Migrating to Office 365 – Step by Step

Volume 1

Dave Kawula - MVP

Cristal Kawula - MVP

Cary Sun – Cisco Champion (CCIE)

PUBLISHED BY

MVPDays Publishing
http://www.mvpdays.com

ISBN:TBA

Warning and Disclaimer

Every effort has been made to make this manual as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Feedback Information

We'd like to hear from you! If you have any comments about how we could improve the quality of this book, please don't hesitate to contact us by visiting www.checkyourlogs.net or sending an email to feedback@mvpdays.com.

Acknowledgements

From Dave

Cristal, you are my rock and my source of inspiration.   For the past 20 + years you have been there with me every step of the way.   Not only are you the "BEST Wife" in the world you are my partner in crime. Christian, Trinity, Keira, Serena, Mickaila and Mackenzie, you kids are so patient with your dear old dad when he locks himself away in the office for yet another book. Taking the time to watch you grow in life, sports, and become little leaders of this new world is incredible to watch.

Thank you, Mom and Dad (Frank and Audry) and my brother Joe. You got me started in this crazy IT world when I was so young.   Brother, you mentored me along the way both coaching me in hockey and helping me learn what you knew about PC's and Servers.   I'll never forget us as teenage kids working the IT Support contract for the local municipal government.   Remember dad had to drive us to site because you weren't old enough to drive ourselves yet.   A great career starts with the support of your family and I'm so lucky because I have all the support one could ever want.

A book like this filled with amazing Canadian MVP's would not be possible without the support from the #1 Microsoft Community Program Manager – Simran Chaudry.   You have guided us along the path and helped us to get better at what we do every day.   Your job is tireless and your passion and commitment make us want to do what we do even more.

Last but not least, the MVPDays volunteers, you have donated your time and expertise and helped us run the event in over 20 cities across North America.   Our latest journey has us expanding the conference worldwide as a virtual conference.   For those of you that will read this book your potential is limitless just expand your horizons and you never know where life will take you.

About the Authors

Dave Kawula - MVP

Dave is a Microsoft Most Valuable Professional (MVP) with over 20 years of experience in the IT industry. His background includes data communications networks within multi-server environments, and he has led architecture teams for virtualization, System Center, Exchange, Active Directory, and Internet gateways. Very active within the Microsoft technical and consulting teams, Dave has provided deep-dive technical knowledge and subject matter expertise on various System Center and operating system topics.

Dave is well-known in the community as an evangelist for Microsoft, 1E, and Veeam technologies. Locating Dave is easy as he speaks at several conferences and sessions each year, including TechEd, Ignite, MVP Days Community Roadshow, and VeeamOn.

Recently Dave has been honored to take on the role of Conference Co-Chair of TechMentor with fellow MVP Sami Laiho. The lineup of speakers and attendees that have been to this conference over the past 20 years is really amazing. Come down to Redmond or Orlando in 2018 and you can meet him in person.

As the founder and Managing Principal Consultant at TriCon Elite Consulting, Dave is a leading technology expert for both local customers and large international enterprises, providing optimal guidance and methodologies to achieve and maintain an efficient infrastructure.

BLOG: www.checkyourlogs.net

Twitter: @DaveKawula

Cristal Kawula – MVP

Cristal Kawula is the co-founder of MVPDays Community Roadshow and #MVPHour live Twitter Chat.   She is the President of TriCon Elite Consulting where she manages the day to day operations of the field consulting and sales teams.

Cristal is also only the 2nd Woman in the world to receive the prestigious Veeam Vanguard Community excellence award. In July of 2017 she was awarded the designation of Microsoft MVP.

Early in her career Cristal worked as a consultant with Microsoft authoring content for internal SMSGR and GTR teams.   This content was used to train internal support engineers and global escalation engineering teams.

Cristal can be found speaking at Microsoft Ignite, MVPDays, and other local user groups.   She is extremely active in the community and has recently helped publish a book for other Women MVP’s called Voices from the Data Platform.

