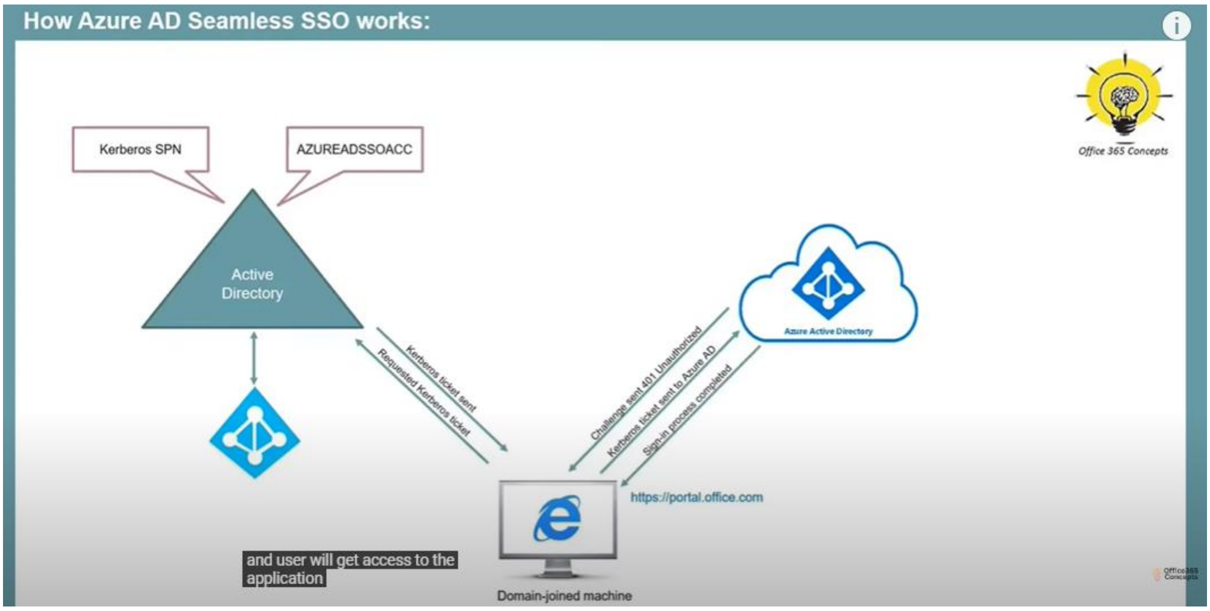
Seamless Single Sign-On

Azure Active Directory SSO Automatically signs users in when they are on their corporate devices connected to your corporate network.



How Azure AD Seamless SSO works:

Kerberos SPN
AZUREADSSOACC
Active Directory
Office 365 Concepts
Azure Active Directory
Kerberos ticket sent
Requested Kerberos ticket
Challenge sent 401 Unauthorized
Kerberos ticket sent to Azure AD
Sign-in process completed
https://portal.office.com
Domain-joined machine

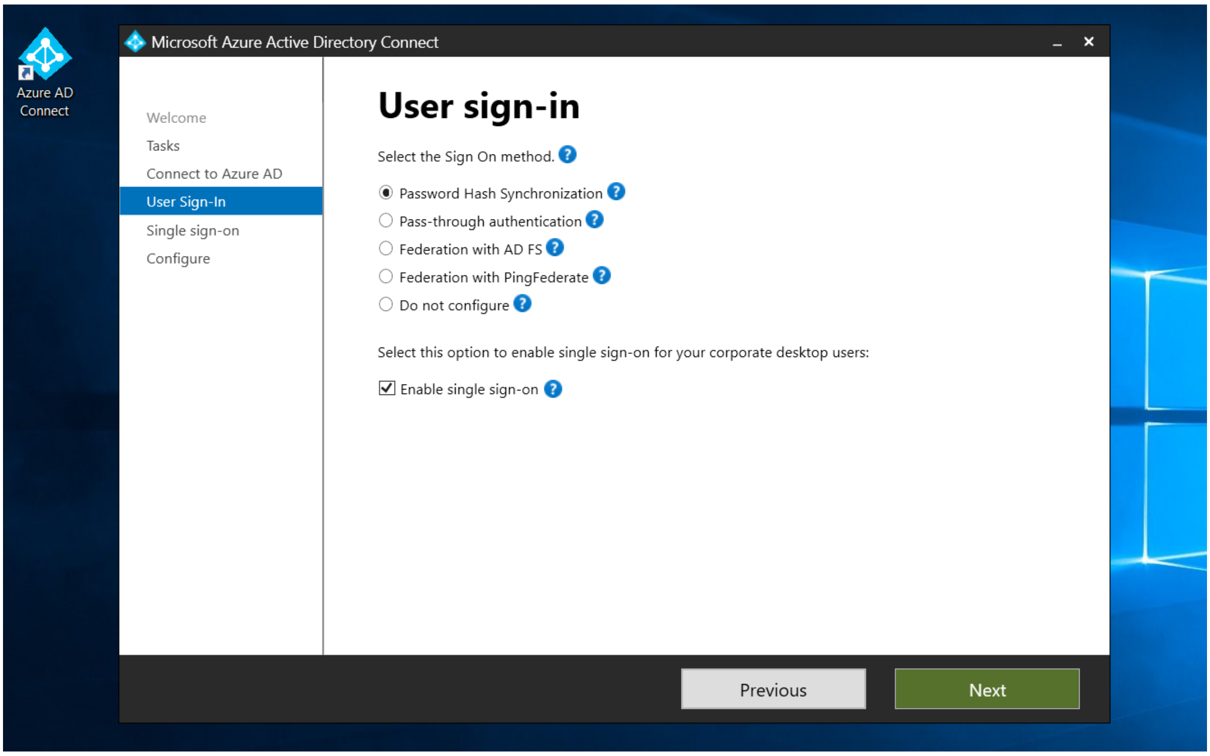
and user will get access to the application

