

Azure Active Directory **Seamless Single Sign-On** Deployment Plan

**How to use this guide**

This step-by-step guide walks through the implementation of Seamless Single Sign-On in a five-step process. The links below take you to each of those steps.



**1**

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

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_Your_Implementation)**

[Your project](#_Planning_Your_Implementation)

**3**

**[Design](#_Design_Considerations)**

[Policies and integration](#_Design_Considerations)

**5**

**[Manage](#_Operationalize_your_Implementation)**

[Your implementation](#_Operationalize_your_Implementation)



**4**

**[Implement](#_Implementing_Seamless_Single)**

[Your design](#_Implementing_Seamless_Single)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

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

Table of Contents

Table of Contents

[Business Value of Seamless Single Sign-On (SSO) 2](#_Toc520921499)

[Stakeholders and Sign-off 3](#_Toc520921500)

[Planning Your Implementation 4](#_Toc520921501)

[General Planning 4](#_Toc520921502)

[Tracking Timelines 4](#_Toc520921503)

[In Scope 4](#_Toc520921504)

[Out of scope 4](#_Toc520921505)

[Licensing 5](#_Toc520921506)

[Key Benefits 5](#_Toc520921507)

[Seamless SSO Supported Capabilities 5](#_Toc520921508)

[**What is the difference between the single sign-on experience provided by Azure AD Join and Seamless SSO?** 6](#_Toc520921509)

[Design Considerations 7](#_Toc520921510)

[Non-Microsoft Browser considerations 7](#_Toc520921511)

[Implementing Seamless Single Sign-on 8](#_Toc520921512)

[Ensure that the following prerequisites are in place: 8](#_Toc520921513)

[Before you roll out the feature 9](#_Toc520921514)

[**Why do you need to modify users' Intranet zone settings?** 9](#_Toc520921515)

[**Option 1: Group Policy** – Using this method will grey out the Trusted sites UI, this means the end user cannot add or remove any sites in the zone as shown below. 10](#_Toc520921516)

[**Option 2: Group Policy Preferences –** Using this option will ensure the users are still allowed to add any sites in to the respective zones. 14](#_Toc520921517)

[Enable the feature 18](#_Toc520921518)

[Operationalize your Implementation 22](#_Toc520921519)

[Purpose of Document 22](#_Toc520921520)

[Required Roles 22](#_Toc520921521)

[Verify Seamless SSO is enabled 22](#_Toc520921522)

[Test the Seamless Single Sign-on experience 23](#_Toc520921523)

[Roll over keys 24](#_Toc520921524)

[Helpful Documentation 25](#_Toc520921525)

# Business Value of Seamless Single Sign-On (SSO)

This document presents an executive summary of the business case for moving forward with enabling Azure Active Directory Seamless Single Sign-On for Password Hash Sync or Pass through Authentication Sign-In options.

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.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Increase.png | **INCREASE PRODUCTIVITY**  Enabling Azure Active Directory Seamless **single sign-on** for Password Hash Sync or Pass through authentication provides a superior log in experience for existing users, reducing or eliminating log on prompts when inside the corporate network using domain join computers. The user’s environment feels more cohesive and is less distracting without multiple prompts. | |  |  | |  |  | | A close up of a sign  Description generated with high confidence | **Easy to deploy & administer**  Turning on Azure Active Directory Seamless Single Sign-On requires no additional components. This works with any of the methods of cloud authentication - Password Hash Synchronization or Pass-through Authentication. This can be rolled out to some or all users using Group Policy. This will enable your organization to Register non-Windows 10 devices with Azure AD without the need for any AD FS infrastructure. This capability needs you to use version 2.1 or later of the workplace-join client. | |  |

# Stakeholders and Sign-off

The following section serves to identify all the stakeholders that are involved in the project and need to sign off, review, or stay informed. Add stakeholders to the table below as appropriate for your organization.

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

|  |  |  |
| --- | --- | --- |
| Name | Role | 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 | **Application Business Owner**  *A representative colleague who can provide input on the user experience and usefulness of this change from an end-user’s perspective and owns the overall business aspect of the application, which may include managing access.* | SO/I |
| Enter name and email | **Security Owner**  *A representative from the security team that can sign off that the plan will meet the security requirements of your organization.* | SO |

# 

# Planning Your Implementation

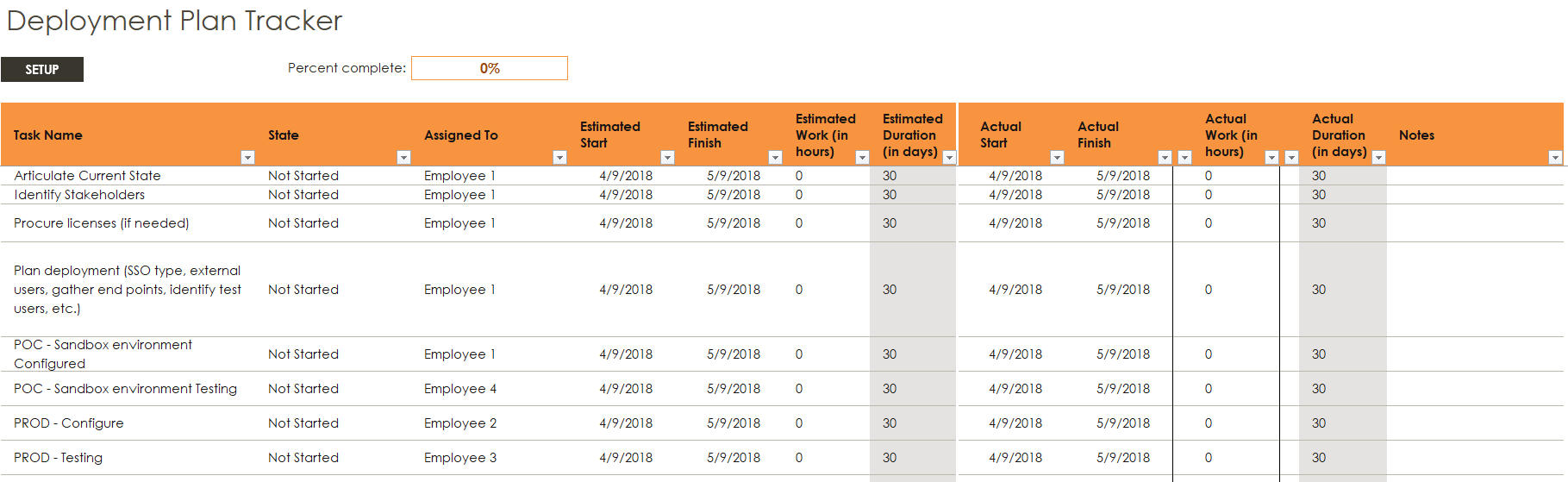
## General Planning

### Tracking Timelines

Tracking your plan is an important aspect of project success.

You may use the embedded Deployment Plan Tracker spreadsheet below to monitor and schedule your committed timelines for this project. Begin tracking additional items as you progress through the deployment plan that may require an action or prerequisite:





### In Scope

The following is in scope for this project:



**Seamless Single Sign-On**

* Enabling seamless single sign-on to your current sign-in option; Passthrough Authentication or Password Hash Sync.
* Implementation of new group policy settings to be rolled out to end users.
* Enabling the support organization to support and manage this new change, ensuring the right helpdesk processes are in place to ensure on-going end-user success.
* Documenting and testing a recovery plan.
* Approving a business continuity plan.
* Designing operational support for the production service.
* The following environments are in scope for this design:
  + Production
  + Test / QA

### Out of scope

The following are out of scope of this project:

* Troubleshooting the Group Policy health of the AD infrastructure before rolling out the policy settings required for seamless single sign-on.

### Licensing

#### Azure Active Directory Licensing

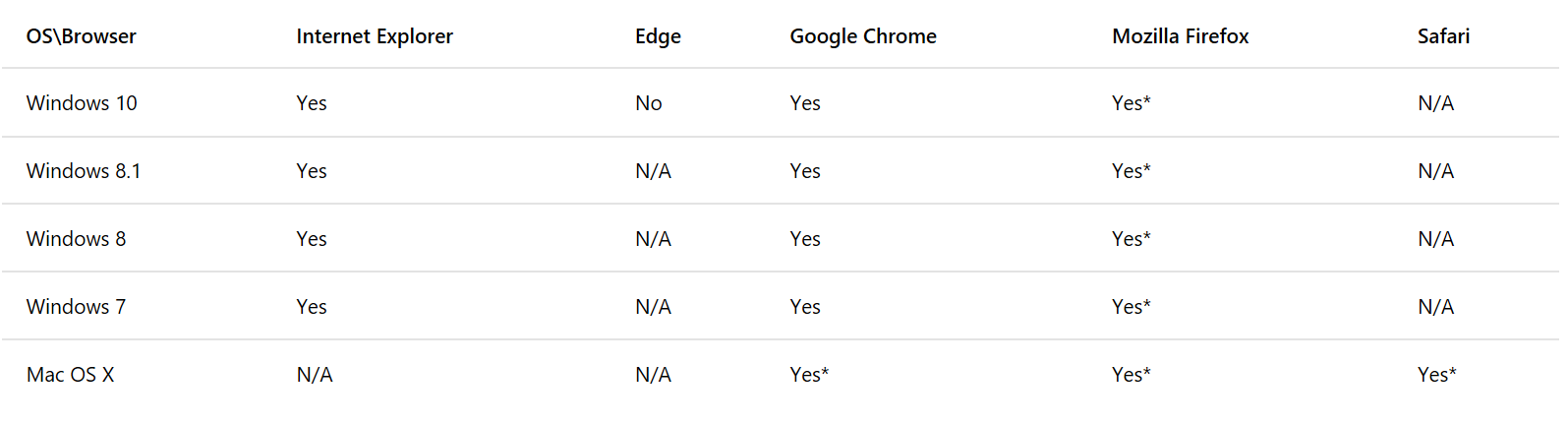
Enabling this feature does not require any special licensing scheme. This is a free feature as part of the Azure AD Connect tool.

