

Azure Active Directory **Password Hash Synchronization**

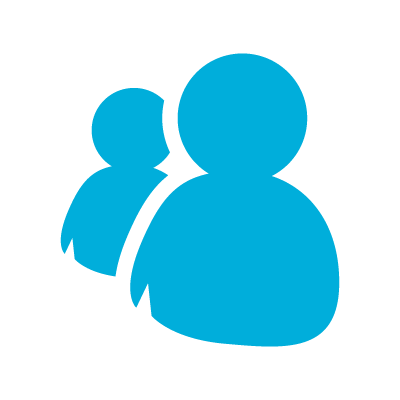
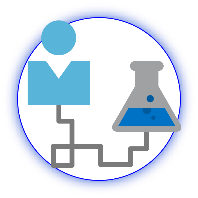
**How to use this guide**

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

Table of Contents

Contents

[Introduction 4](#_Toc518558512)

[Purpose of document 4](#_Toc518558513)

[What is Managed Authentication? 4](#_Toc518558514)

[What is Managed Authentication with Password Hash Synchronization? 4](#_Toc518558515)

[What is Seamless Single Sign-on? 4](#_Toc518558516)

[Goals for Password Hash Synchronization with Seamless Single Sign-on 5](#_Toc518558517)

[Planning for Password Hash Synchronization 6](#_Toc518558518)

[Understanding Password Hash Synchronization 6](#_Toc518558519)

[Password Hash Synchronization Considerations 8](#_Toc518558520)

[Update Azure AD Connect 9](#_Toc518558521)

[Password Hash Synchronization required permissions 9](#_Toc518558522)

[Plan Seamless SSO 9](#_Toc518558523)

[Plan Logging and Auditing 10](#_Toc518558524)

[Planning Deployment and Support 10](#_Toc518558525)

[Plan Change Communications 10](#_Toc518558526)

[Test Planning 12](#_Toc518558527)

[Implementing Your Solution 12](#_Toc518558528)

[Solution Components 12](#_Toc518558529)

[Step 1 – Configure sign-in method to Password Hash Synchronization 12](#_Toc518558530)

[Validate Password Hash Synchronization has completed successfully 12](#_Toc518558531)

[Step 2 – Prepare for Seamless SSO 13](#_Toc518558532)

[Step 3 – Enable Seamless SSO 13](#_Toc518558533)

[Testing and Next Steps 16](#_Toc518558534)

[Test Authentication with Password Hash Synchronization 16](#_Toc518558535)

[Test Seamless single sign on 18](#_Toc518558536)

[Troubleshooting 19](#_Toc518558537)

[Operations 19](#_Toc518558538)

[Roll over the Seamless SSO Kerberos decryption 19](#_Toc518558539)

# Introduction

## Purpose of document

This document describes the key considerations and processes involved to deploy Password Hash Synchronization and Seamless Single Sign-On for Microsoft 365 Business Customers.

## What is Managed Authentication?

Managed Authentication describes a system in which authentication is driven by Azure Active Directory, with a minimal on-premises footprint. 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.

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

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**  Password Hash Synchronization with Seamless SSO enables us to take advantage of user authentication at cloud scale. 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. |
|  |  |