Prerequisites for SSO:

- Setup AD Connect server with Pass Through Authentication or Password Hash Synchronization.
- Use Latest version of Azure AD Connect (1.1644.0 or Later.)
- Credentials of Global Administrator and On-Premises Active Directory Domain Controller.
- Enable modern Authentication on Azure AD Tenant.
- Use Latest version of M365 clients.

Steps to Configure Seamless Single Sign-on:

1. **On the On-Premises Azure AD Connect server open the Azure AD Connect click on configure, Select Change-User Sign in click on Next.**
2. **Now enter the Global Admin Credentials for your Tenant.**
3. **Now enable the single sign-on**



User sign-in

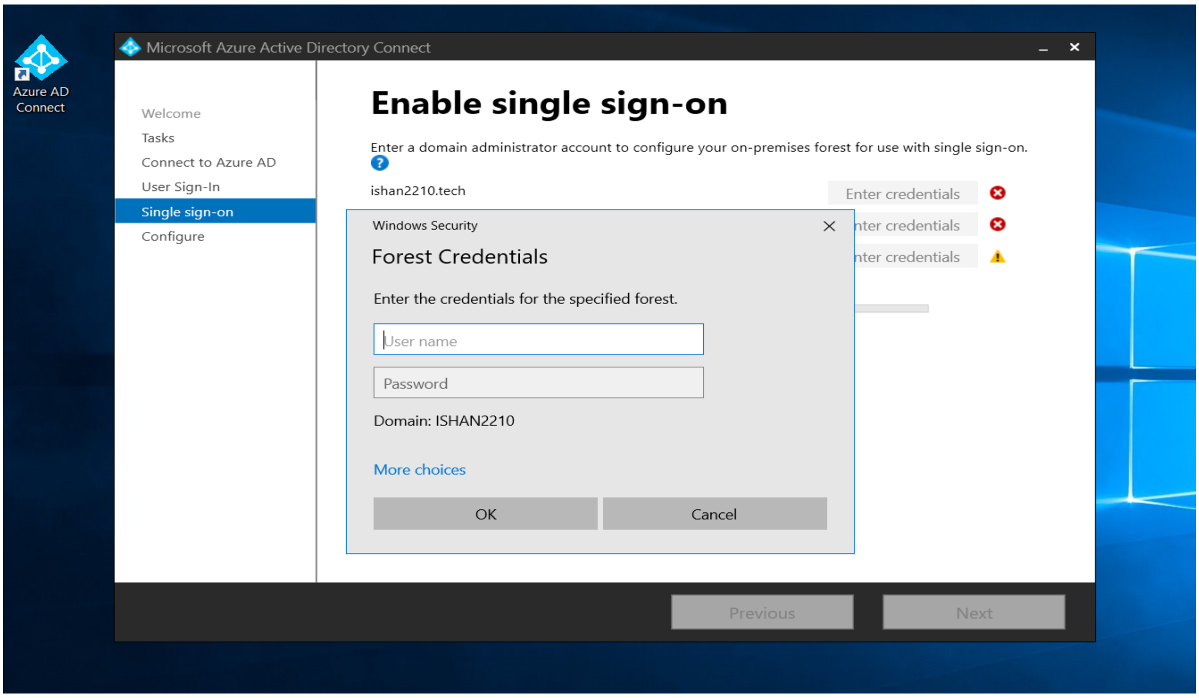
Select the Sign On method.