# Key Benefits

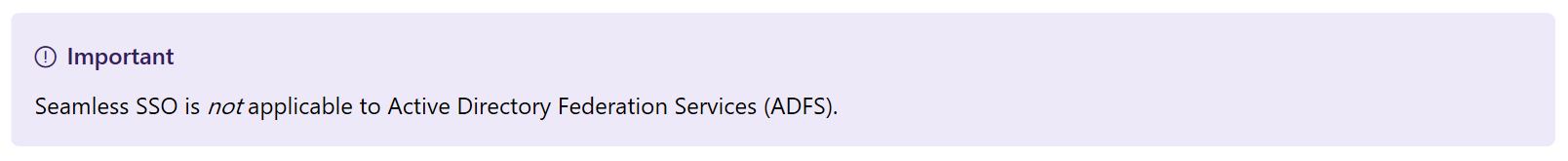
* Great user experience
  + Users are automatically signed into both on-premises and cloud-based applications.
  + Users don't have to enter their passwords repeatedly.
* Easy to deploy & administer
  + No additional components needed on-premises to make this work.
  + Works with any method of cloud authentication - [Password Hash Synchronization](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization) or [Pass-through Authentication](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication).
  + Can be rolled out to some or all your users using Group Policy.
  + Register non-Windows 10 devices with Azure AD without the need for any AD FS infrastructure. This capability needs you to use version 2.1 or later of the [workplace-join client](https://www.microsoft.com/download/details.aspx?id=53554).

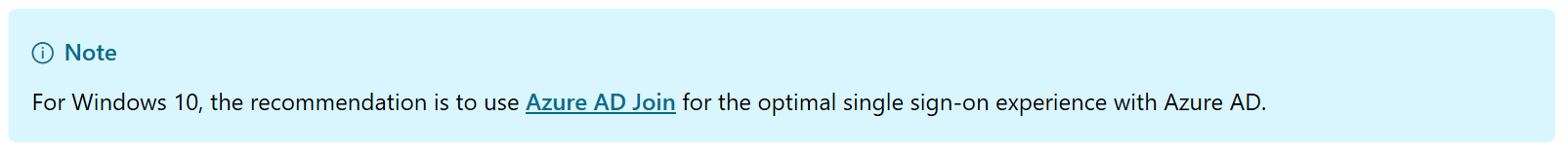
# Seamless SSO Supported Capabilities

* Sign-in username can be either the on-premises default username (userPrincipalName) or another attribute configured in Azure AD Connect (Alternate ID). Both use cases work because Seamless SSO uses the securityIdentifier claim in the Kerberos ticket to look up the corresponding user object in Azure AD.
* Seamless SSO is an opportunistic feature. If it fails for any reason, the user sign-in experience goes back to its regular behavior - i.e, the user needs to enter their password on the sign-in page.
* If an application (for example, https://myapps.microsoft.com/contoso.com) forwards a domain\_hint (OpenID Connect) or whr (SAML) parameter - identifying your tenant, or login\_hint parameter - identifying the user, in its Azure AD sign-in request, users are automatically signed in without them entering usernames or passwords.
* Users also get a silent sign-on experience if an application (for example, <https://contoso.sharepoint.com> ) sends sign-in requests to Azure AD's tenanted endpoints - that is, https://login.microsoftonline.com/contoso.com/<..> or https://login.microsoftonline.com/<tenant\_ID>/<..> - instead of Azure AD's common endpoint - that is, https://login.microsoftonline.com/common/<...>.
* Sign out is supported. This allows users to choose another Azure AD account to sign in with, instead of being automatically signed in using Seamless SSO automatically.
* Office 365 clients (16.0.8730.xxxx and above) are supported using a non-interactive flow.
* It can be enabled via Azure AD Connect.
* It is supported on web browser-based clients and Office clients that support modern authentication on platforms and browsers capable of Kerberos authentication:



\*Requires [additional configuration](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-quick-start#browser-considerations)





## **What is the difference between the single sign-on experience provided by** [**Azure AD Join**](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-azureadjoin-overview) **and Seamless SSO?**

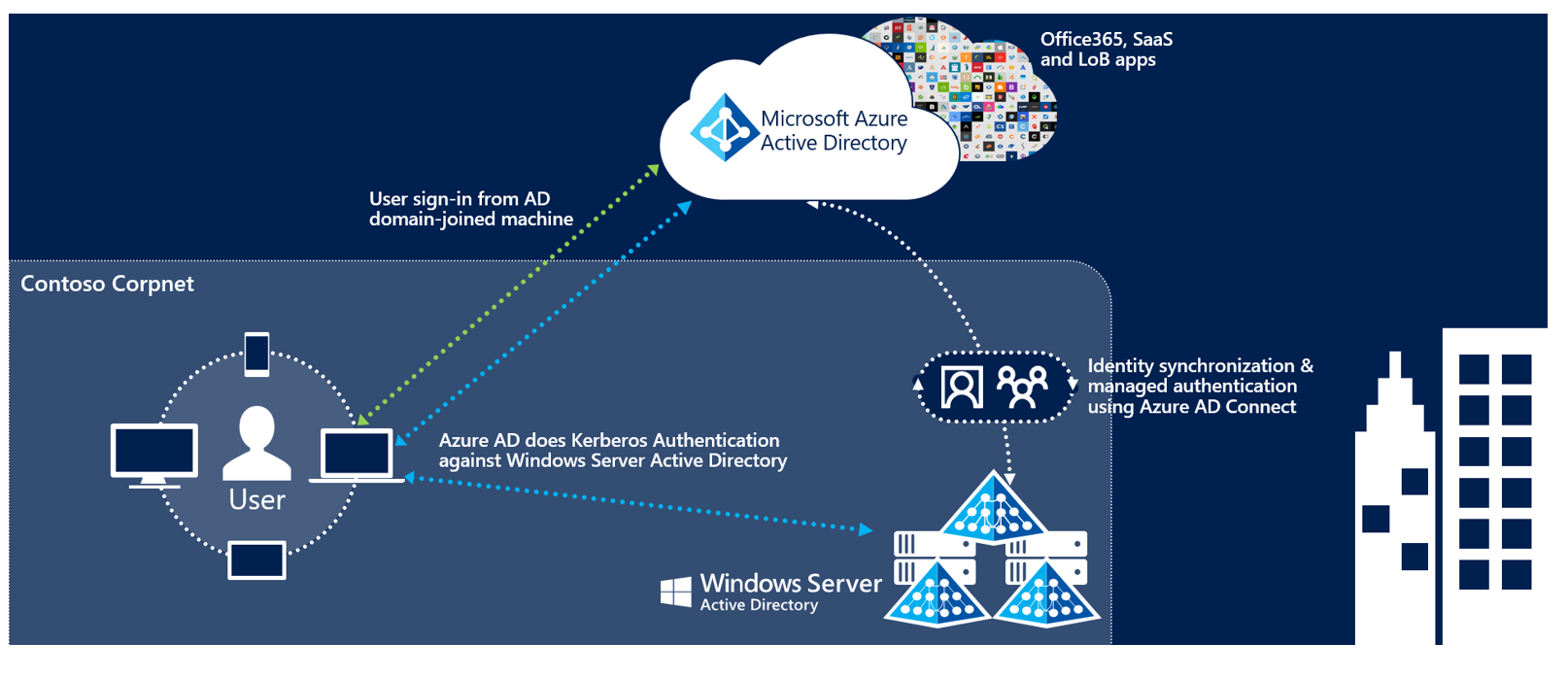
[Azure AD Join](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-azureadjoin-overview) provides SSO to users if their devices are registered with Azure AD. These devices don't necessarily have to be domain-joined. SSO is provided using primary refresh tokens or PRTs, and not Kerberos. The user experience is most optimal on Windows 10 devices. SSO happens automatically on the Edge browser. It also works on Chrome with the use of a browser extension.

You can use both Azure AD Join and Seamless SSO on your tenant. These two features are complementary. If both features are turned on, then SSO from Azure AD Join takes precedence over Seamless SSO.

* **Microsoft recommends** enabling Seamless Single Sign-On option whenever you enable Password Hash Sync or Passthrough Authentication sign-in option for a seamless user experience when signing-in from corporate network.

# Design Considerations

Below is the architecture of how the users will be able to use Kerberos authentication once we enable Seamless Single Sign-on in Azure AD connect.



## Non-Microsoft Browser considerations

#### **Mozilla Firefox (all platforms)**

Mozilla Firefox doesn't automatically use Kerberos authentication. Each user must manually add the Azure AD URL to their Firefox settings by using the following steps:

1. Run Firefox and enter about:config in the address bar. Dismiss any notifications that you see.
2. Search for the **network.negotiate-auth.trusted-uris** preference. This preference lists Firefox's trusted sites for Kerberos authentication.
3. Right-click and select **Modify**.
4. Enter [https://autologon.microsoftazuread-sso.com](https://autologon.microsoftazuread-sso.com/) in the field.
5. Select **OK** and then reopen the browser.

#### **Safari (Mac OS)**

Ensure that the machine running the Mac OS is joined to AD. For instructions on joining AD, see [Best Practices for Integrating OS X with Active Directory](http://www.isaca.org/Groups/Professional-English/identity-management/GroupDocuments/Integrating-OS-X-with-Active-Directory.pdf).

