Configuring Hybrid Azure AD

Prerequisites:

* An up-to-date version of Azure AD connect (Installed on Azure AD Connect Server)

1. <https://www.microsoft.com/en-us/download/details.aspx?id=47594>

There are three different scenarios at “User Sign-In Methods” :

1. Password Hash Synchronization with Enable Single Sign On :

The simplest option and suitable for most of the Microsoft 365 SMB users.

A screenshot of a cell phone

Description generated with very high confidence

1. Pass-through Authentication with Enable Single Sign On :

This is an acceptable solution, **suitable for M365B customers that do not want to store password hashes outside of their directory**. Customers will need to consider high availability of the agent so that users can still authenticate to Office 365 if there is a disruption of their on-premises network connection. If there aren’t any HA agent, the sign in operation will fail.

A screenshot of a cell phone

Description generated with very high confidence

1. Federation with AD FS:

This scenario is not recommended for M365B SMB customers because it introduces unnecessary complexity and does not map to typical SMB scenarios. And at the same time customer have to configure a HA solution because the AD FS is located on customer site and sign in operation works through it.

* Azure AD connect has synchronized the computer objects of the devices you want to be hybrid Azure AD joined to Azure AD. If the computer objects belong to specific organizational units (OU), then these OUs need to be configured for synchronization in Azure AD connect as well.
* If the customer plans a managed or staged hybrid domain-join scenario, keep in mind that the selected (listened) OU will be available for hybrid join. If the computer object OU is not listened and not synced, the hybrid domain-join operation will fail.
* For a staged operation we can create an OU different that the “Computers” OU which will be listed by Azure AD Connect for computer objects

A screenshot of a cell phone

Description generated with very high confidence

A screenshot of a cell phone

Description generated with very high confidence

**KEEP IN MIND** you must select the Computer OU which you want to Join Azure AD in hybrid scenario

Azure AD Connect : (IF NEEDED WE CAN ADD AZURE AD CONNECT INSTALLATION MANUAL)

Keeps the association between the computer account in your on-premises Active Directory (AD) and the device object in Azure AD.

Enables other device related features like Windows Hello for Business.

Make sure that the following URLs are accessible from computers inside your organization network for registration of computers to Azure AD:

https://enterpriseregistration.windows.net

https://login.microsoftonline.com

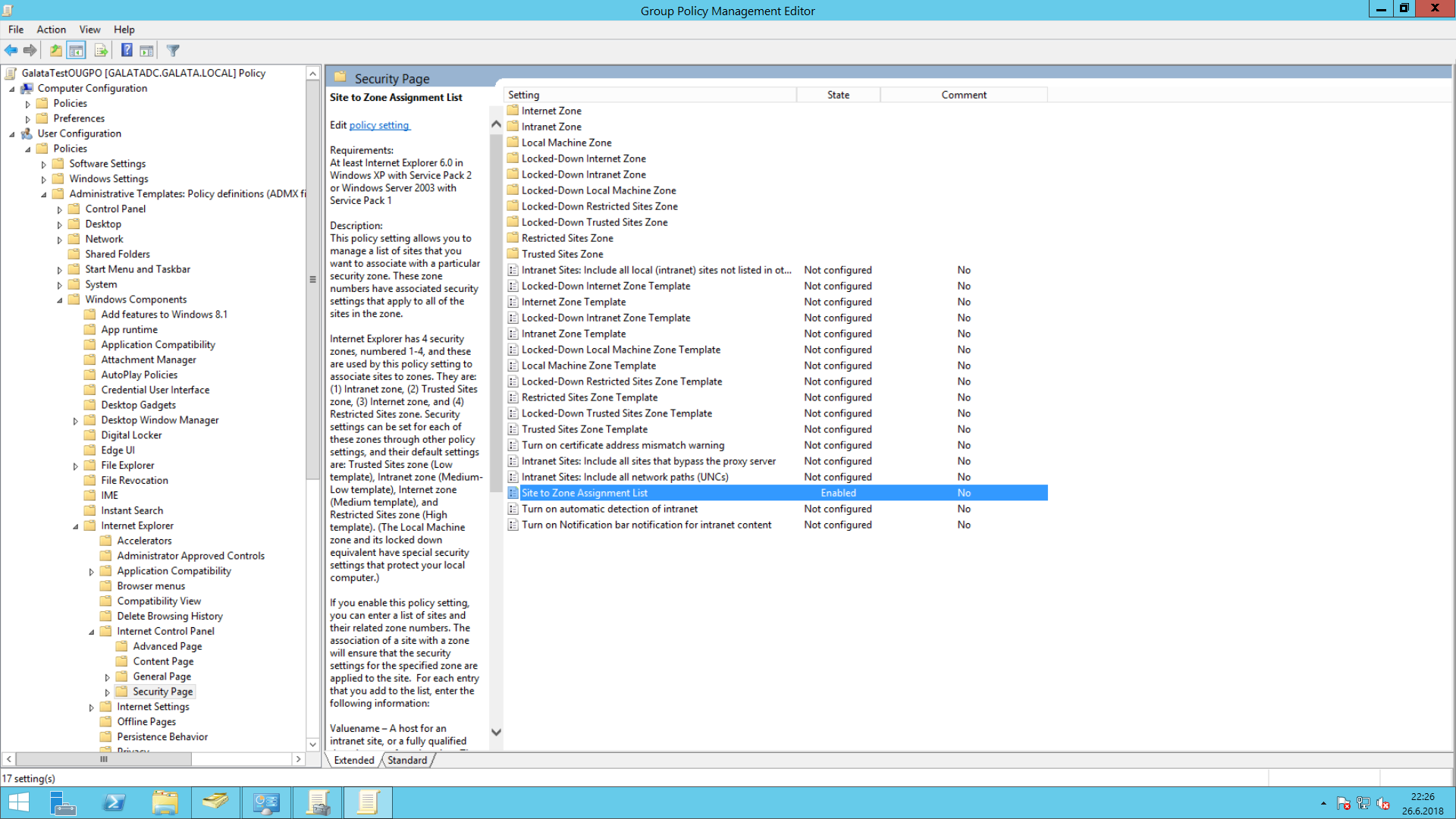
<https://device.login.microsoftonline.com>

