

Azure Active Directory **Pass-Though Authentication**

**How to use this guide**

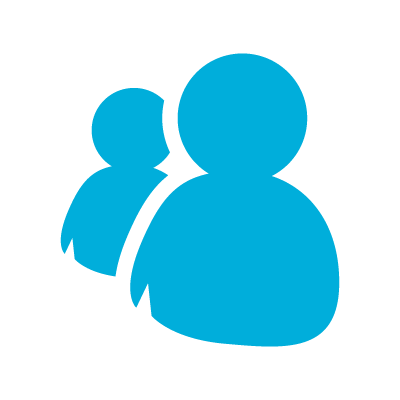
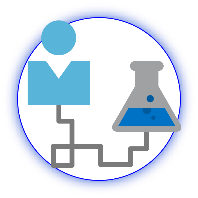
This step-by-step guide walks through the implementation of Pass Through

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

**3**

**[Implement](#_Implementing_Your_Solution)**

[Your solution](#_Implementing_Your_Solution)



**1**

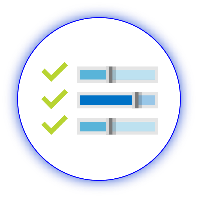
**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_your_Deployment)**

[Your project](#_Planning_your_Deployment)



**4**

**[Manage](#_Manage_your_solution)**

[Your implementation](#_Manage_your_solution)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

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

© 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 5](#_Toc518559034)

[Purpose of document 5](#_Toc518559035)

[What is Managed Authentication? 5](#_Toc518559036)

[What is Managed Authentication with Pass-Through Authentication? 5](#_Toc518559037)

[What is Seamless Single Sign-on? 5](#_Toc518559038)

[Goals for Pass-through Authentication with Seamless Single Sign-on 6](#_Toc518559039)

[Project Scope 7](#_Toc518559040)

[Prerequisites 7](#_Toc518559041)

[In scope 7](#_Toc518559042)

[Out of scope 7](#_Toc518559043)

[Unsupported Scenarios 8](#_Toc518559044)

[Understanding Pass-through Authentication 9](#_Toc518559045)

[Planning for Pass-through Authentication 9](#_Toc518559046)

[Update Azure AD Connect 10](#_Toc518559047)

[Plan Authentication Agent Number and Placement 10](#_Toc518559048)

[Planning for Smart Lockout 11](#_Toc518559049)

[Plan for Modern Authentication 11](#_Toc518559050)

[Plan Seamless SSO 12](#_Toc518559051)

[Plan Logging and Auditing 12](#_Toc518559052)

[Planning Deployment and Support 13](#_Toc518559053)

[Plan Change Communications 13](#_Toc518559054)

[Test Planning 15](#_Toc518559055)

[Implementing Your Solution 15](#_Toc518559056)

[Solution Components 15](#_Toc518559057)

[Step 1 – Prepare for Seamless SSO 15](#_Toc518559058)

[Step 2 – Configure Pass-Through Authentication and enable Seamless SSO 16](#_Toc518559059)

[Testing and Next Steps 20](#_Toc518559060)

[Test Pass-through Authentication 20](#_Toc518559061)

[Test Seamless single sign on 22](#_Toc518559062)

[Support Planning 24](#_Toc518559063)

[Manage your solution 25](#_Toc518559064)

[Roll over the Seamless SSO Kerberos decryption 25](#_Toc518559065)

[Monitoring and logging 25](#_Toc518559066)

# Introduction

## Purpose of document

This document describes the key considerations and processes involved to deploy Pass-Through Authentication and Seamless Single Sign-On in Microsoft 365 Business

## What is Managed Authentication?

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

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

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

## What is Managed Authentication with Pass-Through Authentication?

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

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

For a deeper technical and security explanation, see the [Security deep dive](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-security-deep-dive) article.

## What is Seamless Single Sign-on?

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

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

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

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

# Project Scope

## Prerequisites

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

* The latest build of AAD Connect is installed. For more information see the [Update Azure AD Connect](#_Update_Azure_AD) section.
* Port 80/443 outbound is allowed from the AAD Connect server and any other servers where you plan to install the PTA agent.
* Specific public target FQDN’s are whitelisted on your firewall/proxy, and are resolvable for the PTA agents to install, register, and communicate successfully with Azure AD. Specific network requirements for the PTA agents are detailed [here](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-quick-start#in-your-on-premises-environment).
* The servers where you will install the PTA agents on are running Windows Server 2012R2 or Windows Server 2016.
* An Azure Global Administrator account is available to configure PTA in your tenant and migrate from federated to managed.
* A Domain Administrator account is available to configure Seamless SSO in the on-premises Active Directory.
* Modern Authentication is enabled in your Office 365 tenant for both Exchange Online and Skype for Business Online. Please refer to [this](https://support.office.com/en-us/article/Enable-or-disable-modern-authentication-in-Exchange-Online-58018196-f918-49cd-8238-56f57f38d662) article for steps on enabling Modern Authentication.
* Modern Authentication is enabled for any Office 2013 clients.