#### **Google Chrome (Mac OS only)**

For Google Chrome on Mac OS and other non-Windows platforms, refer to [The Chromium Project Policy List](https://dev.chromium.org/administrators/policy-list-3#AuthServerWhitelist) for information on how to whitelist the Azure AD URL for integrated authentication.

The use of third-party Active Directory Group Policy extensions to roll out the Azure AD URL to Firefox and Google Chrome on Mac users is outside the scope of this article.

#### **Known browser limitations**

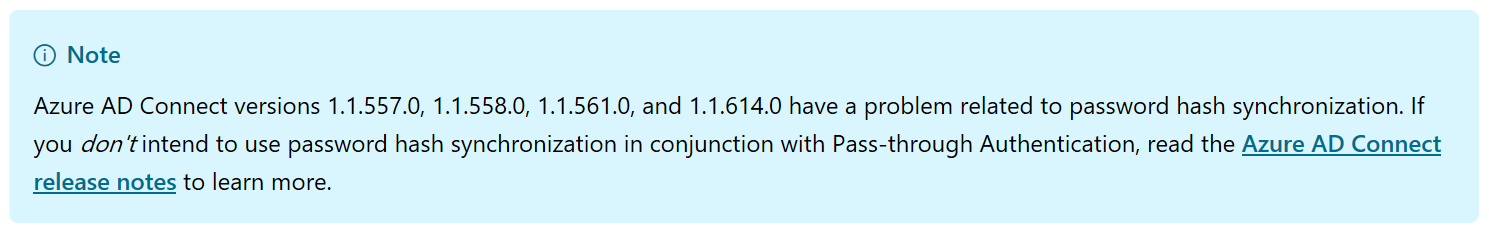
Seamless SSO doesn't work in private browsing mode on Firefox and Edge browsers. It also doesn't work on Internet Explorer if the browser is running in Enhanced Protected mode.

# Implementing Seamless Single Sign-on

## Ensure that the following prerequisites are in place:

**Set up your Azure AD Connect server**  
If you use [Pass-through Authentication](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication) as your sign-in method, no additional prerequisite check is required. If you use [password hash synchronization](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization) as your sign-in method, and if there is a firewall between Azure AD Connect and Azure AD, ensure that:

* You use version 1.1.644.0 or later of Azure AD Connect.
* If your firewall or proxy allows DNS whitelisting, whitelist the connections to the **\*.msappproxy.net** URLs over port 443. If not, allow access to the [Azure datacenter IP ranges](https://www.microsoft.com/download/details.aspx?id=41653), which are updated weekly. This prerequisite is applicable only when you enable the feature. It is not required for actual user sign-ins.

[](https://docs.microsoft.com/azure/active-directory/connect/active-directory-aadconnect-version-history#116470)

**Set up domain administrator credentials:** You need to have domain administrator credentials for each Active Directory forest that:

* You synchronize to Azure AD through Azure AD Connect.
* Contains users you want to enable for Seamless SSO.

**Use a supported Azure AD Connect topology:** Ensure that you are using one of Azure AD Connect's supported topologies described [here](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-topologies).

**Enable modern authentication**: You need to enable [modern authentication](https://aka.ms/modernauthga) on your tenant for this feature to work.

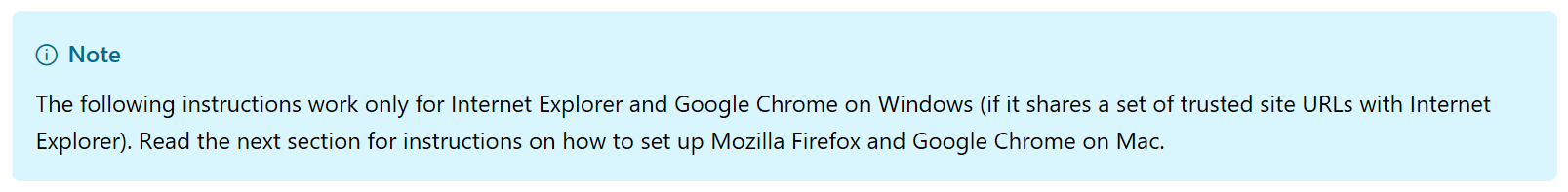
**Use the latest versions of Office 365 clients**: To get a silent sign-on experience with Office 365 clients (Outlook, Word, Excel, and others), your users need to use versions 16.0.8730.xxxx or above.

## Before you roll out the feature

To roll out the feature to your users, you need to add the following Azure AD URL to the users' Intranet zone settings by using Group Policy in Active Directory:

* [https://autologon.microsoftazuread-sso.com](https://autologon.microsoftazuread-sso.com/)

In addition, you need to enable an Intranet zone policy setting called **Allow updates to status bar via script** through Group Policy.



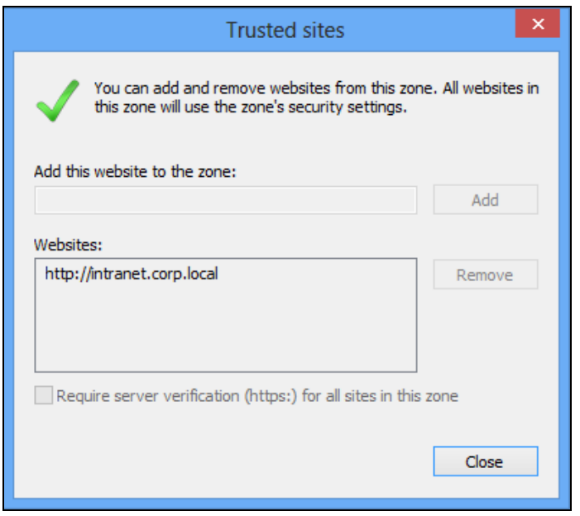
### **Why do you need to modify users' Intranet zone settings?**

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.

There are 2 ways to implement this using Group Policy.

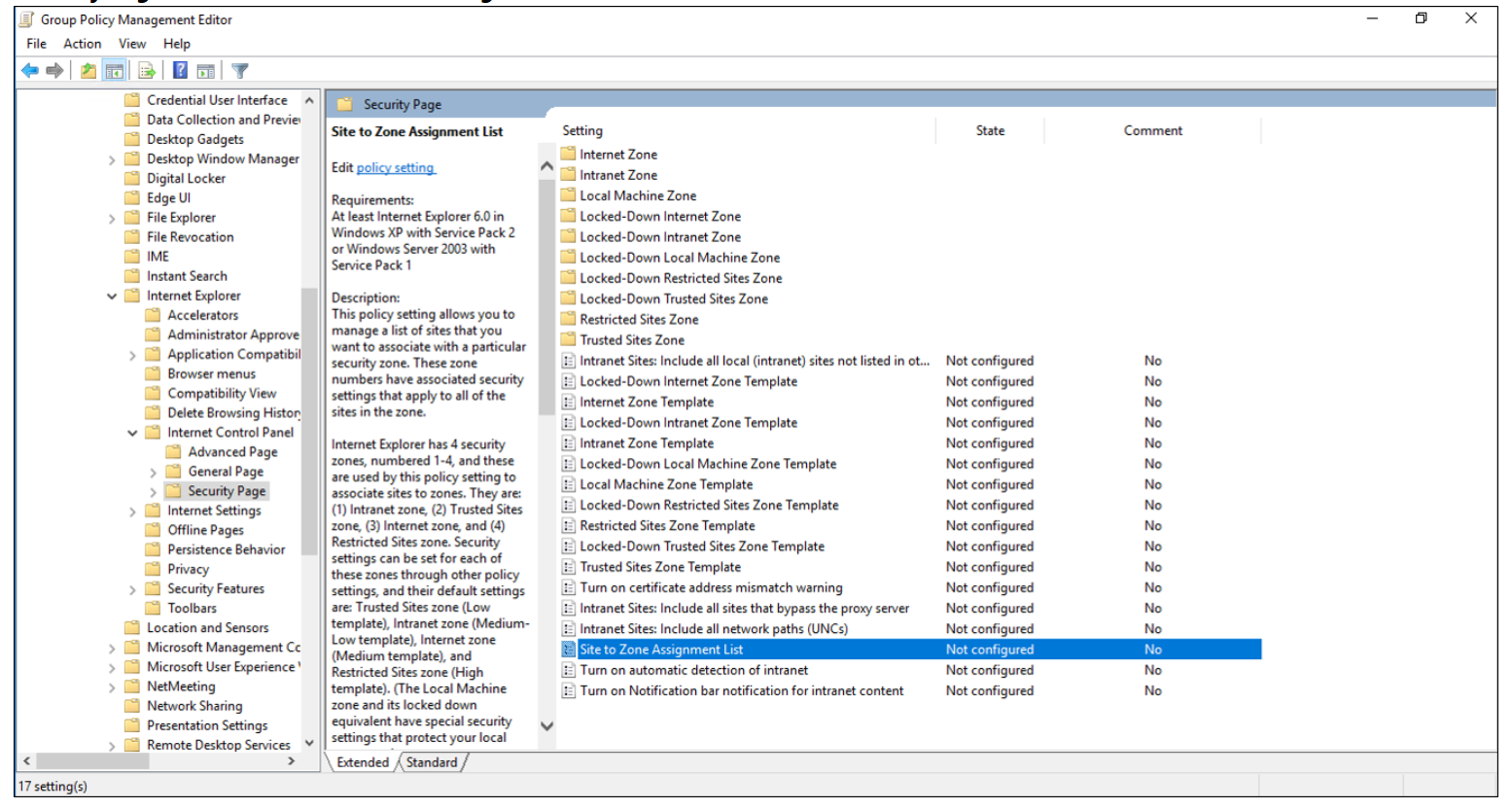
|  |  |  |
| --- | --- | --- |
| Options | User Experience | Admin Decision |
| Option 1 - Group Policy | User cannot modify the zone | This option is preferred if you want to lock down editing of the zone. (secure but not flexible) |
| Option 2 – Group Policy Preferences | User can modify the zone | This option is preferred if you want users to have the flexibility to add application to the zone. (less secure but better end user experience) |

### **Option 1: Group Policy** – Using this method will grey out the Trusted sites UI, this means the end user cannot add or remove any sites in the zone as shown below.