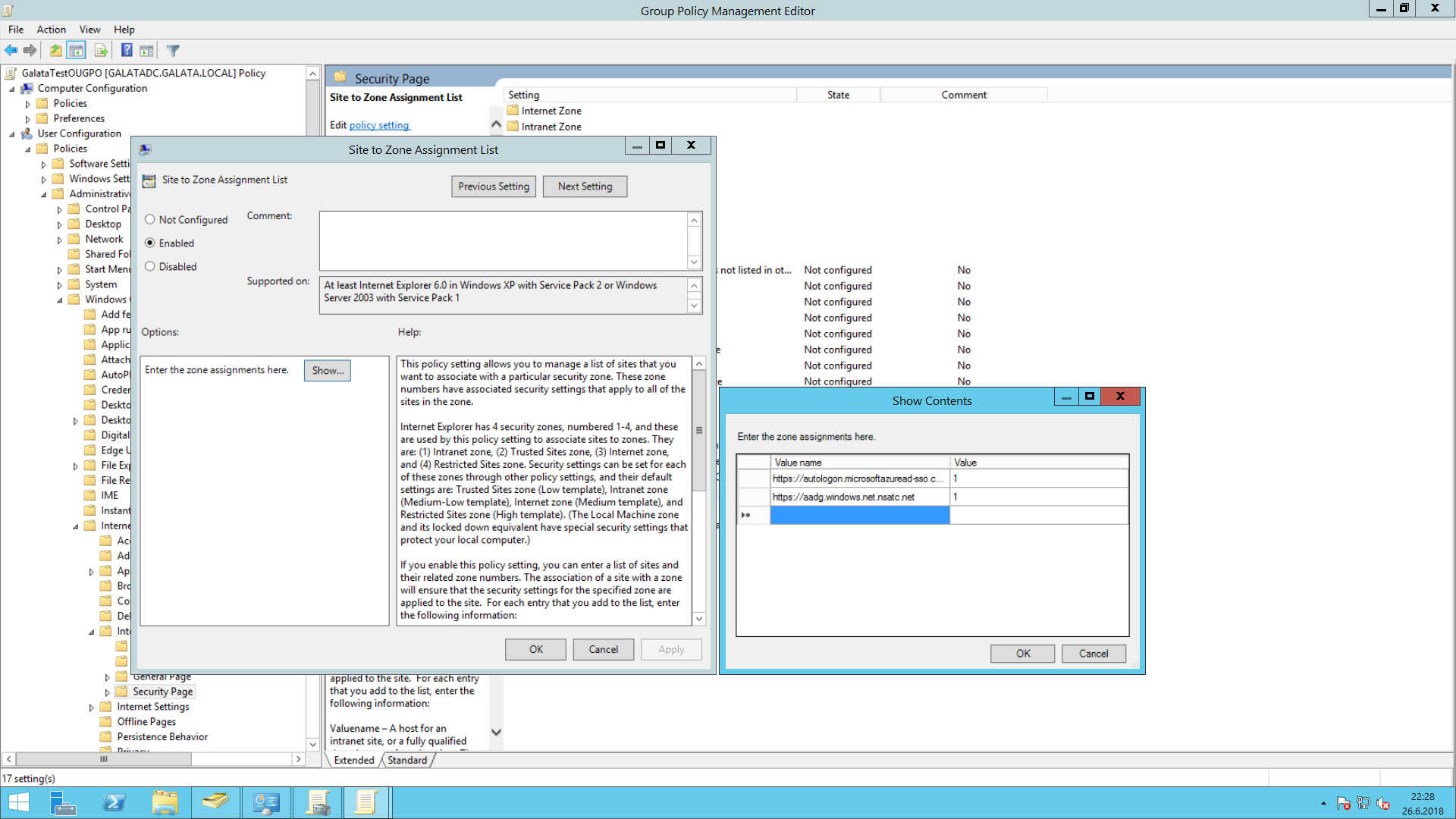
If your organization is planning to use Seamless SSO, then the following URLs need to be reachable from the computers inside your organization and they must also be added to the user's local intranet zone:

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

[**https://aadg.windows.net.nsatc.net**](https://aadg.windows.net.nsatc.net) **(enable with GPO)**

Also, the following setting should be enabled in the user's intranet zone: "Allow status bar updates via script." Use GPO for this operation.





**KEEP IN MIND** Apply the GPO to the OU which you want to sync for managed distribution.

If your organization requires access to the Internet via an outbound proxy, you must implement Web Proxy Auto-Discovery (WPAD) to enable Windows 10 computers to register to Azure AD.

***For Pass-Through Seamless Single Sign On Scenario*** you must have a verified domain on Azure AD and/or Office 365 Directory. You have to change users logon UPN suffix to the verified domain if you are using “domain.local” for login at local active directory. If a verified domain is not set up on local directory add it first.

A screenshot of a social media post

Description generated with very high confidence

A screenshot of a computer

Description generated with very high confidence

**KEEP IN MIND** This operation do not change the log in habit of users for computer logon. But in some operations on administration level it will be effected. So please inform the users to use new logon suffix if needed.

**KEEP IN MIND** If you are using Azure AD and/or Office 365 platform before configuring Azure AD Connect, the password for log in to the Office 365 platform will be different than the local domain password. After this operation the local domain password and Office 365 services password will be the same. Some inform the users that the Office 365 services password will be the same with local domain password. And some services will need re-enter the new password.

**KEEP IN MIND** Seamless single sign on scenario, after log in to the computer supported browsers will be log in automatically to the office 365 services from the supported browsers and this property will not work in Browsers Private Sessions.

**Configure service connection point:**

The service connection point (SCP) object is used by your devices during the registration to discover Azure AD tenant information. In your on-premises Active Directory (AD), the SCP object for the hybrid Azure AD joined devices must exist in the configuration naming context partition of the computer's forest. There is only one configuration naming context per forest. In a multi-forest Active Directory configuration, the service connection point must exist in all forests containing domain-joined computers.