## In scope

The following are in scope for this project:

**Enabling Pass-through Authentication**

* Configure the user sign-in method through Azure AD Connect
* Installing the pass-through authentication agent(s)

**Enabling Seamless SSO**

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

**Deployment and Support**

* Testing and validation steps
* Troubleshooting

## Out of scope

The following are out of scope of this project:

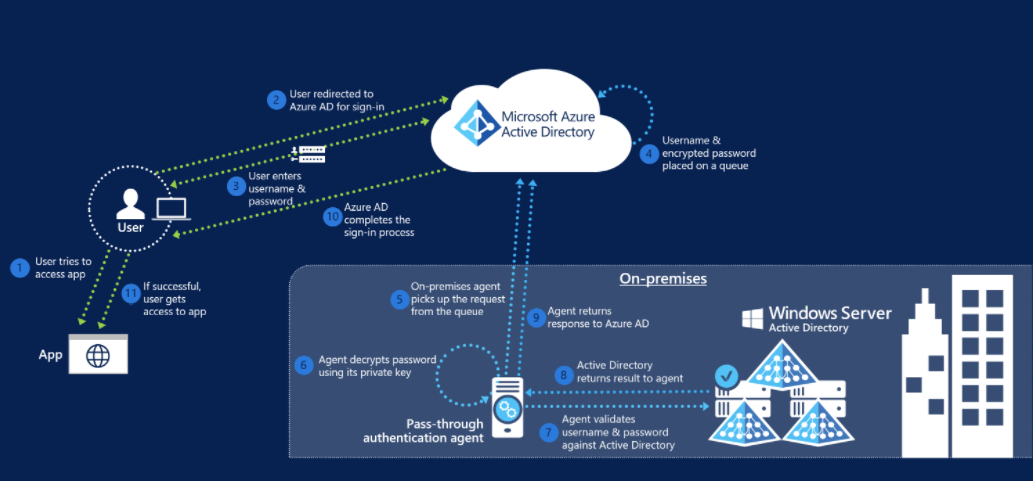
* Deployment of Azure AD Connect
* Migrating any AD FS custom claims authorization rules to conditional access policies
* Configuring Multi-factor authentication (Azure MFA)
* Assigning licenses to users
* Providing detailed backup and restoration steps for AD FS
* Configuring Hybrid Azure AD join

### Unsupported Scenarios

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

## Understanding Pass-through Authentication

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



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

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

## Planning for Pass-through Authentication

### Update Azure AD Connect

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

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

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

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

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

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

### Plan Authentication Agent Number and Placement

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

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

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

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

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

If performance is a concern for your Azure AD Connect server, or if you wish to prevent the agent installed on it from servicing any authentication requests then the agent services, “Microsoft Azure AD Connect Authentication Agent” and “Microsoft Azure AD Connect Agent Updater”, can be safely disabled provided you have successfully installed at least another agent on a server elsewhere in your environment. Record your plan below.

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

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

## Planning for Smart Lockout

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

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

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

For more information on Smart Lockout feature and how to edit its configuration please refer to [this document.](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-smart-lockout)

If you don’t have an [account lockout threshold](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold) group policy set today in Active Directory, then there is no requirement for you to edit the Smart Lockout behavior and you can safely go with the default settings and still stay protected. If you have an on-premises Group Policy object that locks accounts after fewer than 10 failed password attempts, an Azure AD P2 license is required for a single Global Administrator account so that they can edit Smart Lockout settings in Azure AD to tune it to your environment and prevent unintended lockouts resulting from pass-through authentication requests.