## 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**.

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

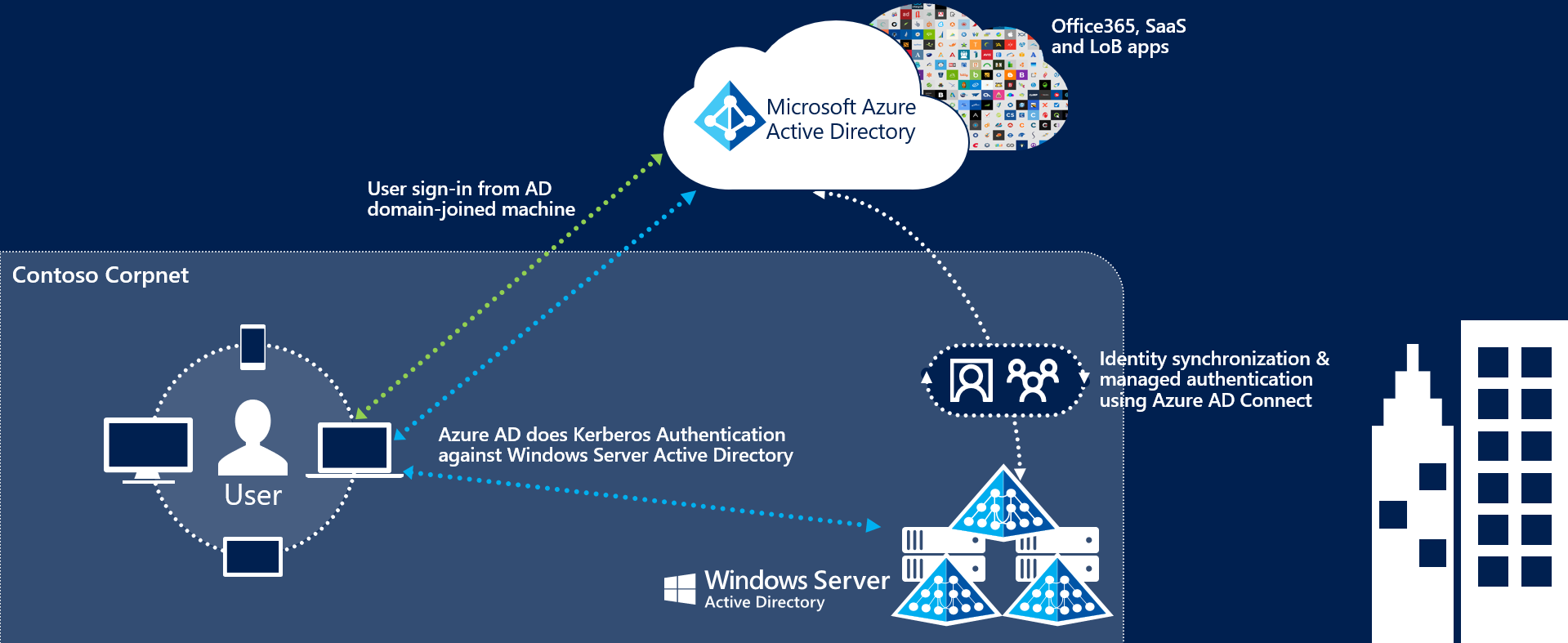
Now is a good time to validate these permissions are in place for all domains in the forest.

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 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 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 – Configure sign-in method to Password Hash 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.

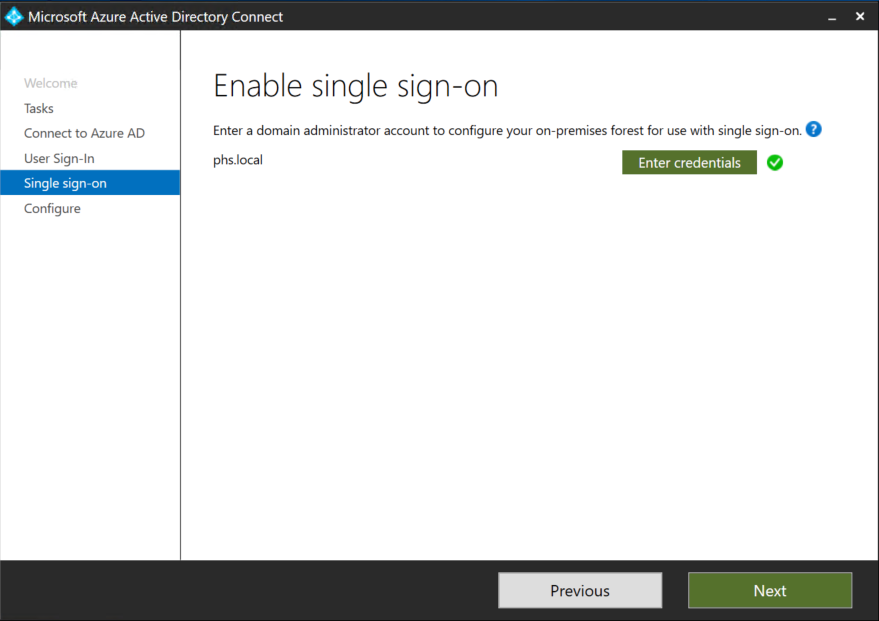
Follow the steps on the following article to make the required changes to your devices.