You can use the ***Get-ADRootDSE*** cmdlet to retrieve the configuration naming context of your forest.

For a forest with the Active Directory domain name fabrikam.com, the configuration naming context is:

***CN=Configuration,DC=fabrikam,DC=com***

***A screenshot of a cell phone

Description generated with very high confidence***

Depending on how you have deployed Azure AD Connect, the SCP object may have already been configured. You can verify the existence of the object and retrieve the discovery values using the following Windows PowerShell script:

***$scp = New-Object System.DirectoryServices.DirectoryEntry;***

***$scp.Path = "LDAP://CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=fabrikam,DC=com";***

***$scp.Keywords;***

The $scp.Keywords output shows the Azure AD tenant information, for example:

**azureADName:microsoft.com**

**azureADId:72f988bf-86f1-41af-91ab-2d7cd011db47**

A screenshot of a social media post

Description generated with very high confidence

If the service connection point does not exist, you can create it by running the Initialize-ADSyncDomainJoinedComputerSync cmdlet on your Azure AD Connect server. Enterprise admin credential is required to run this cmdlet.

The cmdlet:

* Creates the service connection point in the Active Directory forest Azure AD Connect is connected to.
* Requires you to specify the AdConnectorAccount parameter. This is the account that is configured as Active Directory connector account in Azure AD connect.

The following script shows an example for using the cmdlet. In this script, $aadAdminCred = Get-Credential requires you to type a user name. You need to provide the user name in the user principal name (UPN) format ([user@example.com](mailto:user@example.com)).

***Import-Module -Name "C:\Program Files\Microsoft Azure Active Directory Connect\AdPrep\AdSyncPrep.psm1";***

***$aadAdminCred = Get-Credential;***

***Initialize-ADSyncDomainJoinedComputerSync –AdConnectorAccount [connector account name] -AzureADCredentials $aadAdminCred;***

**KEEP IN MIND**

* Uses the Active Directory PowerShell module and AD DS Tools, which rely on Active Directory Web Services running on a domain controller. Active Directory Web Services is supported on domain controllers running Windows Server 2008 R2 and later.
* Is only supported by the MSOnline PowerShell module version 1.1.166.0.
* If the AD DS tools are not installed, the Initialize-ADSyncDomainJoinedComputerSync will fail. The AD DS tools can be installed through Server Manager under Features - Remote Server Administration Tools - Role Administration Tools.

**Control deployment and rollout**

All domain-joined devices running Windows 10 Anniversary Update and Windows Server 2016 automatically register with Azure AD at device restart or user sign-in.

New devices register with Azure AD when the device restarts after the domain join operation is completed.

Devices that were previously Azure AD registered (for example, for Intune) transition to “Domain Joined, AAD Registered”; however it takes some time for this process to complete across all devices due to the normal flow of domain and user activity

**KEEP IN MIND** You can use a Group Policy object to control the rollout of automatic registration of Windows 10 and Windows Server 2016 domain-joined computers. If you do not want these devices to automatically register with Azure AD or you want to control the registration, then you must roll out group policy disabling the automatic registration to all these devices first, before starting with configuration steps. After you are done configuring, and when you are ready to test, you must roll out group policy enabling the automatic registration only to the test devices and then to all other devices as you choose

Open Server Manager, and then go to Tools > Group Policy Management.

Go to the domain node that corresponds to the domain where you want to activate auto-registration of Windows current computers.

Right-click Group Policy Objects, and then select New.

Type a name for your Group Policy object. For example, \*Hybrid Azure AD join.

Click OK.

Right-click your new Group Policy object, and then select Edit.

Go to Computer Configuration > Policies > Administrative Templates > Windows Components > Device Registration.

Right-click Register domain-joined computers as devices, and then select Edit.

A screenshot of a computer

Description generated with very high confidence

A screenshot of a computer

Description generated with very high confidence

If you are running a pre local domain joined machine you have to update the GPO rules by this command:

**gpupdate /force**

**KEEP IN MIND**

* you have synced the devices and users with Azure AD
* you have updated the applied GPO on computer
* some features and “**Windows 10 Business”** upgrade may take some time to apply and may need restart of client devices.