## Plan for Modern Authentication

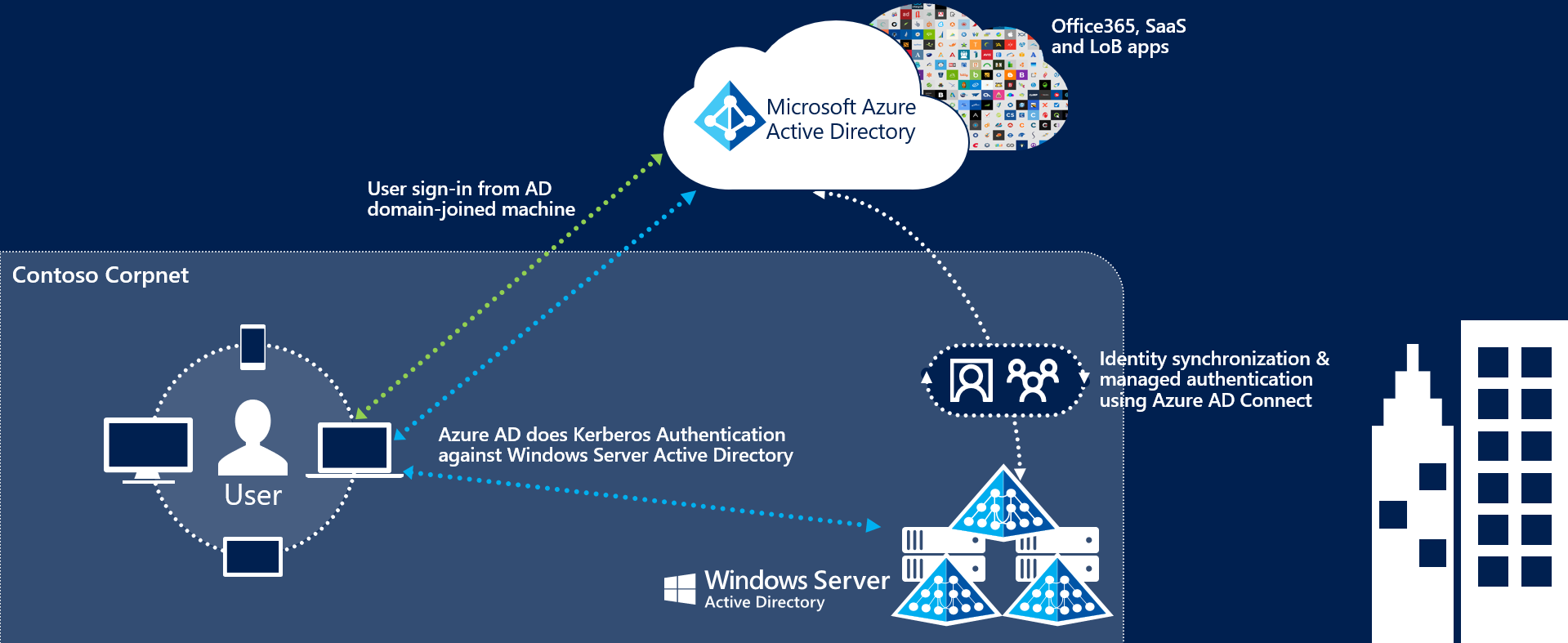
While pass-through authentication does support authenticating certain legacy clients (Exchange ActiveSync, Outlook 2010/2013 etc.) organizations are encouraged to switch to modern authentication, if possible. Modern authentication brings Active Directory Authentication Library (ADAL)-based sign-in to Office client apps across platforms. This enables sign-in features such as Multi-Factor Authentication (MFA), smart card and certificate-based authentication, and it removes the need for Outlook to use the basic authentication protocol. Modern authentication allows for Pass-through Authentication support. It also helps you secure your user accounts by using conditional access features. To verify that your Office 365 tenant is configured for modern authentication please refer to this article:

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

* **Microsoft Recommends** enabling Modern Authentication

## Plan Seamless SSO

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



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

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

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

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

## Plan Logging and Auditing

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

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

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

## Planning Deployment and Support

### Plan Change Communications

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

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

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

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

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

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

### Test Planning

In this section, document how you will test during the 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 PTA | From a non-domain joined PC or any device connected to an external network, navigate to myapps.microsoft.com/contoso.com | The user should see the Azure AD login page where they will have to enter in both a username and password. They should be successfully signed. |
| Verify Exchange ActiveSync | On a mobile device, configure the ActiveSync client. | The user will need to enter in both a username and password. The ActiveSync client will be using the PTA flow. |

# Implementing Your Solution

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

## Solution Components

Implementation includes the following components:

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

## Step 1 – Prepare for Seamless SSO

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

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

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

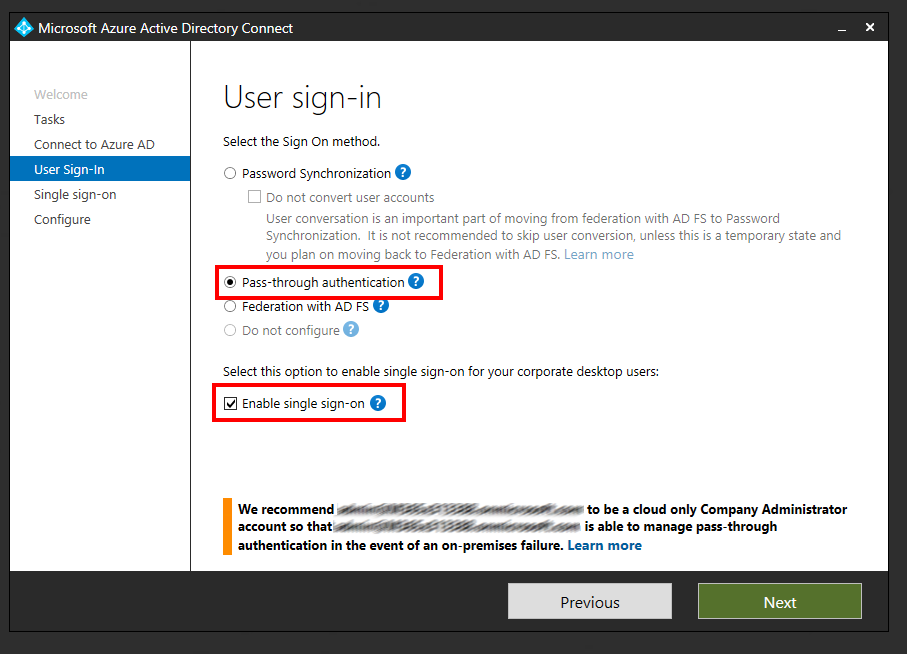
<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-quick-start#step-3-roll-out-the-feature>