● Password Hash Synchronization
○ Pass-through authentication
○ Federation with AD FS
○ Federation with PingFederate
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

☑ Enable single sign-on

4. **Enter the credentials of the On-Premises DC for which you want to configure SSO.**



Enable single sign-on

Enter a domain administrator account to configure your on-premises forest for use with single sign-on.

ishan2210.tech Enter credentials

Windows Security

Forest Credentials

Enter the credentials for the specified forest.

User name

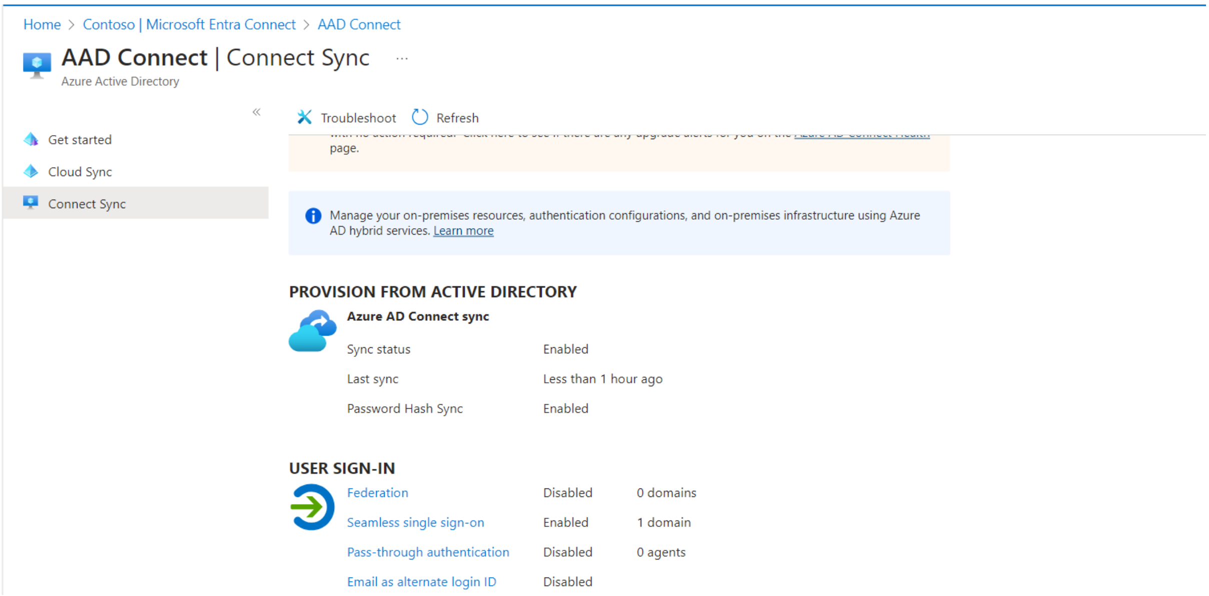
Password

Domain: ISHAN2210

More choices

OK Cancel

5. **Now go to Microsoft Entra ID click on Microsoft Entra connect: check whether the SSO is configured for the domain.**



Home > Contoso | Microsoft Entra Connect > AAD Connect

AAD Connect | Connect Sync

Azure Active Directory

page.

Manage your on-premises resources, authentication configurations, and on-premises infrastructure using Azure AD hybrid services. Learn more