BLOG: http://www.checkyourlogs.net

Twitter: @supercristal1

MVP Microsoft® Most Valuable Professional

Cary Sun – CCIE #4531 (Cisco Champion)

Cary Sun is CISCO CERTIFIED INTERNETWORK EXPERT (CCIE No.4531) and MCSE, MCIPT, Citrix CCA with over twenty years in the planning, design, and implementation of network technologies and Management and system integration. Background includes hands-on experience with multi-platform, all LAN/WAN topologies, network administration, E-mail and Internet systems, security products, PCs and Servers environment. Expertise analyzing user's needs and coordinating system designs from concept through implementation. Exceptional analysis, organization, communication, and interpersonal skills. Demonstrated ability to work independently or as an integral part of team to achieve objectives and goals. Specialties: CCIE /CCNA / MCSE / MCITP / MCTS / MCSA / Solution Expert / CCA

Cary's is a very active blogger at checkyourlogs.net and always available online for questions from the community. He passion about technology is contagious and he makes everyone around him better at what they do.

Blog:http://www.checkyourlogs.net

Twitter:@SifuSun

Contents

Introduction

North American MVPDays Community Roadshow

The purpose of this book is to showcase the amazing expertise of our guest speakers at the North American MVPDays Community Roadshow.   They have so much passion, expertise, and expert knowledge that it only seemed fitting to write it down in a book.

MVPDays was founded by Cristal and Dave Kawula back in 2013. It started as a simple idea; “There’s got to be a good way for Microsoft MVPs to reach the IT community and share their vast knowledge and experience in a fun and engaging way” I mean, what is the point in recognizing these bright and inspiring individuals, and not leveraging them to inspire the community that they are a part of.

We often get asked the question “Who should attend MVPDays”?

Anyone that has an interest in technology, is eager to learn, and wants to meet other like-minded individuals.   This Roadshow is not just for Microsoft MVP’s it is for anyone in the IT Community.

Make sure you check out the MVPDays website at: www.mvpdays.com. You never know maybe the roadshow will be coming to a city near you.

The goal of this particular book is to bring you real world step-by-step guidance from our expert MVP Authors on Migrating to Office 365 from an on premises Exchange environment. It has been written with the most current techniques possible to help with your migrations and learning process.

Sample Files

All sample files for this book can be downloaded from www.checkyourlogs.net and www.github.com/dkawula

Additional Resources

In addition to all tips and tricks provided in this book, you can find extra resources like articles and video recordings on our blog http://www.checkyourlogs.net.