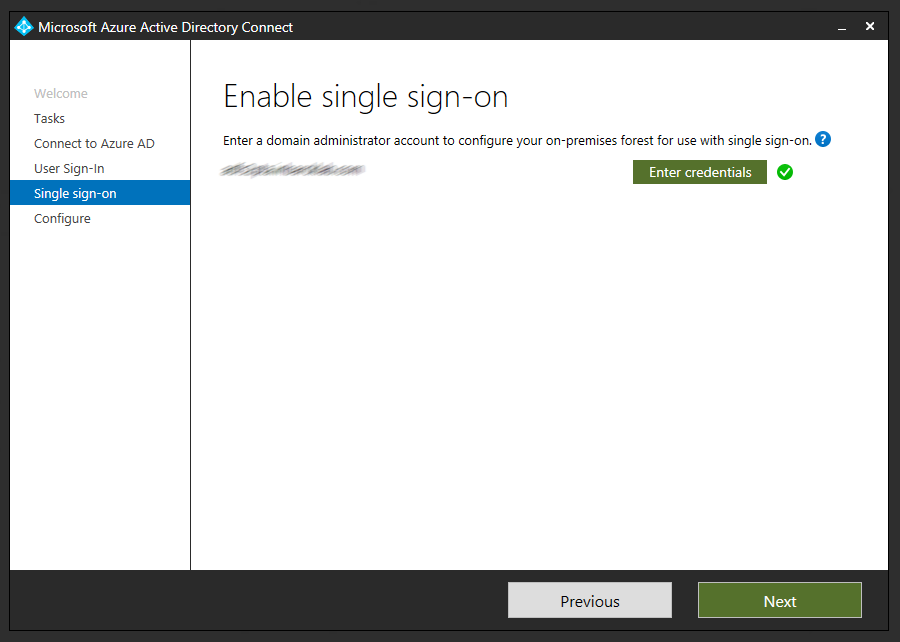
**Important!** Making this change won’t modify the way your users sign in to Azure AD. However, it’s important this configuration is applied to all your devices before you continue with the Step 3. Also note that users signing in on devices that have not received this configuration will simply need to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

## Step 2 – Configure Pass-Through Authentication and enable Seamless SSO

#### Configure user Sign in method

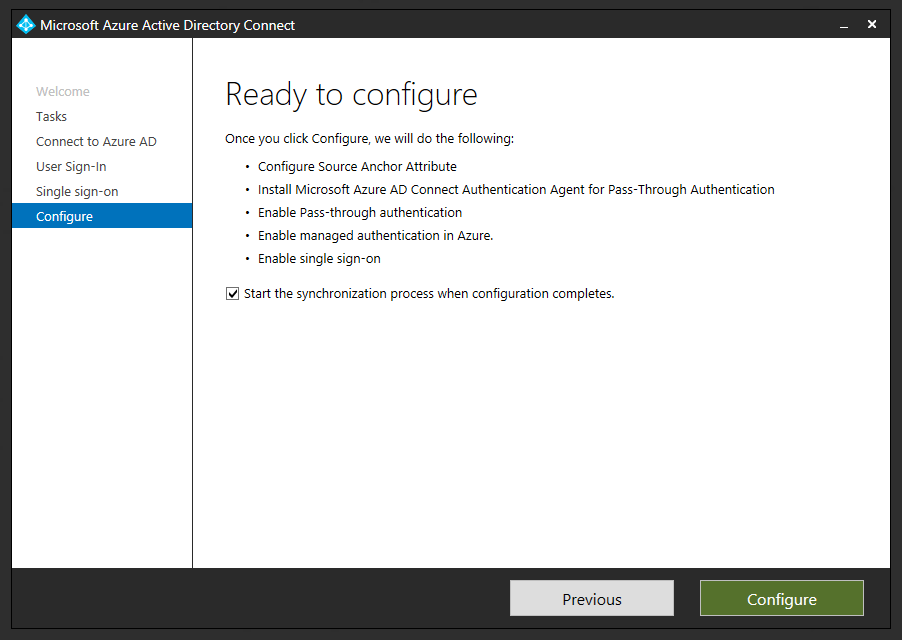
1. On the Azure AD Connect Server, open the wizard.
2. Select **Change User Sign in** and then select **Next**.
3. In the **Connect to Azure AD** screen provide the username and password of a Global Administrator.
4. The **User Sign-in** screen, change the radio button from **Federation with AD FS**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