<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 – Enable Seamless SSO

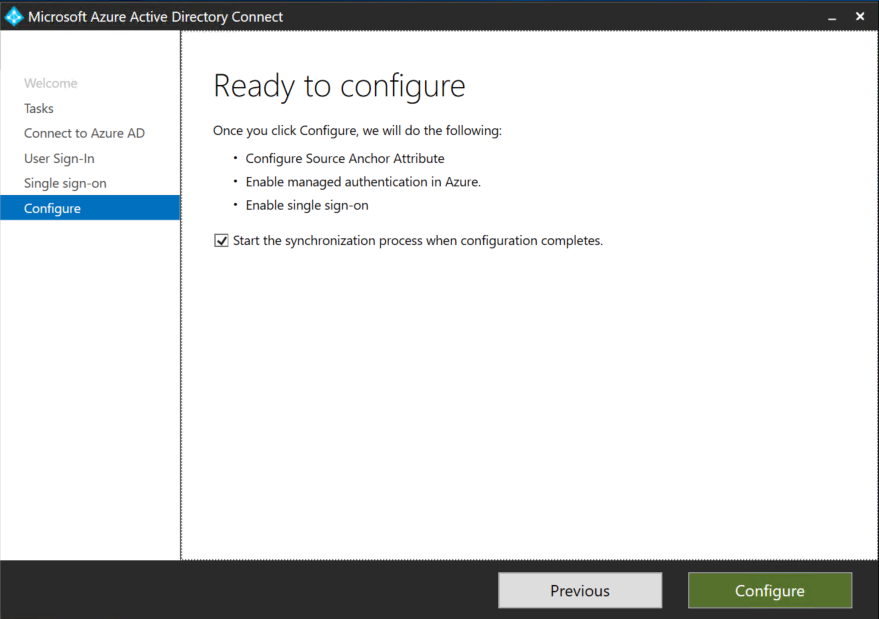
1. In the **User Sign-in** screen, select the radio **Password Hash Synchronization,** and make sure to check the box **Do not convert user accounts** as this is a deprecated step and will be removed from a future version of AAD Connect. Also select **Enable single sign-on** then select **Next.**
2. 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

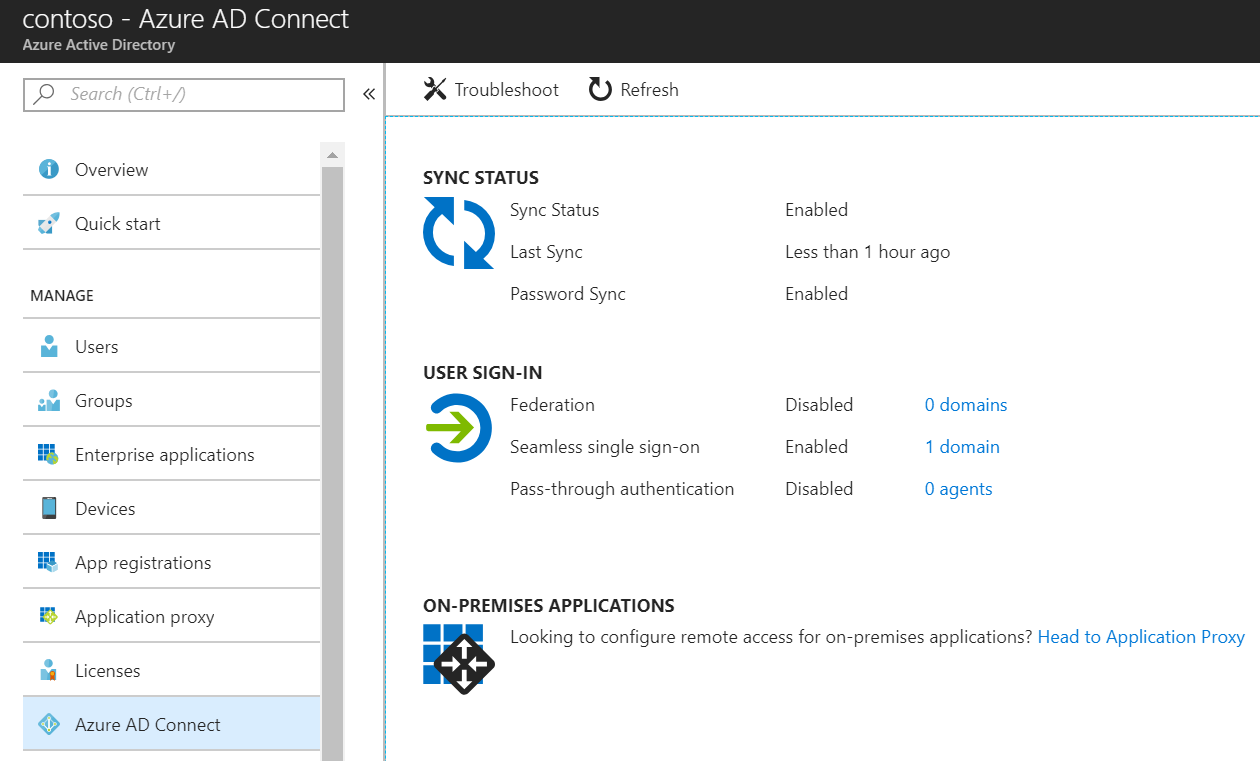
* A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
* The computer account's Kerberos decryption key is shared securely with Azure AD.
* In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that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