*\*User cannot modify the zone*

1. Open the Group Policy Management Editor tool.
2. Edit the group policy that's applied to some or all your users. This example uses **Default Domain Policy**.
3. Browse to **User Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page**. Then select **Site to Zone Assignment List**.



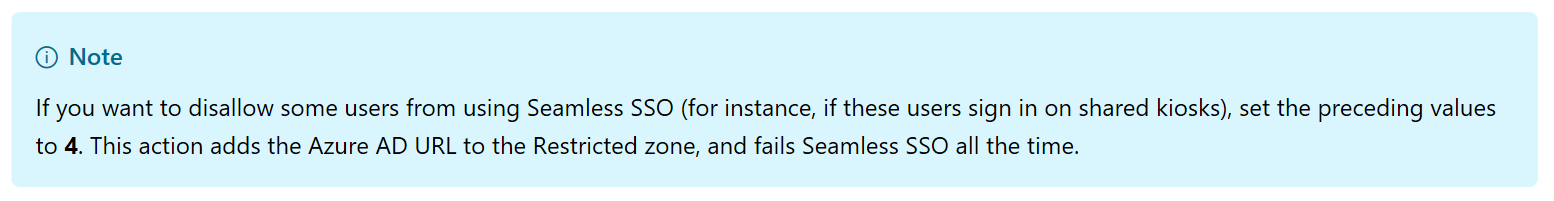
1. Enable the policy, and then enter the following values in the dialog box:

* **Value name**: The Azure AD URL where the Kerberos tickets are forwarded.
* **Value** (Data): **1** indicates the Intranet zone.

The result looks like this:

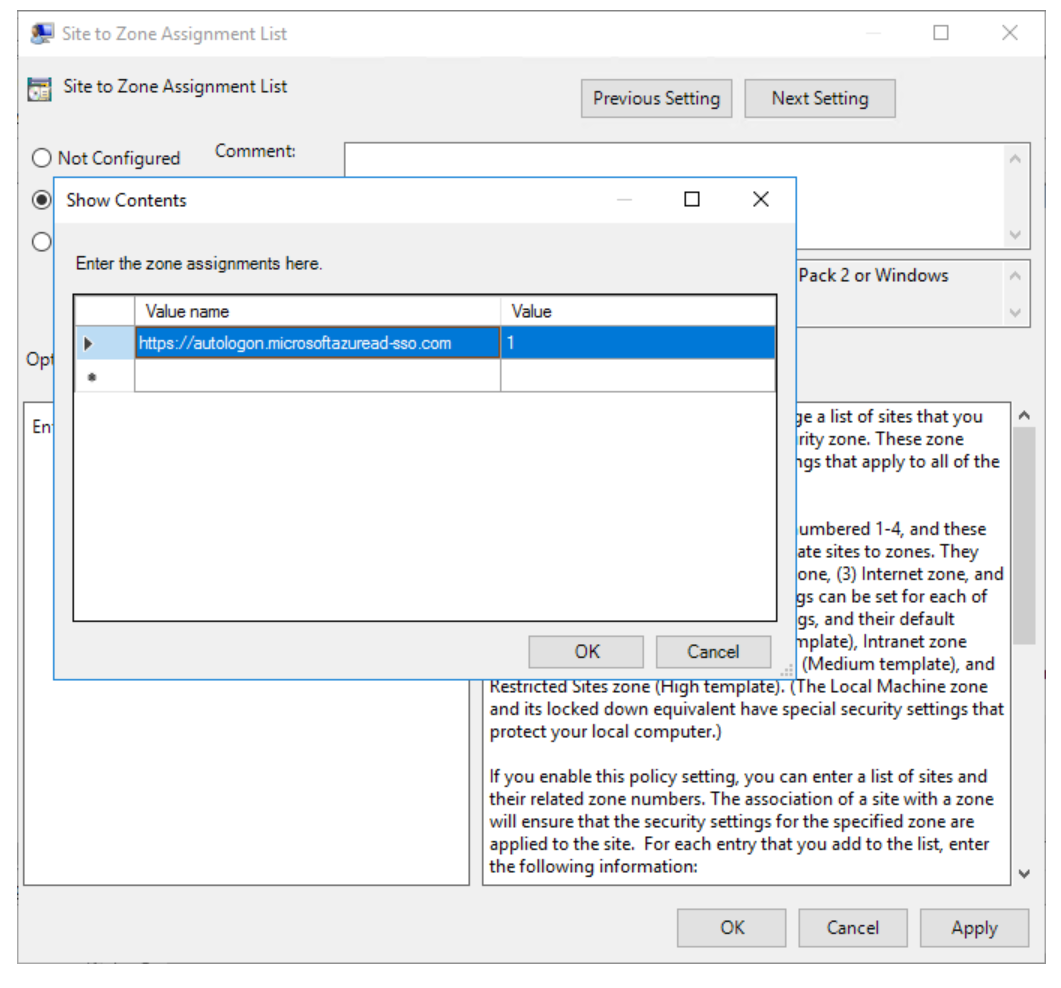
Value: [https://autologon.microsoftazuread-sso.com](https://autologon.microsoftazuread-sso.com/)

Data: 1

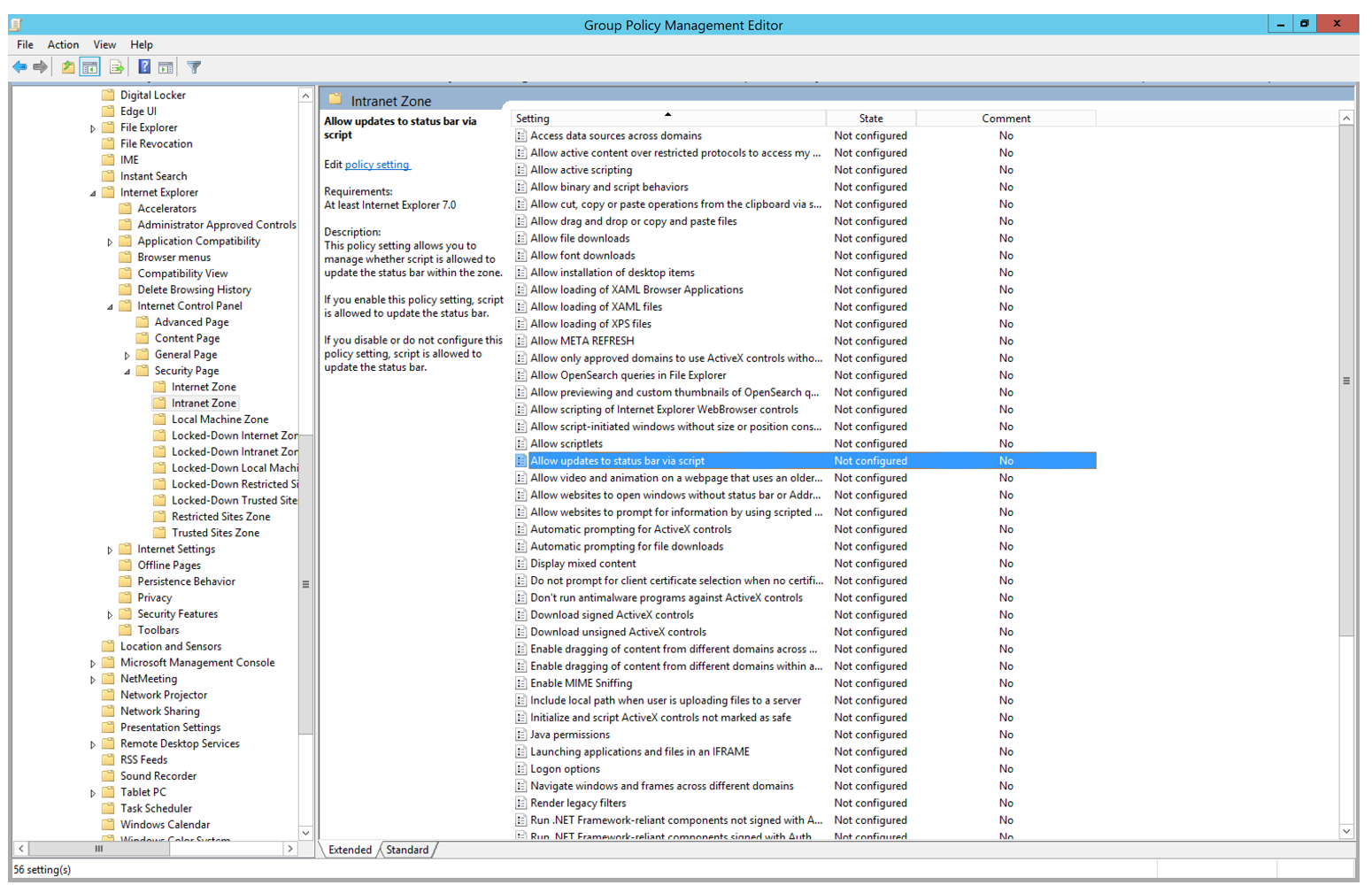


The policy to disallow some users from using Seamless SSO must be applied using a separate GPO and must applied to users logging into kiosk machines.