PROVISION FROM ACTIVE DIRECTORY

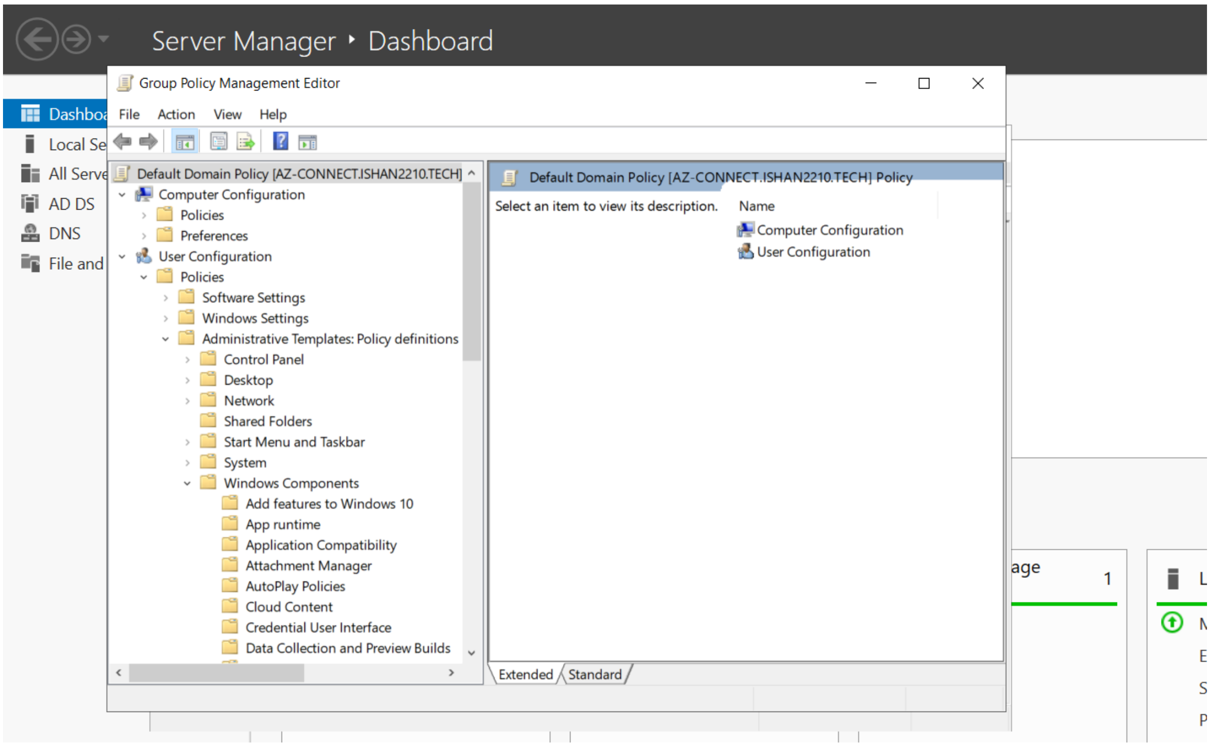
Azure AD Connect sync

Sync status	Enabled
Last sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Disabled	0 agents
Email as alternate login ID	Disabled	

Now we have to create a Group Policy on-premises Active Directory to roll out seamless SSO to the users

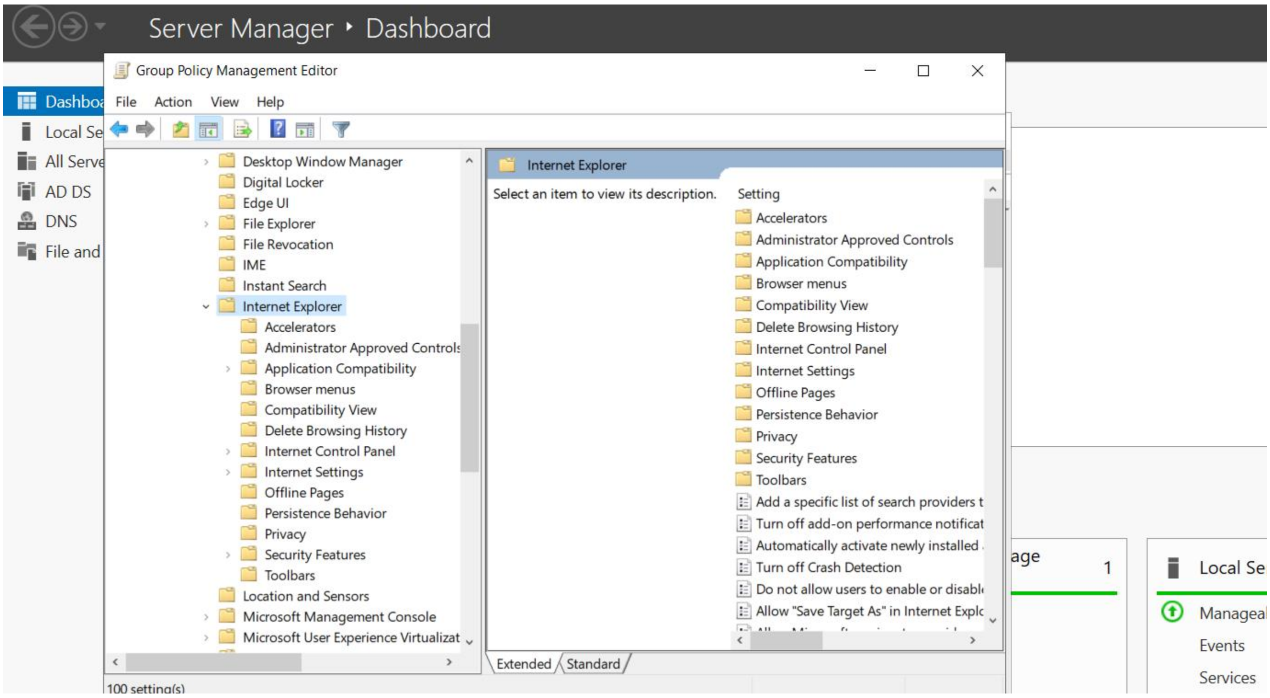


```
Default Domain Policy [AZ-CONNECT.ISHAN2210.TECH]
  Computer Configuration
    Policies
    Preferences
  User Configuration
    Policies
      Software Settings
      Windows Settings
      Administrative Templates: Policy definitions
        Control Panel
        Desktop
        Network
        Shared Folders
        Start Menu and Taskbar
        System
        Windows Components
          Add features to Windows 10
          App runtime
          Application Compatibility
          Attachment Manager
          AutoPlay Policies
          Cloud Content
          Credential User Interface
          Data Collection and Preview Builds
```

