Synchronization](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-troubleshoot-password-hash-synchronization)

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

If users are experiencing authentication issues with any legacy authentication protocol flows such as with Exchange ActiveSync, or Outlook 2010, or if Admin initiated Self Service Password Resets for users is failing from the Azure AD portal then there is a single extra troubleshooting step that may be required, which is to perform a one-time user conversion process using the following cmdlet.

Convert-MsolFederatedUser -UserPrincipalName [pattifuller@contoso.com](mailto:pattifuller@contoso.com)

This command converts a federated user into a standard user but should only be required on an as-is troubleshooting basis only if you encounter the issues as described above. If this command fixes the issue, please contact Microsoft Support for guidance.

# Operations

This section describes the recommended task to be performed regularly on Password Hash Synchronization 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)?