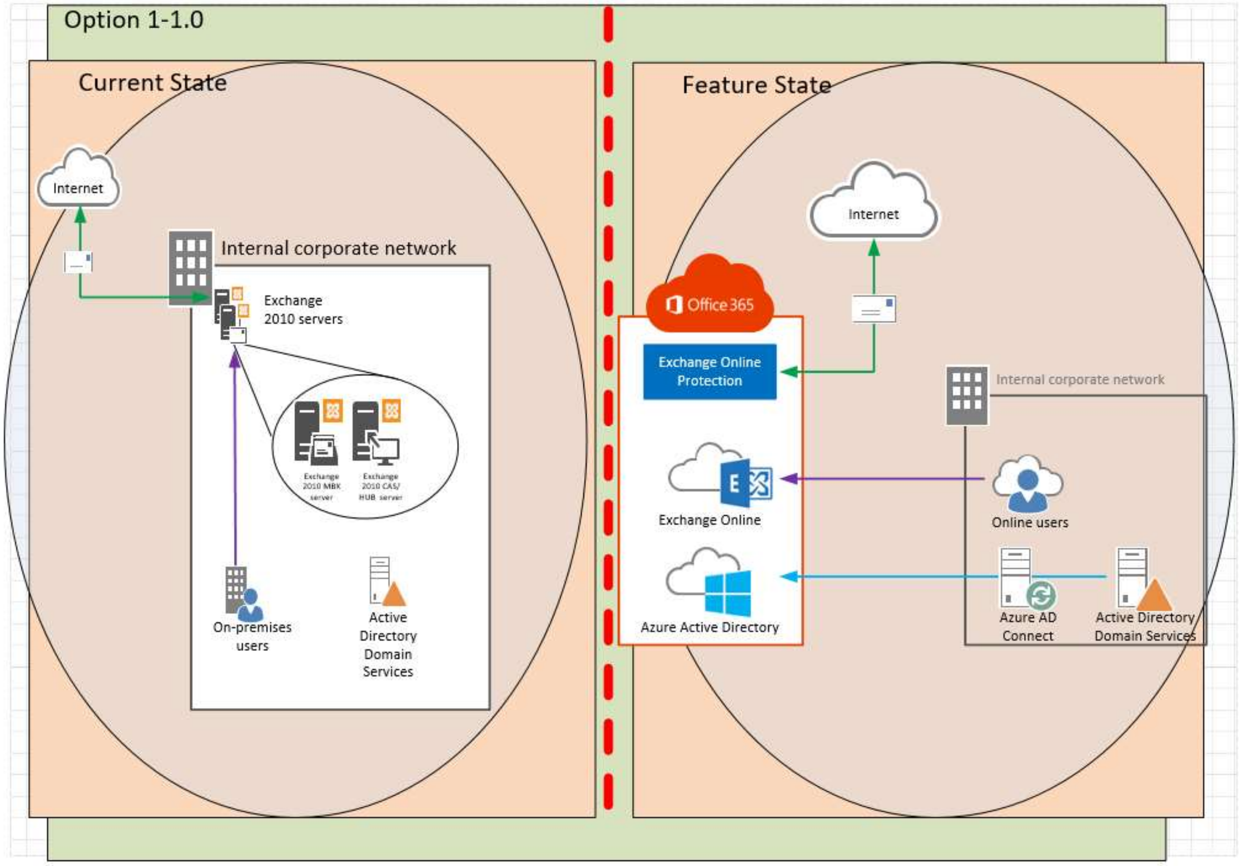
Chapter 1

Environment Overview

Exchange Migration to Office 365

This document serves as both a guideline for redeployment document for the Exchange Migration performed at the [Company]. The information within will be primarily prescriptive, but will include annotations of any issues encountered, as well as any issues that might arise should the need to redeploy occur.

The process described mainly focuses on a typical transition of Exchange 2010 (2016) to Office 365 environment, converting the Exchange 2010 (2016) server to Office 365 CAS role, HUB role and MBX role. Additional role options such as the Unified Messaging Server role and Edge Transport role, are out-of-scope within this document.



Prerequisites

On-premises Exchange organization

On-premises environment	Exchange 2016-based hybrid deployment	Exchange 2013-based hybrid deployment	Exchange 2010-based hybrid deployment

Exchange 2016	Supported	Not supported	Not supported
Exchange 2013	Supported	Supported	Not supported
Exchange 2010	Supported	Supported	Supported
Exchange 2007	Not supported	Supported	Supported

On-premises Exchange releases

Hybrid deployments require the latest cumulative update or update rollup available for the version of Exchange you have installed in your on-premises organization. If you can't install the latest cumulative update or update rollup, the immediately previous release is also supported. Older cumulative updates or update rollups aren't supported.