Default Domain Policy [AZ-CONNECT.ISHAN2210.TECH] Policy

Select an item to view its description.

Name
Computer Configuration
User Configuration

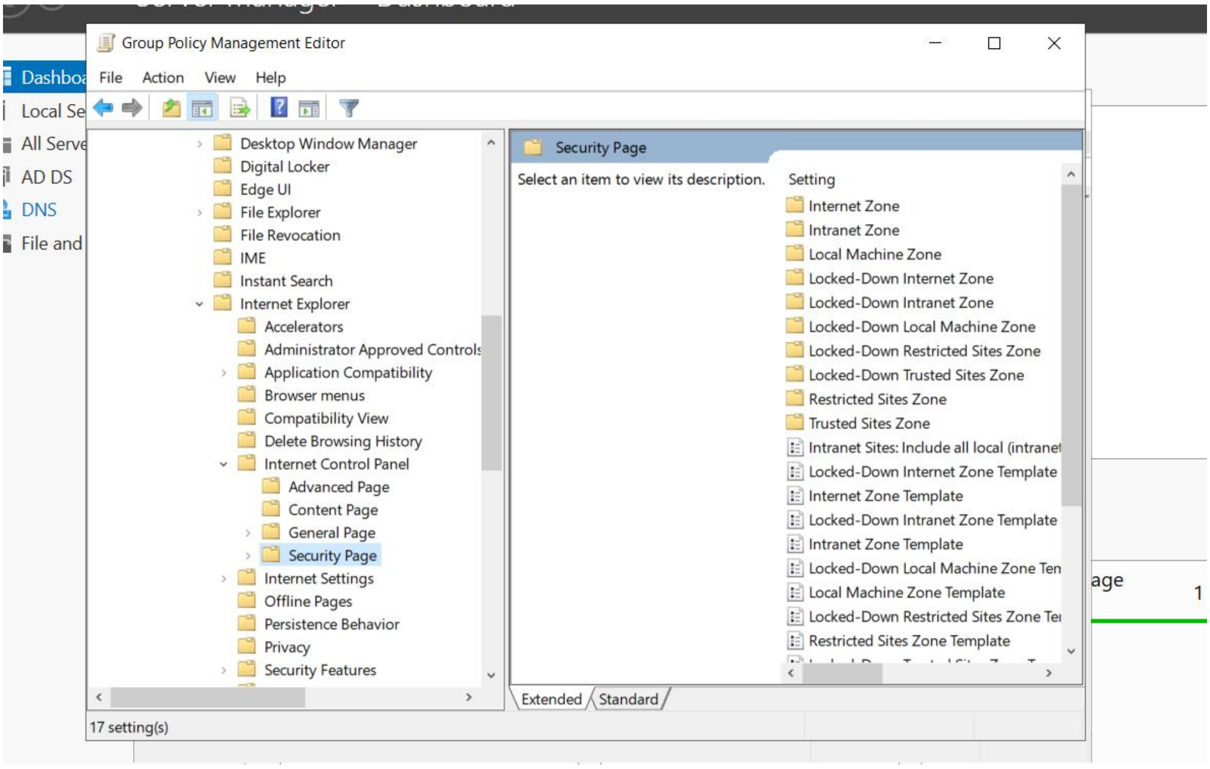


Internet Explorer

Select an item to view its description.