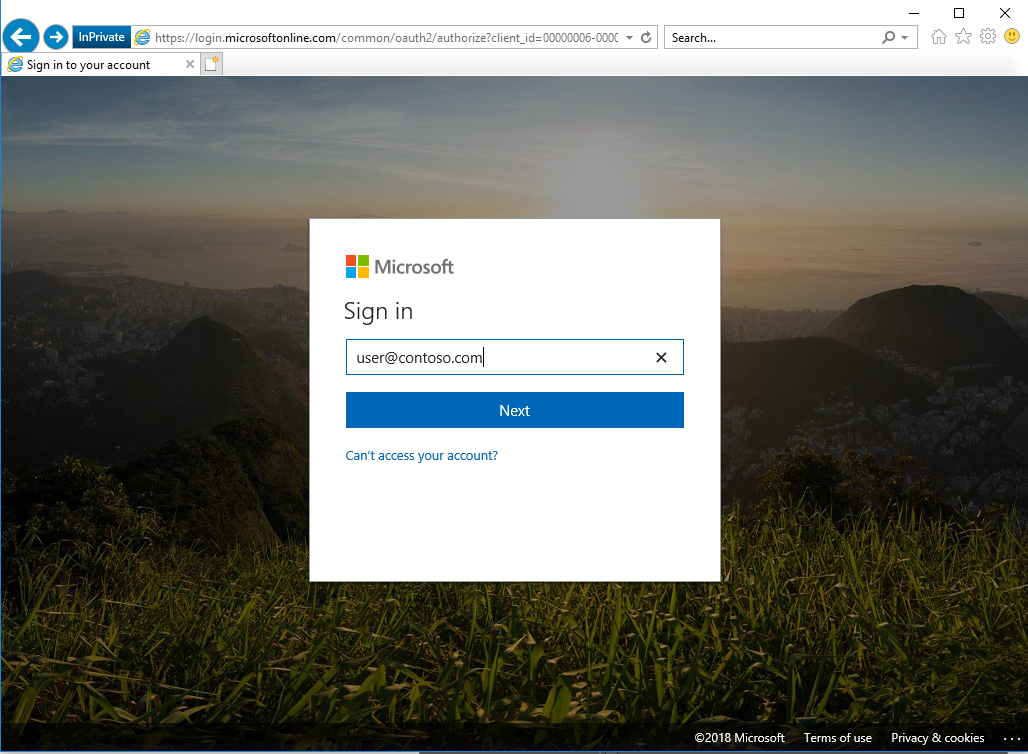
1. Go to [**Testing and Next Steps**](#_Next_Steps_and).