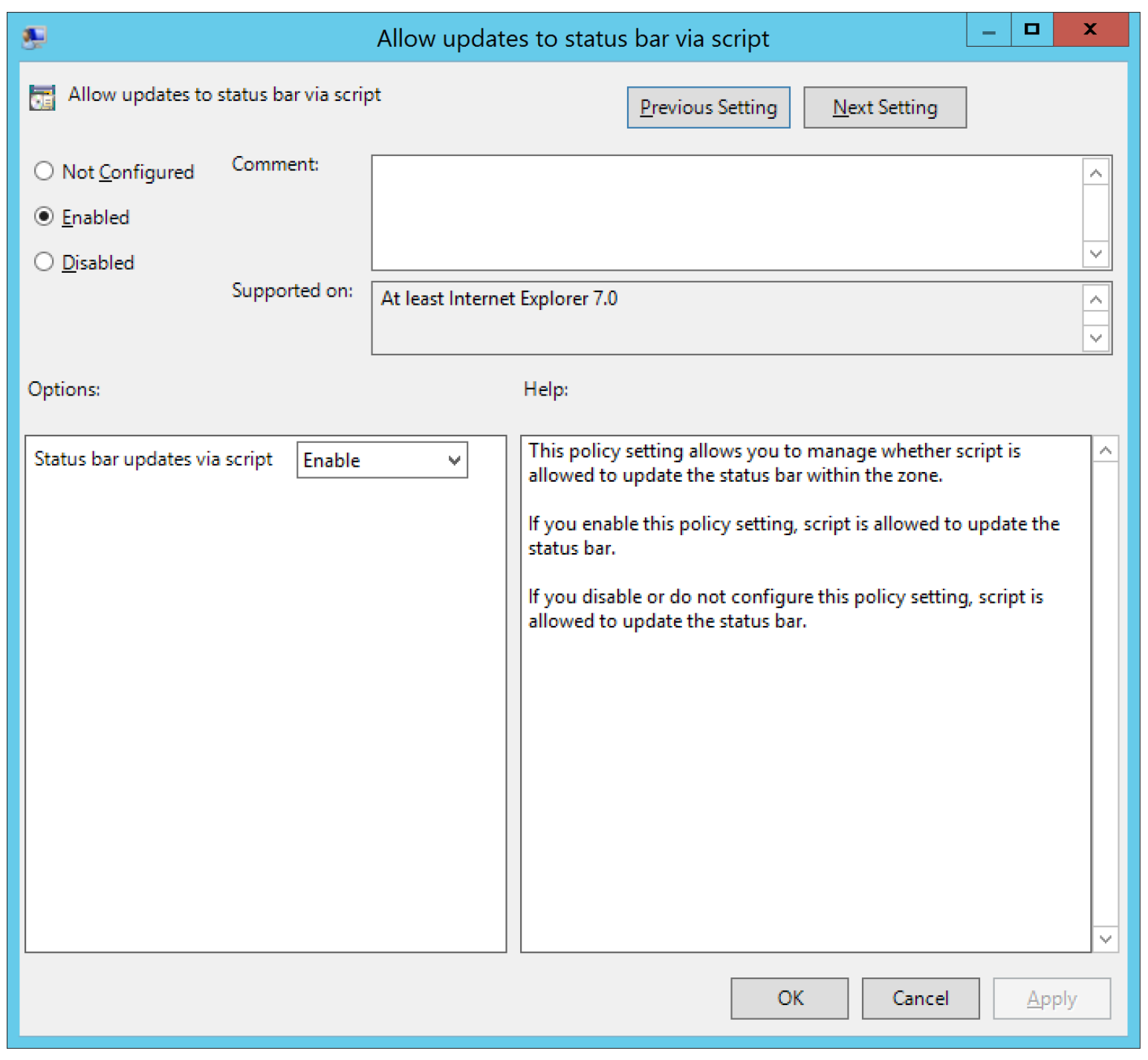
1. Select **OK**, and then select **OK** again.



1. Browse to **User Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page** > **Intranet Zone**. Then select **Allow updates to status bar via script**.



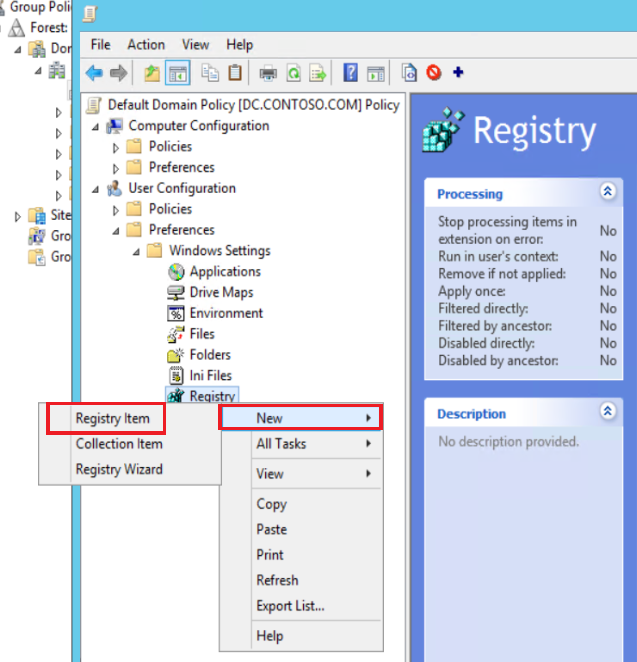
1. Enable the policy setting, and then select **OK**.



### **Option 2: Group Policy Preferences ­­–** Using this option will ensure the users are still allowed to add any sites in to the respective zones.

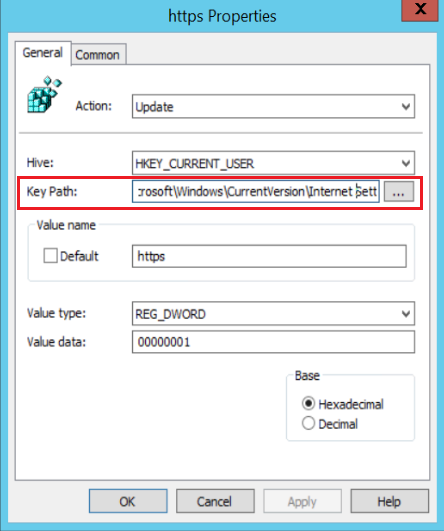
The benefit of this is that your users can edit the zone lists and view all the added sites.

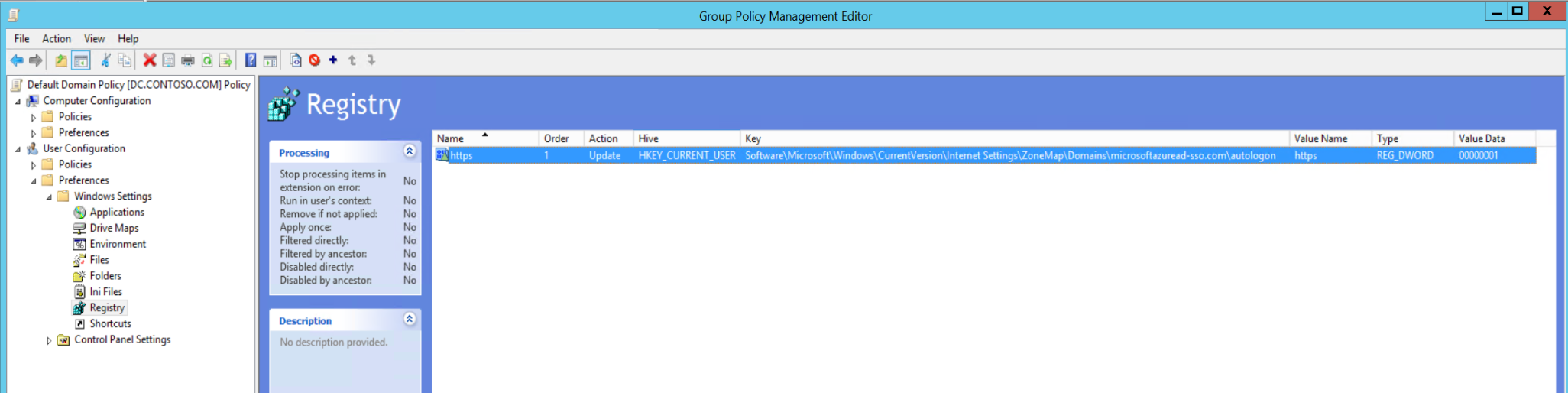
1. Logon to the machine where you have the Group Policy Management Editor tool, this can be done from a domain controller.
2. Now open the Group Policy Management Editor tool.
3. Edit the group policy that's applied to some or all your users. This example uses **Default Domain Policy**.
4. Browse to **User Configuration** > **Preferences > Windows Settings > Registry > New > Registry Item**



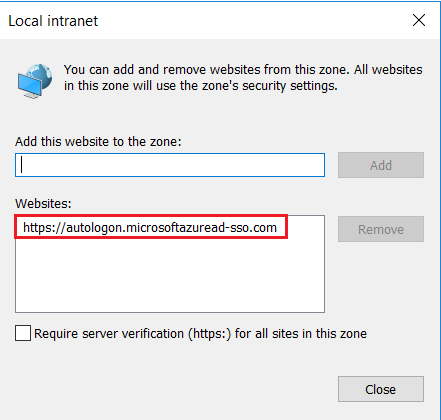
1. Under Key Path: Please add below and click Apply and Ok

**Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\microsoftazuread-sso.com\autologon**

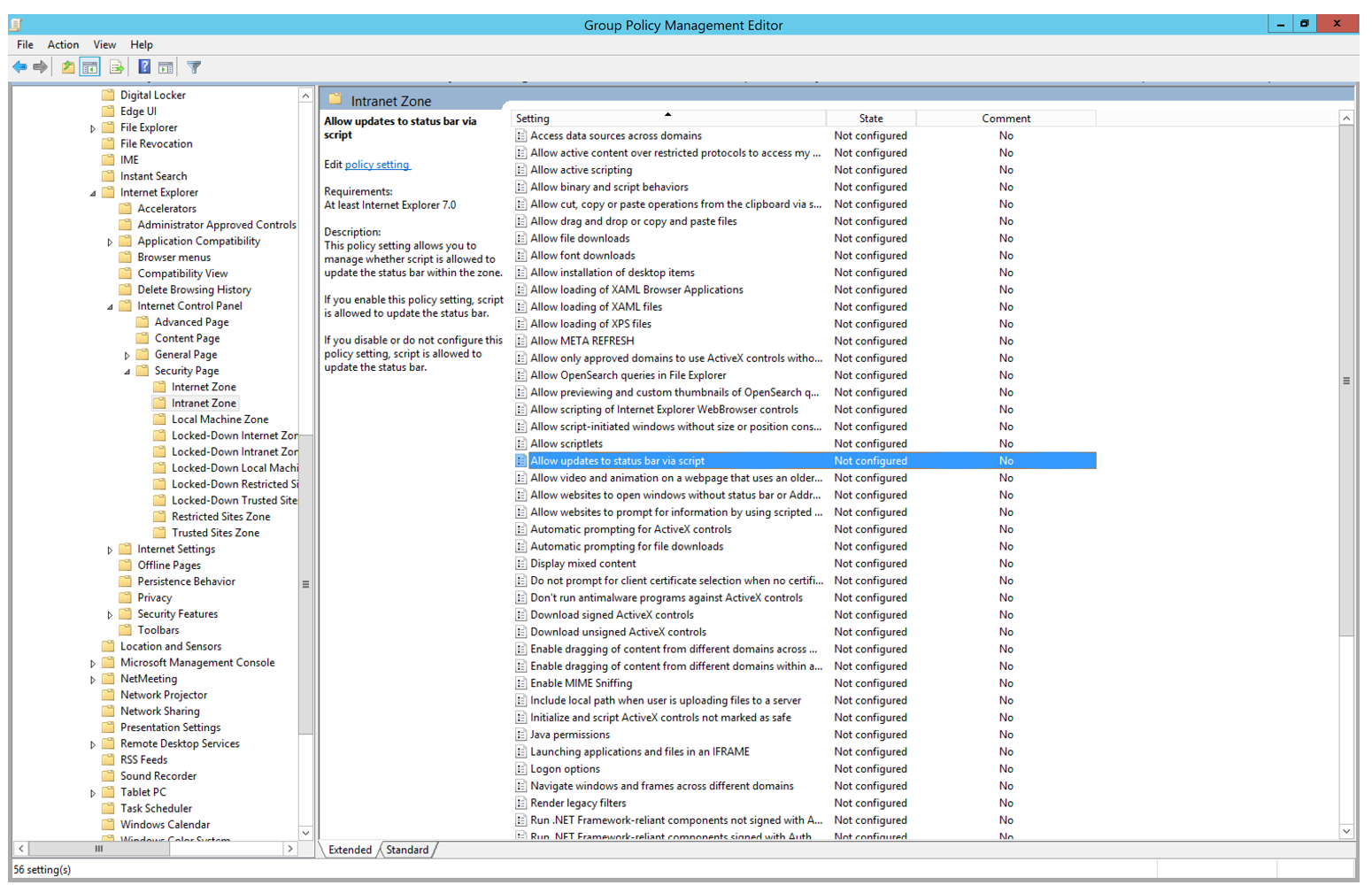




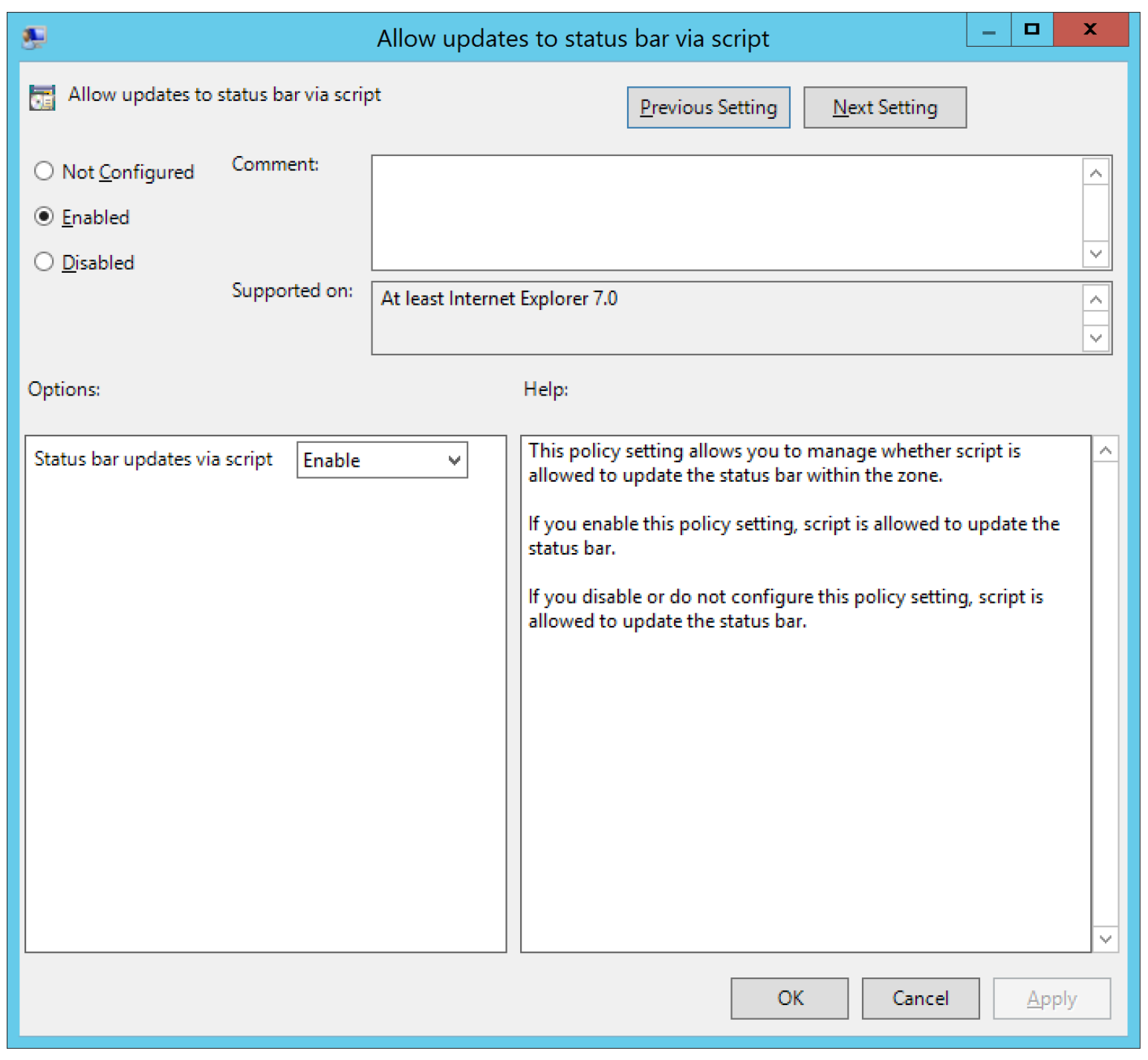
1. Once the user logs into a client machine they will see that this URL is added under the Local Intranet Zone.



1. Browse to **User Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page** > **Intranet Zone**. Then select **Allow updates to status bar via script**.