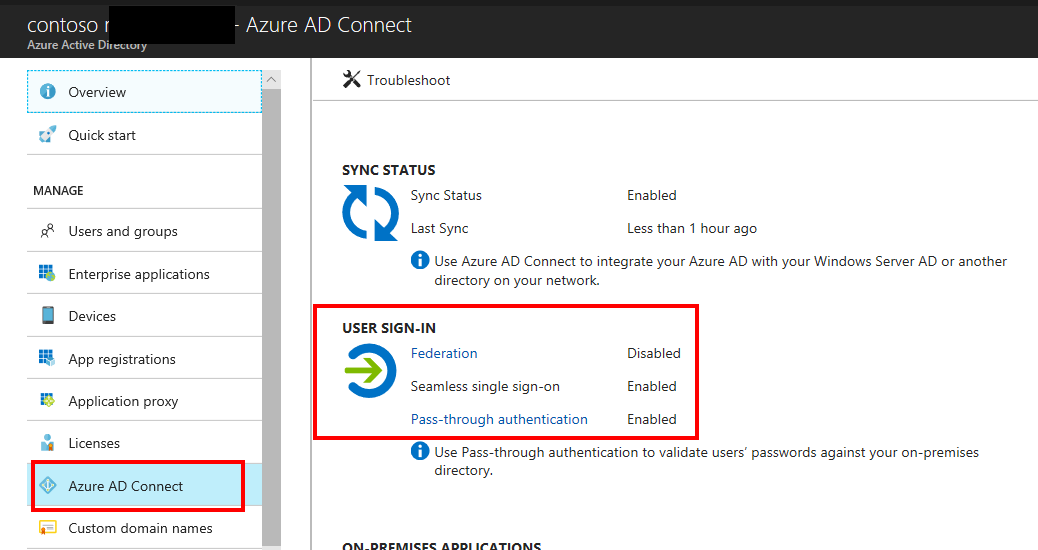


1. In **Enable Single Sign-on** screen, enter the credentials of Domain Administrator account, then select **Next**.  
   

**Note**: Domain Administrator credentials are required for enabling Seamless Single Sign-on as the process performs the following actions which require these elevated permissions. The domain administrator credentials are not stored in Azure AD Connect or in Azure AD. They're used only to enable the feature and then discarded after successful completion

* A computer account named AZUREADSSOACC (which represents Azure AD) is created in your on-premises Active Directory (AD).
* The computer account's Kerberos decryption key is shared securely with Azure AD.
* In addition, two Kerberos service principal names (SPNs) are created to represent two URLs that are used during Azure AD sign-in.
* The domain administrator credentials are not stored in Azure AD Connect or in Azure AD. They're used only to enable the feature and then discarded after successful completion

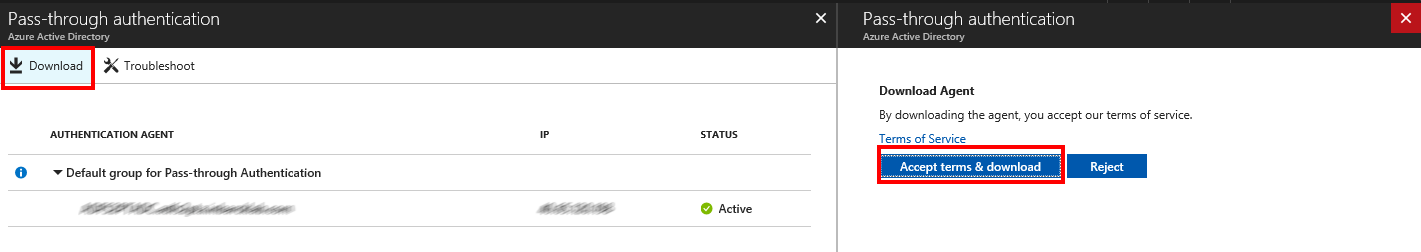
1. In the **Ready to Configure** screen, make sure “**Start Synchronization process when configuration completes**” checkbox is selected. Then select **Configure**.  
   
2. Open the **Azure AD portal**, select **Azure Active Directory**, and then select **Azure AD Connect**.
3. Verify that that **Federation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