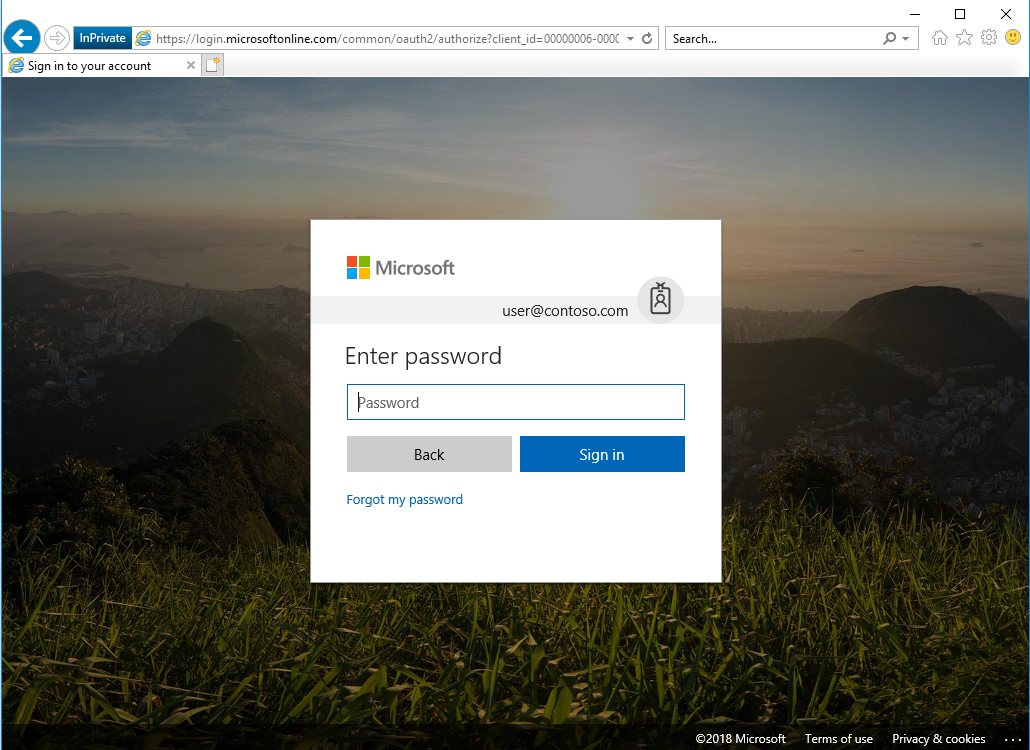
## Testing and Next Steps

### Test Authentication with Password Hash Synchronization

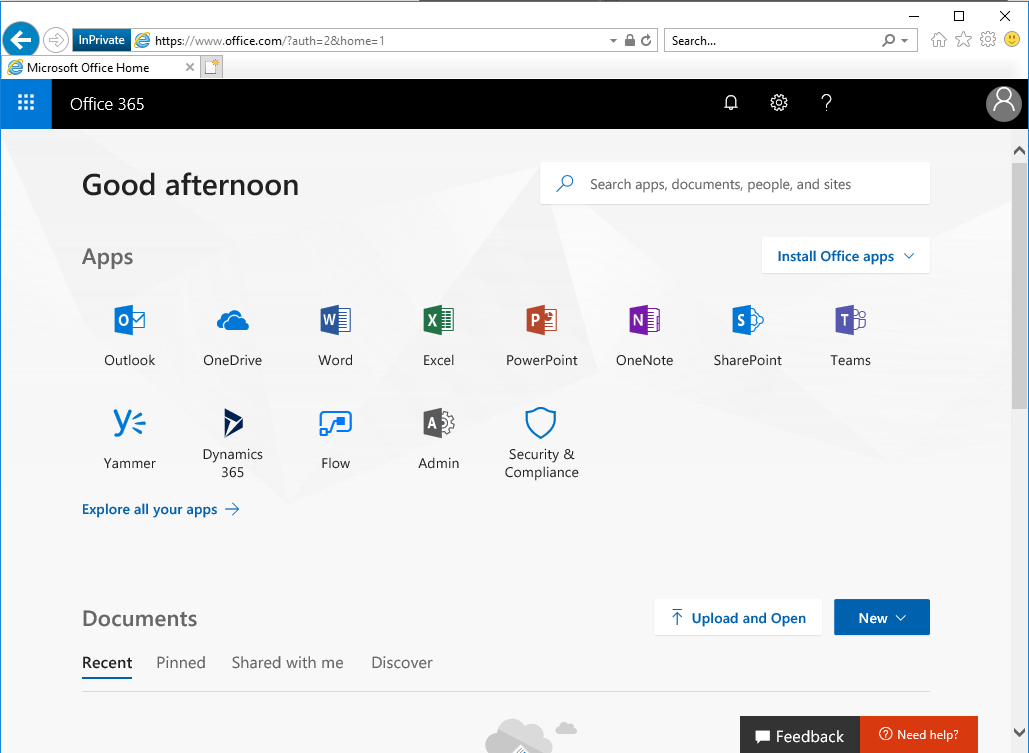
Users will login directly through the Azure AD Login page.