1. Enable the policy setting, and then select **OK**.

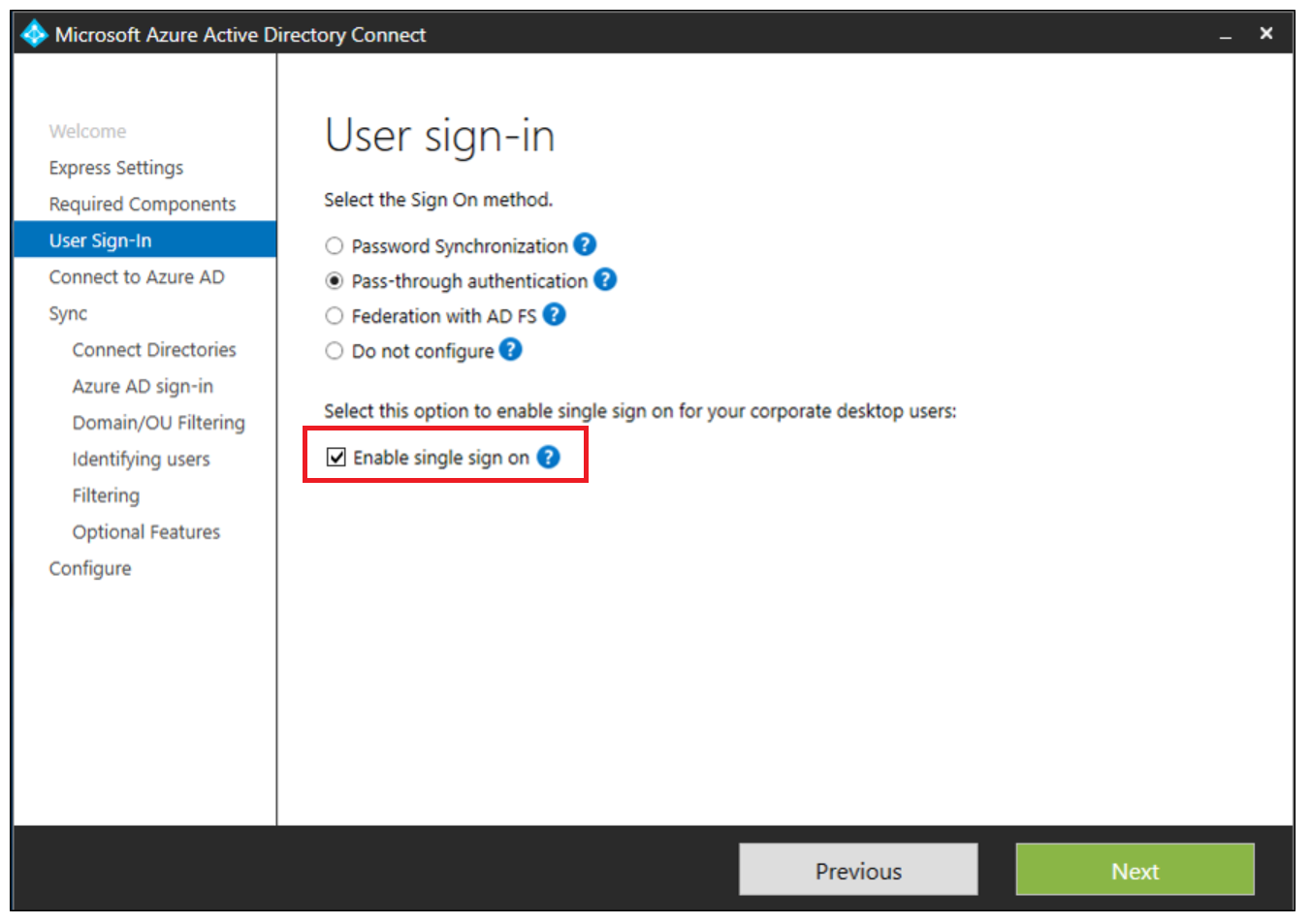


# Enable the feature

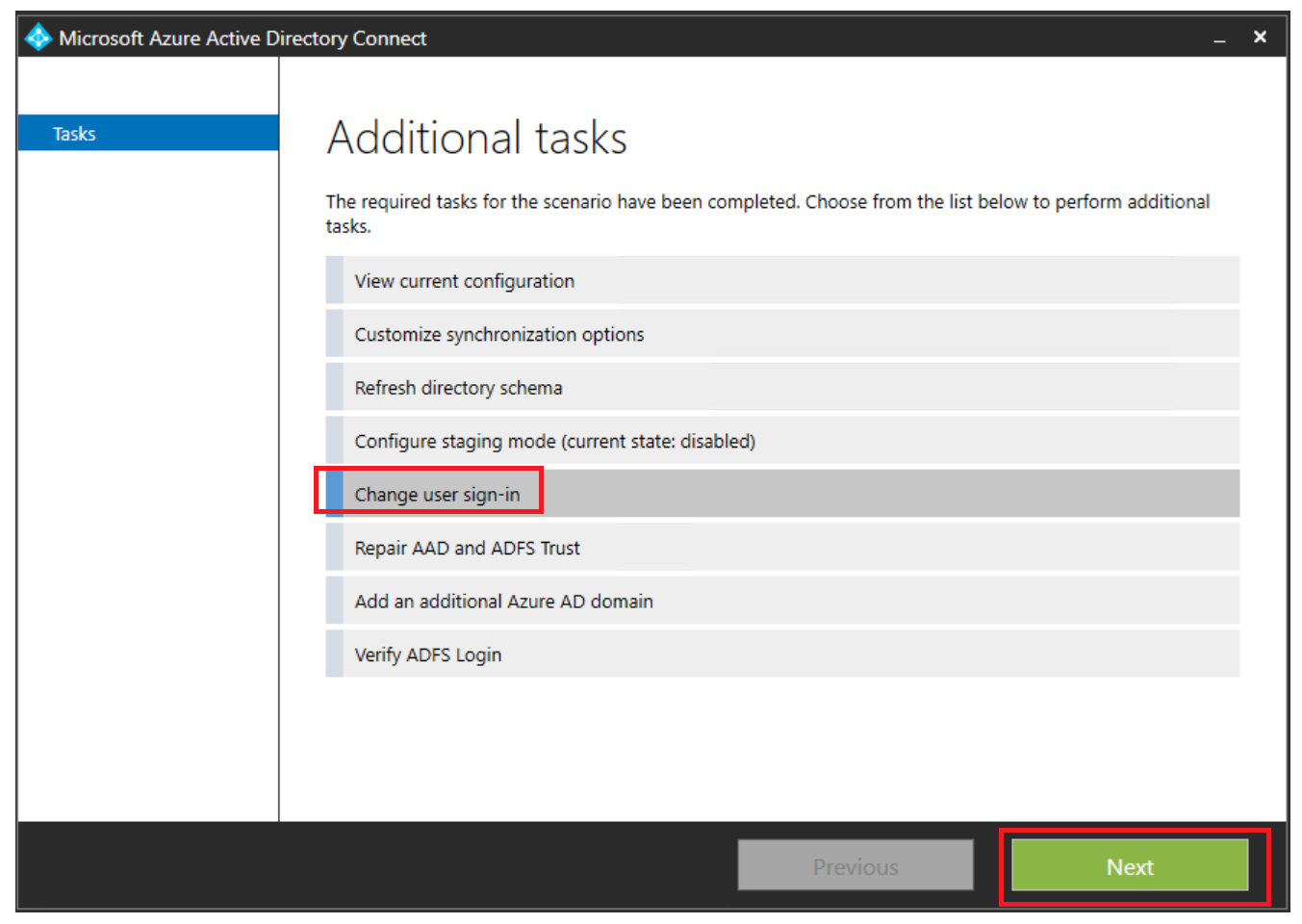
Please logon to the Azure AD Connect server.

Enable Seamless SSO through [Azure AD Connect](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect) following the below steps.

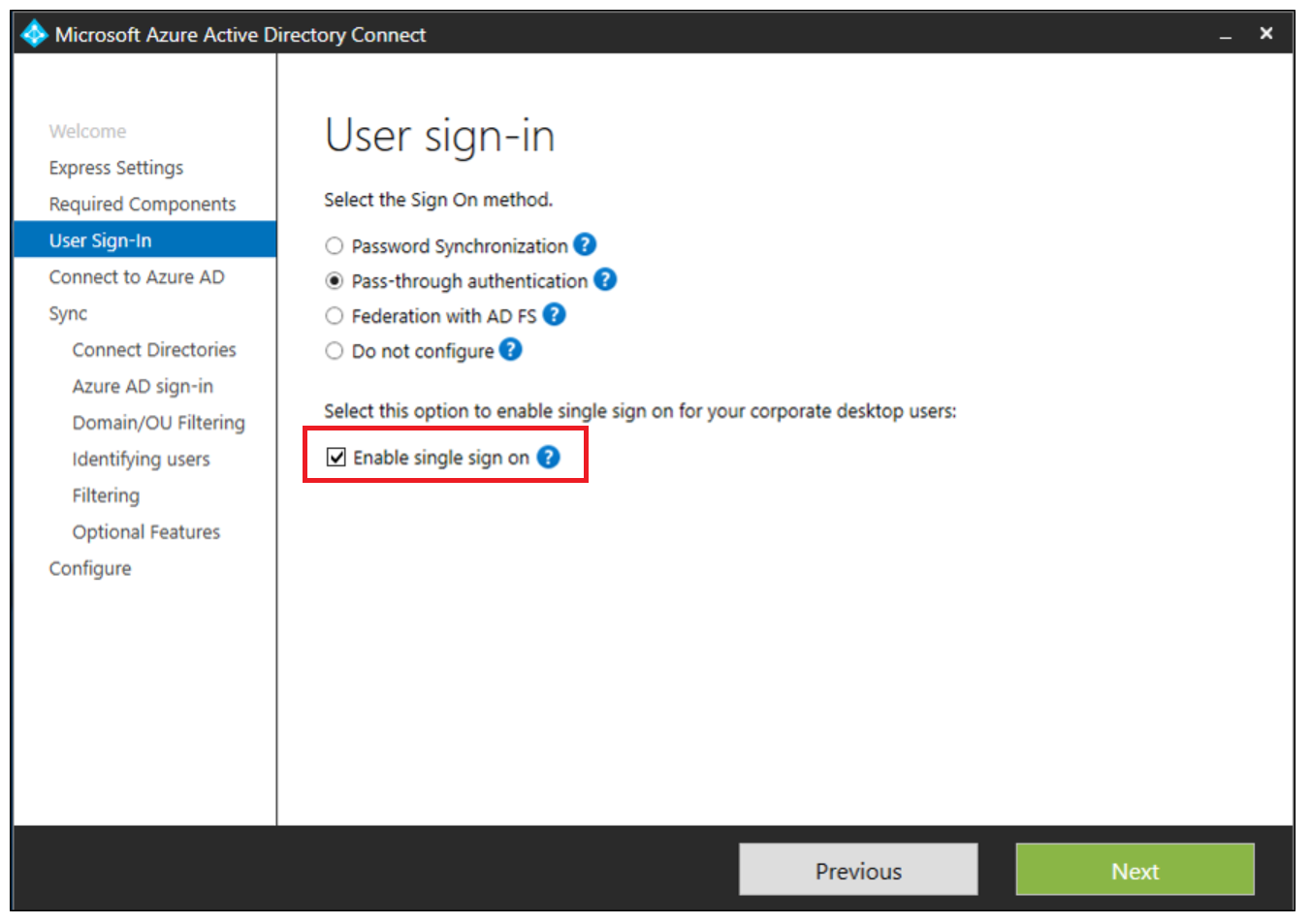
* If you're doing a fresh installation of Azure AD Connect, choose the [custom installation path](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-get-started-custom). At the **User sign-in** page, select the **Enable single sign on** option.



* If you already have an installation of Azure AD Connect, select the **Change user sign-in** page in Azure AD Connect, and then select **Next**.