Setting
Accelerators
Administrator Approved Controls
Application Compatibility
Browser menus
Compatibility View
Delete Browsing History
Internet Control Panel
Internet Settings
Offline Pages
Persistence Behavior
Privacy
Security Features
Toolbars
Add a specific list of search providers t
Turn off add-on performance notificat
Automatically activate newly installed
Turn off Crash Detection
Do not allow users to enable or disabl
Allow "Save Target As" in Internet Explo

100 setting(s)



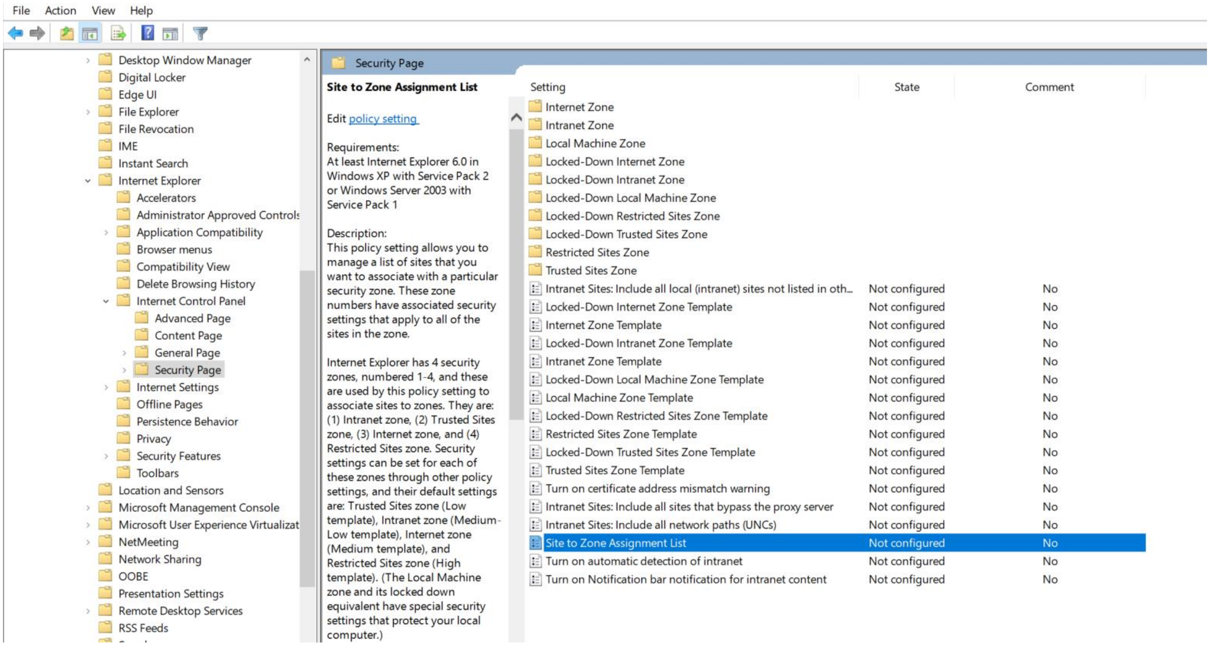
Security Page

Select an item to view its description.

Setting
Internet Zone
Intranet Zone
Local Machine Zone
Locked-Down Internet Zone
Locked-Down Intranet Zone
Locked-Down Local Machine Zone
Locked-Down Restricted Sites Zone
Locked-Down Trusted Sites Zone
Restricted Sites Zone
Trusted Sites Zone
Intranet Sites: Include all local (intranet
Locked-Down Internet Zone Template
Internet Zone Template
Locked-Down Intranet Zone Template
Intranet Zone Template
Locked-Down Local Machine Zone Ten
Local Machine Zone Template
Locked-Down Restricted Sites Zone Te
Restricted Sites Zone Template

17 setting(s)