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.





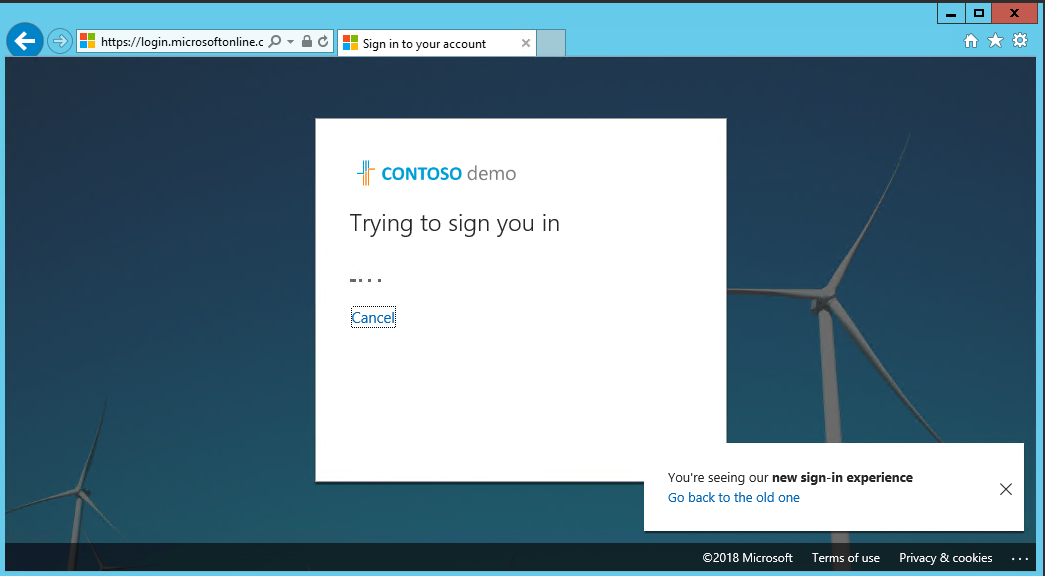
Once you type the password, you should get redirected to the Office 365 portal.



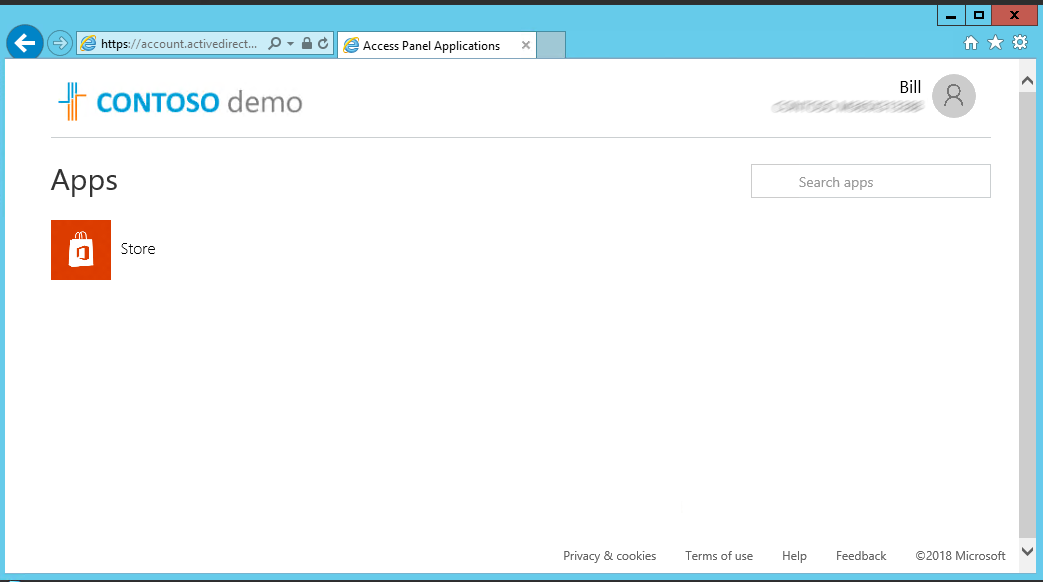
### Test Seamless single sign on

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.

### 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)?