#### Deploy Additional Authentication Agents

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

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

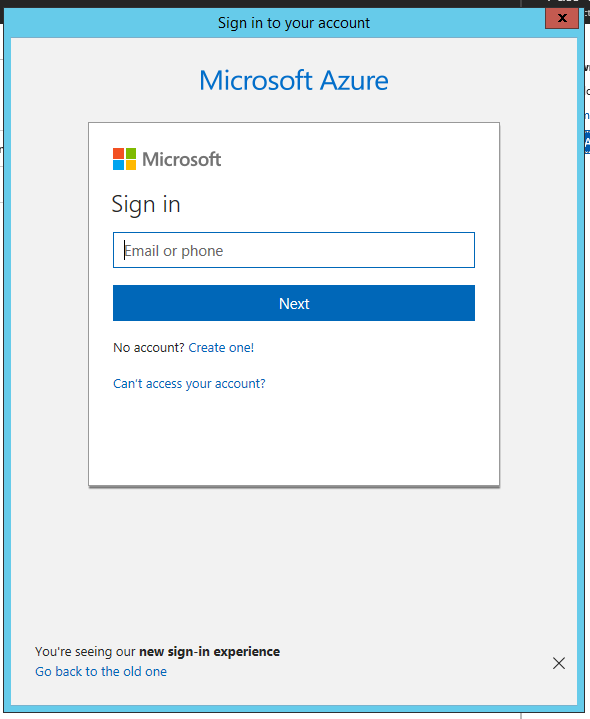


The download of additional authentication agents will begin. Install the secondary Authentication Agent on a domain-joined server.

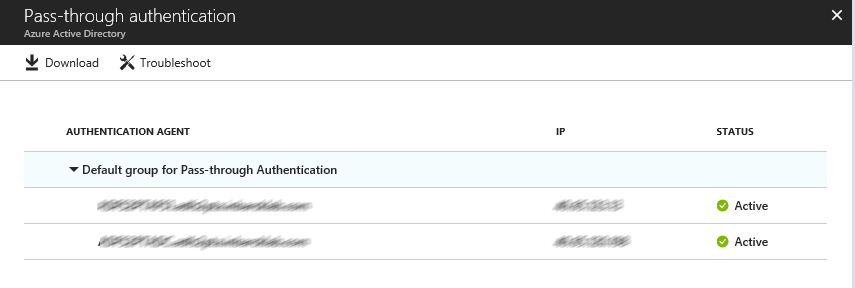
***NOTE:*** the first agent is always installed on the Azure AD Connect server itself as part of the configuration changes made in the User Sign In section of the Azure AD Connect tool. Any additional Authentication Agents should be installed on a separate server. It is recommended to have between 2-3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

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





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



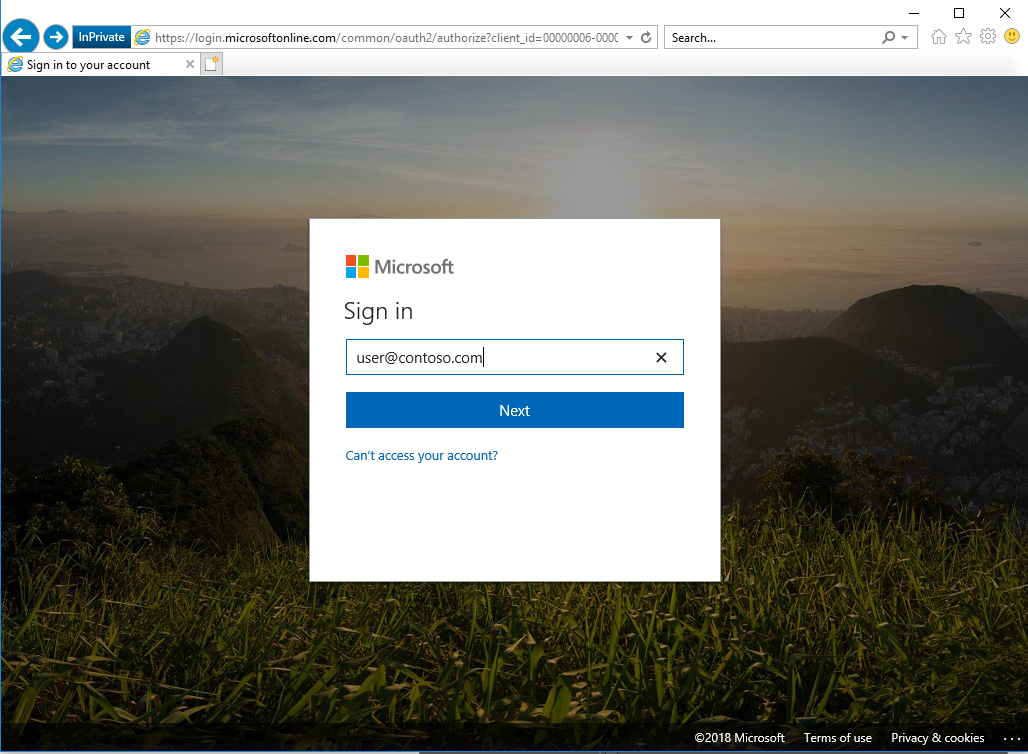
Go to [**Testing and Next Steps**](#_Next_Steps_and).