On-premises server roles

On-premises environment	Requirement
Exchange 2010	At least one server with the Mailbox, Hub Transport, and Client Access server roles installed. While it's possible to install the Mailbox, Hub Transport, and Client Access roles on separate servers, we strongly recommend that you install all of the roles on each server to provide additional reliability and improved performance
Exchange 2013	At least one server with the Mailbox and Client Access server roles installed. While it's possible to install the Mailbox and Client Access roles on separate servers, we strongly recommend that you install both roles on each server to provide additional reliability and improved performance

Exchange 2016 and newer	At least one server that has the Mailbox server role installed

Office 365

Hybrid deployments are supported in all Office 365 plans that support Azure Active Directory synchronization. All Office 365 Enterprise, Government, Academic and Midsize plans support hybrid deployments. Office 365 Business and Home plans don’t support hybrid deployments.

Custom domains

Register any custom domains you want to use in your hybrid deployment with Office 365. You can do this by using the Office 365 Administrative portal, or by optionally configuring Active Directory Federation Services (AD FS) in your on-premises organization.

Active Directory synchronization

Deploy the Azure Active Directory Connect tool to enable Active Directory synchronization with your on-premises organization.

Autodiscover DNS records

Configure the Autodiscover public DNS records for your existing SMTP domains to point to an on-premises Exchange 2010 (2013) Client Access server or Exchange 2016 server.

Office 365 organization in the Exchange admin center (EAC)

The Office 365 organization node is included by default in the on-premises EAC, but you must connect the EAC to your Office 365 organization using your Office 365 administrator credentials before you can use the Hybrid Configuration wizard. This also allows you to manage both the on-premises and Exchange Online organizations from a single management console.

Certificates (If Active Directory Federation Services is being deployed)

Install and assign Exchange services to a valid digital certificate purchased from a trusted public certificate authority (CA). Although self-signed certificates should be used for the on-premises federation trust with the Microsoft Federation Gateway, self-signed certificates can't be used for Exchange services in a hybrid deployment. The Internet Information Services (IIS) instance on the Exchange servers configured in the hybrid deployment must have a valid digital certificate purchased from a trusted CA. Additionally, the EWS external URL and the Autodiscover endpoint specified in your public DNS must be listed in Subject Alternative Name (SAN) of the certificate. The certificate installed on the Exchange servers used for mail transport in the hybrid deployment must all use the same certificate (that is, they are issued by the same CA and have the same subject).

Hybrid deployment protocols, ports, and endpoints

Hybrid deployment features and components require certain incoming protocols, ports and connection endpoints to be accessible to Office 365 in order to work correctly. Before configuring your hybrid deployment, verify that your on-premises network and security configuration can support the features and components in the table below.

Transport Protocol	Upper Level Protocol	Feature/Component	On-premises Endpoint	On-premises Path	Authentication Provider	Authorization Method
TCP 25 (SMTP)	SMTP/TLS	Mail flow between Office 365 and on-premises	Exchange 2016 Mailbox/Edge Exchange 2013 CAS/Edge Exchange 2010 HUB/Edge	N/A	N/A	Certificate-based
TCP 443	Autodiscover	Autodiscover	Exchange 2016 Mailbox	/autodiscover/autodiscover.svc /wssecurity	Azure AD authentica	WS-Security

(HTTPS)			Exchange 2013/2010 CAS	/autodiscover/autodiscover.svc	tion system	Authentication
TCP 443 (HTTPS)	EWS	Free/busy, MailTips, Message Tracking	Exchange 2016 Mailbox Exchange 2013/2010 CAS	/ews/exchange.asmx/wssecurity	Azure AD authentication system	WS-Security Authentication
TCP 443 (HTTPS)	EWS	Multi-mailbox search	Exchange 2016 Mailbox Exchange 2013/2010 CAS	/ews/exchange.asmx/wssecurity /autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc	Auth Server	WS-Security Authentication
TCP 443 (HTTPS)	EWS	Mailbox migrations	Exchange 2016 Mailbox Exchange 2013/2010 CAS	/ews/mrsproxy.svc	Basic	Basic
TCP 443 (HTTPS)	Autodiscover EWS	OAuth	Exchange 2016 Mailbox Exchange 2013/2010 CAS	/ews/exchange.asmx/wssecurity /autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc	Auth Server	WS-Security Authentication
TCP 443 (HTTPS)	N/A	AD FS (included with Windows)	Windows 2008/2012 Server	/adfs/*	Azure AD authentication system	Varies per config.