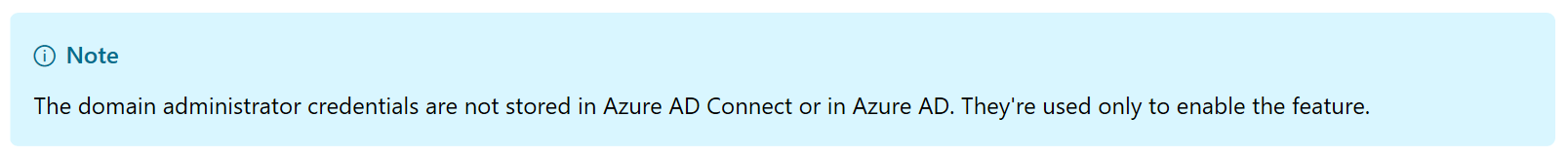
Continue through the wizard until you get to the **Enable single sign on** page.



Provide domain administrator credentials for each Active Directory forest that:

* You synchronize to Azure AD through Azure AD Connect.
* Contains users you want to enable for Seamless SSO.

After completion of the wizard, Seamless SSO is enabled on your tenant.



# Operationalize your Implementation

## Purpose of Document

The intent for the *Operationalize your Implementation* is to verify the fact that Seamless Single Sign-on configuration is enabled and test the seamless single sign-on access from an end user experience. This includes logging into the Azure AD Portal and checking the status of Seamless single sign-on.

## Required Roles

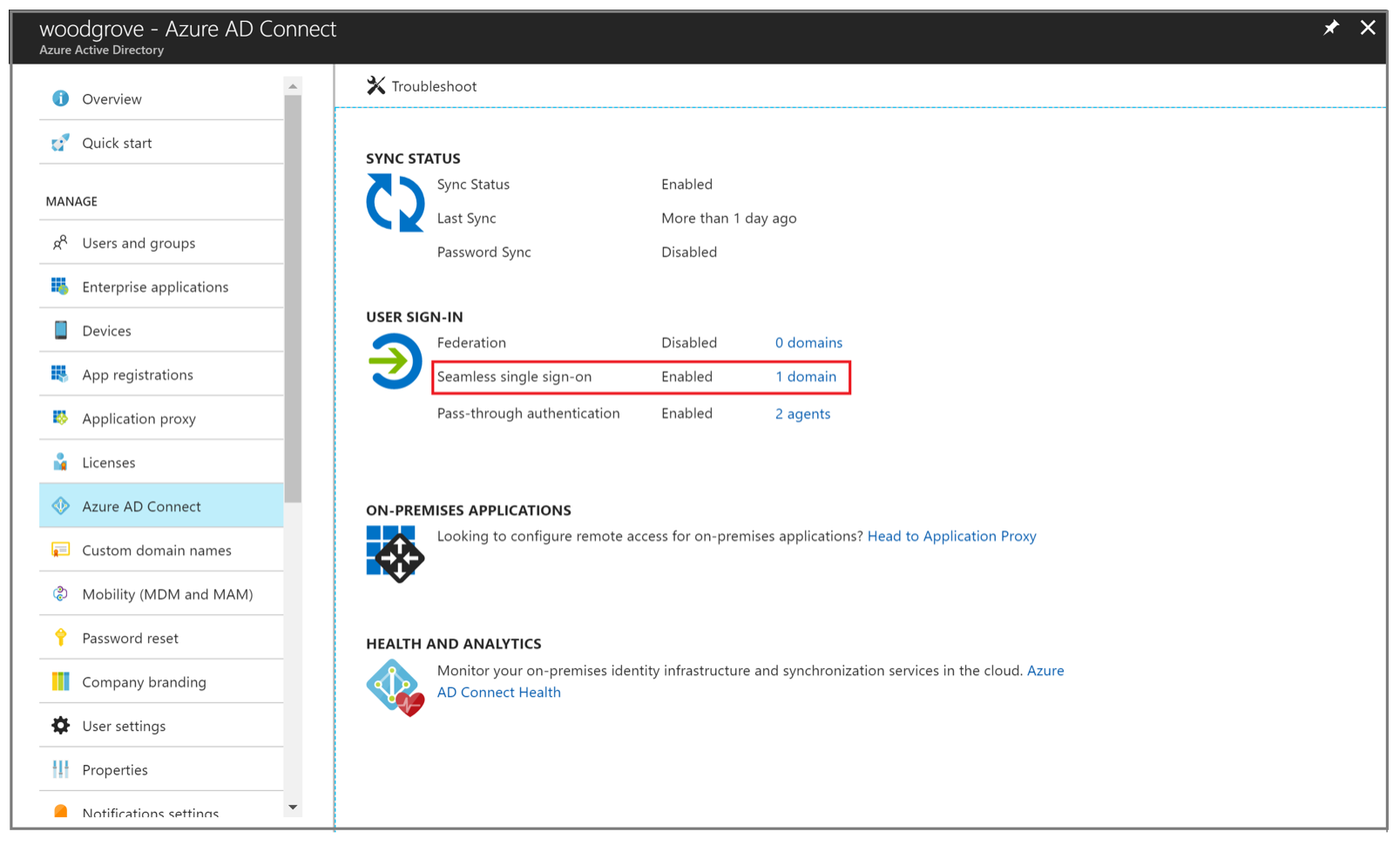
Microsoft recommends using the less role to accomplish the required task within Azure Active Directory. Microsoft recommend [review the different roles that are available](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal) and choose the right one to solve your needs for each persona for this application. Some roles may need to be applied temporarily and removed after the deployment has been completed.

|  |  |  |  |
| --- | --- | --- | --- |
| Personas | Roles | Azure AD Role (if required) | Assign to |
| Help Desk Admin | Tier 1 Support | None |  |
| Identity Admin | Login to the Azure AD Portal | Global Admin |  |
|  |  |  |  |
| Infrastructure Admins | Login to the Azure AD Connect Server | Enterprise Admin |  |
| Business Owner/Stakeholder | User Attestation of seamless single sign-on to Office 365 apps. | None |  |

## Verify Seamless SSO is enabled

Follow these instructions to verify that you have enabled Seamless SSO correctly:

1. Sign in to the [Azure Active Directory administrative center](https://aad.portal.azure.com/) with the global administrator credentials for your tenant.
2. Select **Azure Active Directory** in the left pane.
3. Select **Azure AD Connect**.
4. Verify that the **Seamless single sign-on** feature appears as **Enabled**.



## Test the Seamless Single Sign-on experience

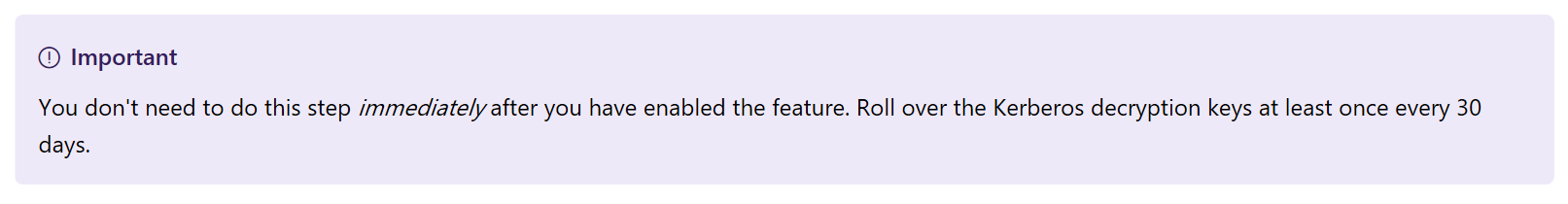
To test the feature for a specific user, ensure that all the following conditions are in place:

* The user signs in on a corporate device.
* The device is joined to your Active Directory domain.
* The device has a direct connection to your domain controller (DC), either on the corporate wired or wireless network or via a remote access connection, such as a VPN connection.
* You have [rolled out the feature](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-quick-start##step-3-roll-out-the-feature) to this user through Group Policy.

|  |  |  |
| --- | --- | --- |
| Test Scenario | Expected Result | Actual Result |
| To test the scenario where the user enters only the username, but not the password   * Sign in to <https://myapps.microsoft.com/> in a new private browser session. | User is not prompted to enter the password after entering the username. |  |
| To test the scenario where the user doesn't have to enter the username or the password, use one of these steps:   * Sign in to <https://myapps.microsoft.com/contoso.onmicrosoft.com> in a new private browser session. Replace contoso with your tenant's name. OR * Sign in to <https://myapps.microsoft.com/contoso.com> in a new private browser session. Replace contoso.com with a verified domain (not a federated domain) on your tenant. | User logs in directly into the my apps portal. |  |

## Roll over keys

When you enable the feature, Azure AD Connect creates computer accounts (representing Azure AD) in all the Active Directory forests on which you have enabled Seamless SSO. To learn more, see [Azure Active Directory Seamless Single Sign-On: Technical deep dive](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-how-it-works). For improved security, we recommend that you periodically roll over the Kerberos decryption keys of these computer accounts. For instructions on how to roll over keys, see [How can I roll over the Kerberos decryption key of the AZUREADSSOACC computer account?.](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-faq" \l "how-can-i-roll-over-the-kerberos-decryption-key-of-the-azureadssoacc-computer-account)



## 

# Helpful Documentation

* [**Quick Start**](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-quick-start) - Get up and running Azure AD Seamless SSO.
* [**Frequently Asked Questions**](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-faq) - Answers to frequently asked questions.
* [**Troubleshoot**](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-troubleshoot-sso) - Learn how to resolve common issues with the feature.
* [**UserVoice**](https://feedback.azure.com/forums/169401-azure-active-directory/category/160611-directory-synchronization-aad-connect) - For filing new feature requests.

**IMPORTANT NOTICES**

© 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