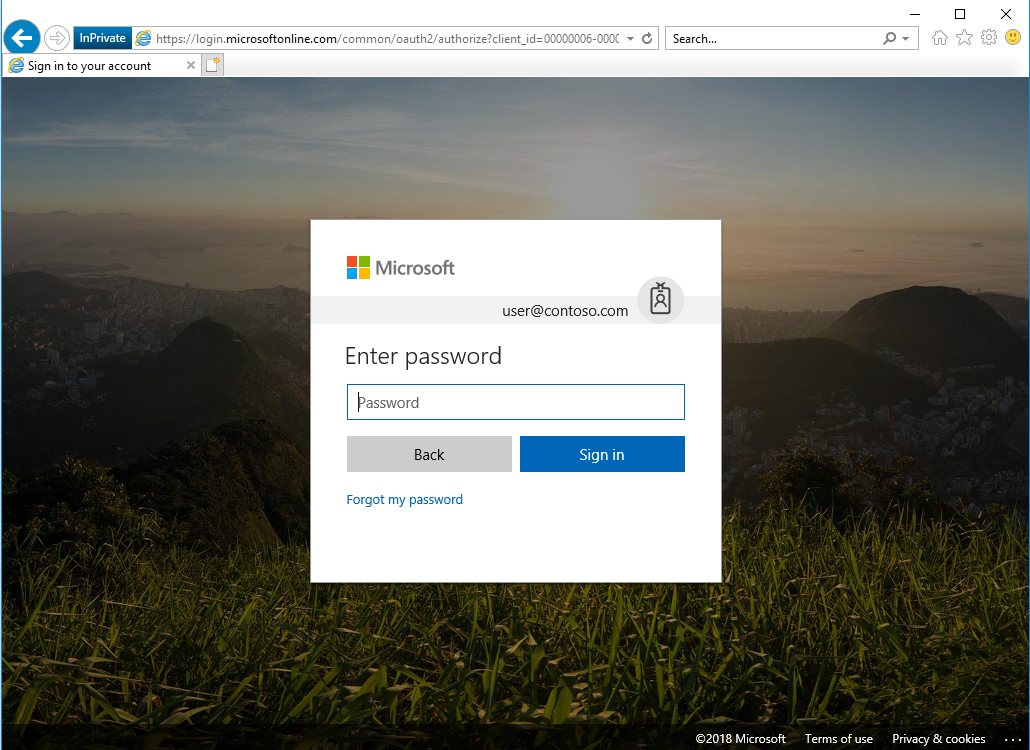
## Testing and Next Steps

### Test Pass-through Authentication

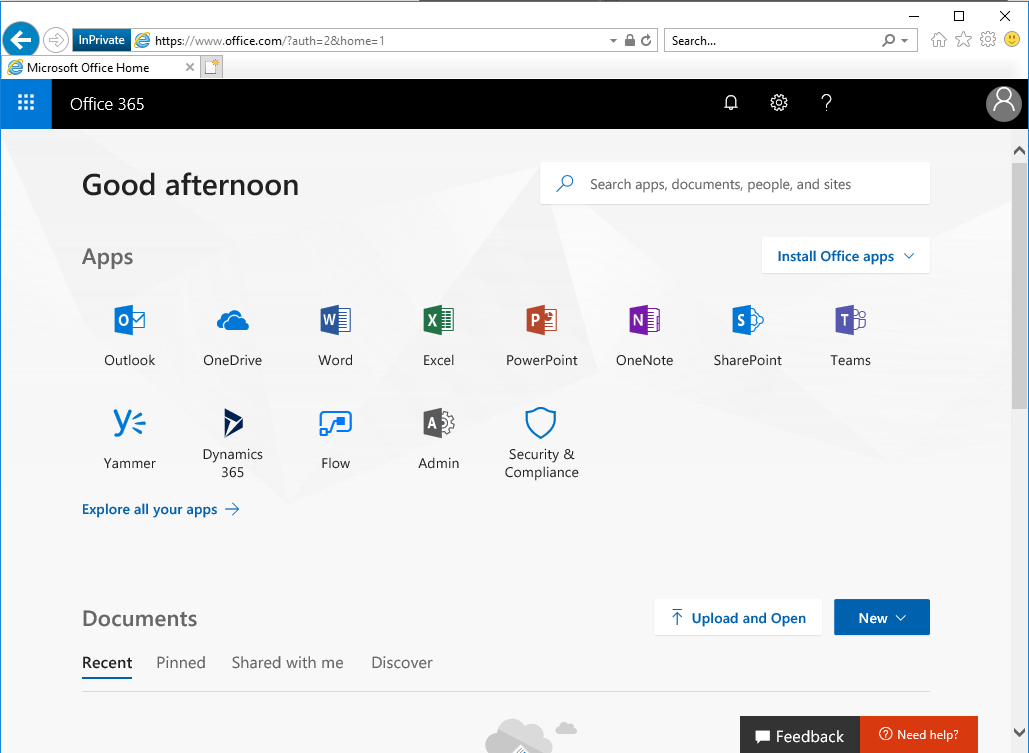
When your tenant was using federation, users were getting redirected from the Azure AD login page to your AD FS environment. Now that the tenant is configured to use Pass-through Authentication instead of federation, users will not get redirected to AD FS and instead will login directly through the Azure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