On-premises Active Directory

- The AD schema version and forest functional level must be Windows Server 2003 or later. The domain controllers can run any version as long as the schema and forest level requirements are met.
- If you plan to use the feature **password writeback**, then the Domain Controllers must be on Windows Server 2008 (with latest SP) or later. If your DCs are on 2008 (pre-R2), then you must also apply hotfix KB2386717
- The domain controller used by Azure AD must be writable. It is not supported to use a RODC (read-only domain controller) and Azure AD Connect does not follow any write redirects.
- It is not supported to use on-premises forests/domains using SLDs (Single Label Domains).
- It is not supported to use on-premises forests/domains using "dotted" (name contains a period ".") NetBIOS names.
- It is recommended to enable the Active Directory recycle bin

Hybrid Identity Required Ports and Protocols

Protocol	Ports	Description
HTTP	80 (TCP/UDP)	Used to download CRLs (Certificate Revocation Lists) to verify SSL certificates.
HTTPS	443(TCP/UDP)	Used to synchronize with Azure AD.
Azure Service Bus	5671 (TCP/UDP)	Outbound

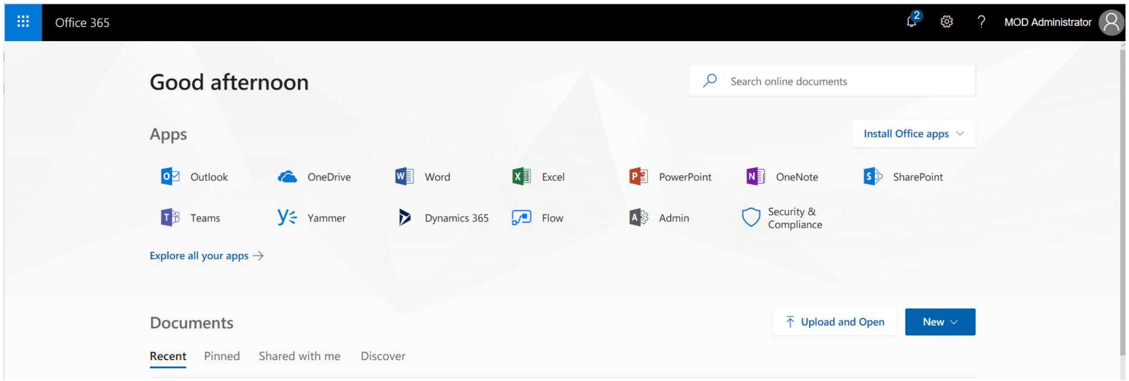
Chapter 2

Configure Azure AD (Office365)