Enable the Site to zone Assignment List and enter the URL



Site to Zone Assignment List

Edit policy setting

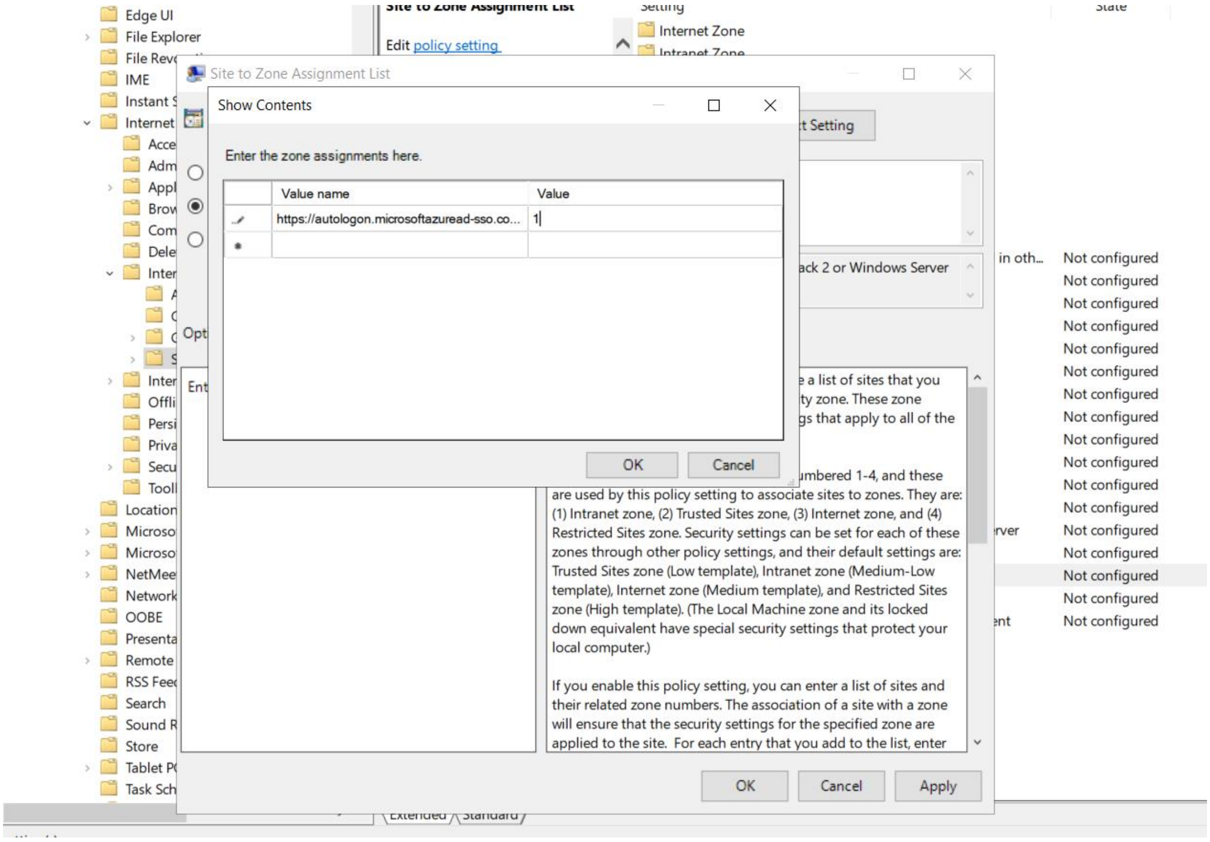
Requirements:
At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1

Description:
This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone.

Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local computer.)

Setting	State	Comment
Internet Zone		
Intranet Zone		
Local Machine Zone		
Locked-Down Internet Zone		
Locked-Down Intranet Zone		
Locked-Down Local Machine Zone		
Locked-Down Restricted Sites Zone		
Locked-Down Trusted Sites Zone		
Restricted Sites Zone		
Trusted Sites Zone		
Intranet Sites: Include all local (intranet) sites not listed in oth...	Not configured	No
Locked-Down Internet Zone Template	Not configured	No
Internet Zone Template	Not configured	No
Locked-Down Intranet Zone Template	Not configured	No
Intranet Zone Template	Not configured	No
Locked-Down Local Machine Zone Template	Not configured	No
Local Machine Zone Template	Not configured	No
Locked-Down Restricted Sites Zone Template	Not configured	No
Restricted Sites Zone Template	Not configured	No
Locked-Down Trusted Sites Zone Template	Not configured	No
Trusted Sites Zone Template	Not configured	No
Turn on certificate address mismatch warning	Not configured	No
Intranet Sites: Include all sites that bypass the proxy server	Not configured	No
Intranet Sites: Include all network paths (UNCs)	Not configured	No
Site to Zone Assignment List	Not configured	No
Turn on automatic detection of intranet	Not configured	No
Turn on Notification bar notification for intranet content	Not configured	No