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





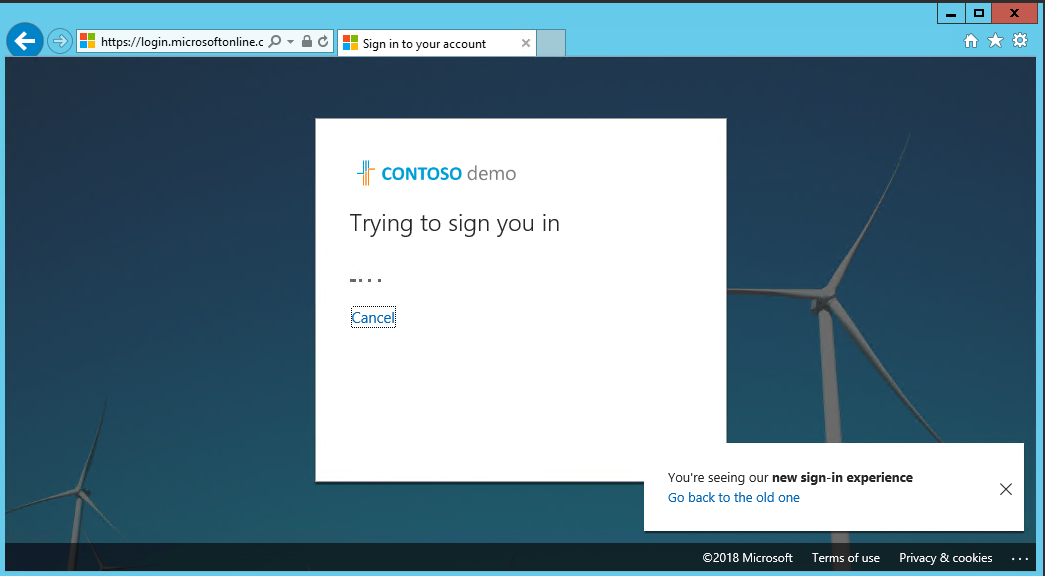
Once you type the password, you should get redirected to the Office 365 portal.



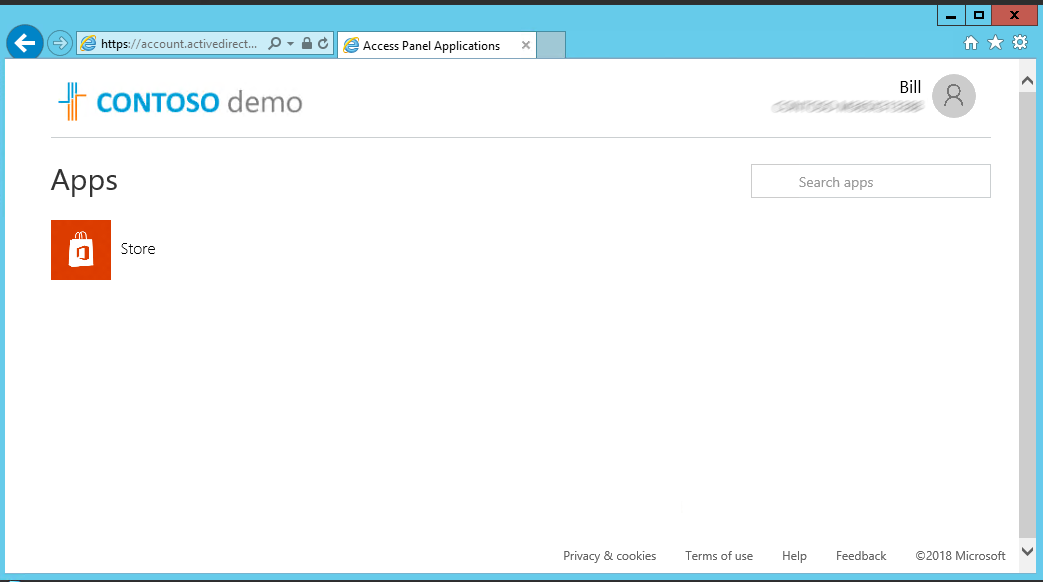
### Test Seamless single sign on

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

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



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



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

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

### Support Planning

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

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

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

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.

# Manage your solution

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

## Roll over the Seamless SSO Kerberos decryption

It is important to frequently roll over the Kerberos decryption key of the AZUREADSSOACC computer account (which represents Azure AD) created in your on-premises AD forest. We highly recommend that you roll over the Kerberos decryption key at least every 30 days to align with how Active Directory domain members submit password changes. As there is no associated device attached to the AZUREADSSOACC computer account object the roll over needs to be performed manually.

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

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

## Monitoring and logging

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

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

Troubleshooting logs can be enabled if required.

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

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