https://autologon.microsoftazuread-sso.com value 1



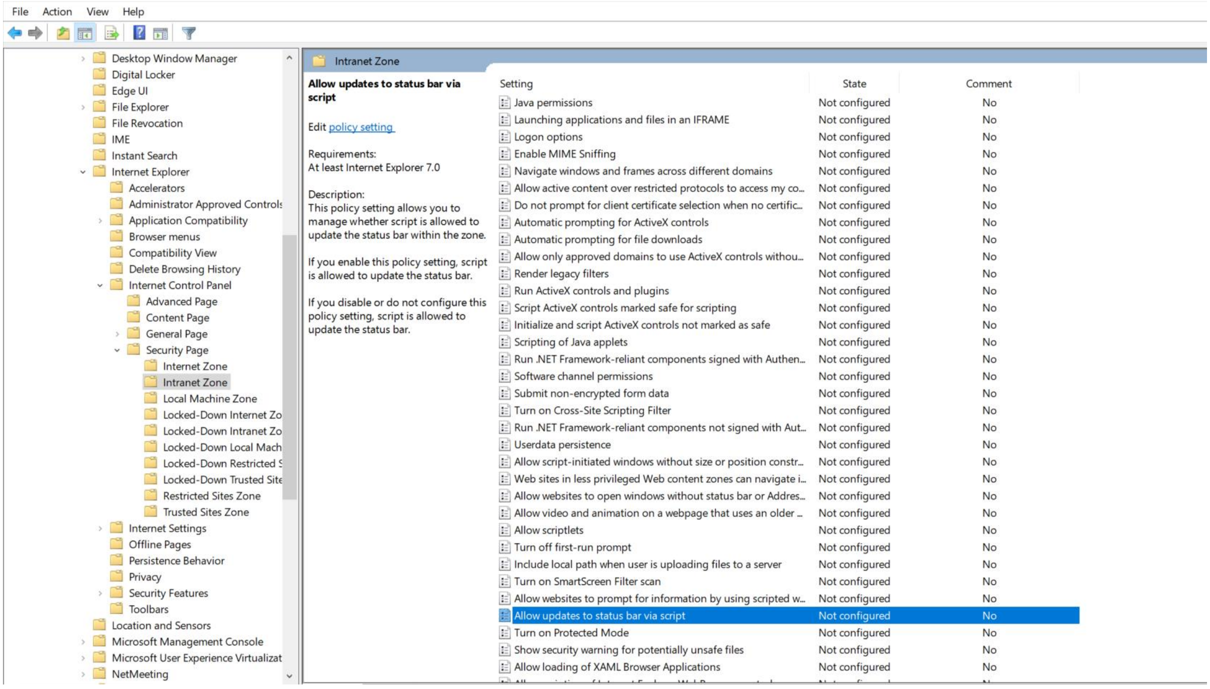
Enter the zone assignments here.

Value name	Value
https://autologon.microsoftazuread-sso.co...	1

...are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local computer.)

If you enable this policy setting, you can enter a list of sites and their related zone numbers. The association of a site with a zone will ensure that the security settings for the specified zone are applied to the site. For each entry that you add to the list, enter

Now under the Internet control Panel → Security Page→ Intranet Zone→ Allow updates to status bar via script.



Allow updates to status bar via script

Edit policy setting

Requirements:
At least Internet Explorer 7.0

Description:
This policy setting allows you to manage whether script is allowed to update the status bar within the zone.

If you enable this policy setting, script is allowed to update the status bar.

If you disable or do not configure this policy setting, script is allowed to update the status bar.

Setting	State	Comment
Java permissions	Not configured	No
Launching applications and files in an IFRAME	Not configured	No
Logon options	Not configured	No
Enable MIME Sniffing	Not configured	No
Navigate windows and frames across different domains	Not configured	No
Allow active content over restricted protocols to access my co...	Not configured	No
Do not prompt for client certificate selection when no certific...	Not configured	No
Automatic prompting for ActiveX controls	Not configured	No
Automatic prompting for file downloads	Not configured	No
Allow only approved domains to use ActiveX controls withou...	Not configured	No
Render legacy filters	Not configured	No
Run ActiveX controls and plugins	Not configured	No
Script ActiveX controls marked safe for scripting	Not configured	No
Initialize and script ActiveX controls not marked as safe	Not configured	No
Scripting of Java applets	Not configured	No
Run .NET Framework-reliant components signed with Authen...	Not configured	No
Software channel permissions	Not configured	No
Submit non-encrypted form data	Not configured	No
Turn on Cross-Site Scripting Filter	Not configured	No
Run .NET Framework-reliant components not signed with Aut...	Not configured	No
Userdata persistence	Not configured	No
Allow script-initiated windows without size or position constr...	Not configured	No
Web sites in less privileged Web content zones can navigate i...	Not configured	No
Allow websites to open windows without status bar or Addres...	Not configured	No
Allow video and animation on a webpage that uses an older ...	Not configured	No
Allow scriptlets	Not configured	No
Turn off first-run prompt	Not configured	No
Include local path when user is uploading files to a server	Not configured	No
Turn on SmartScreen Filter scan	Not configured	No
Allow websites to prompt for information by using scripted w...	Not configured	No
Allow updates to status bar via script	Not configured	No
Turn on Protected Mode	Not configured	No
Show security warning for potentially unsafe files	Not configured	No
Allow loading of XAML Browser Applications	Not configured	No

Double click on this Policy click on Apply and Ok.

Now go to User Configuration→ Preferences → Windows Settings→ Registry now right click on registry click on new→Registry Item

Follow this article: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sso-quick-start

To update the values in the registry.

Now go to command prompt: gpupdate /force.