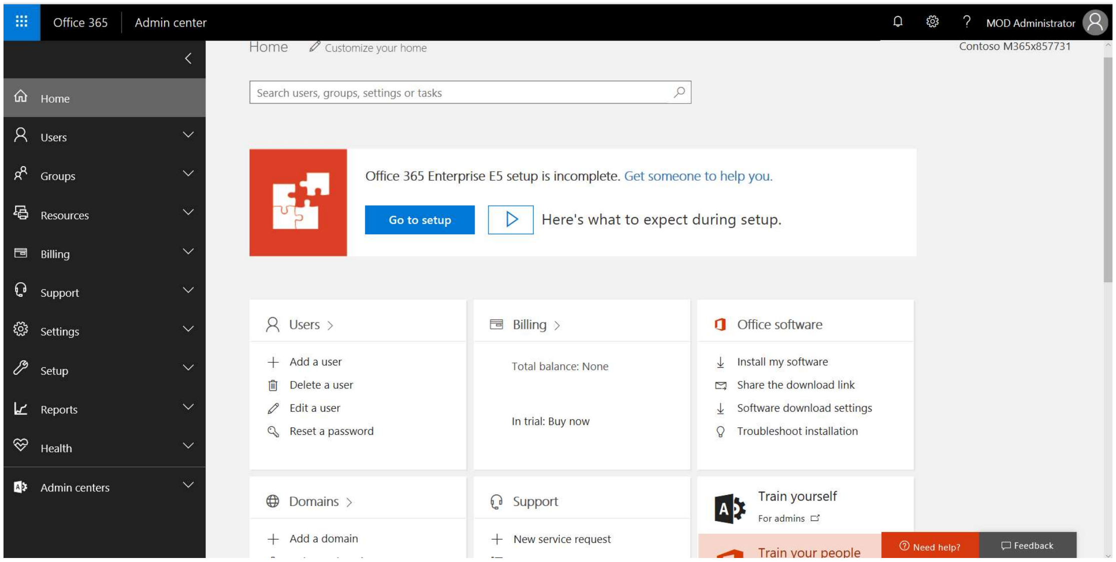
Add and verify the on-premise domain in Azure AD (Office 365)

We need to connect on-premise domain with office 365.

1. Login to office 365 tenant and then click **Admin**.



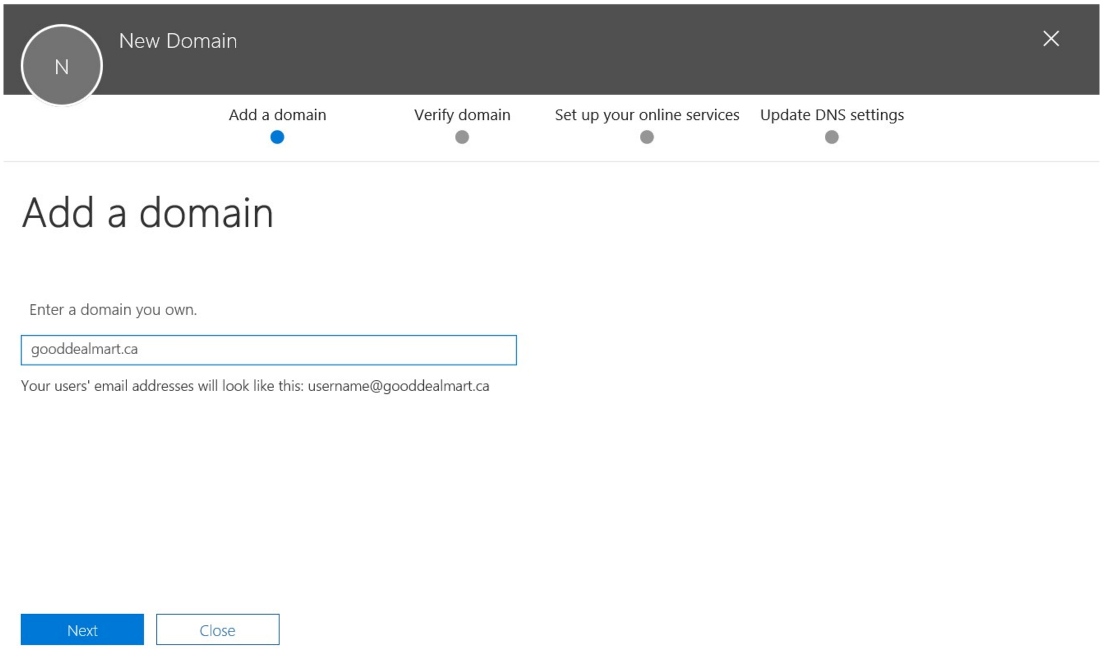
2. On the **Home** Page, click **Add a domain**.



Office 365 Enterprise E5 setup is incomplete. Get someone to help you.

Here's what to expect during setup.

3. Enter on-premise domain name to **Enter a domain you own**, click **Next**.



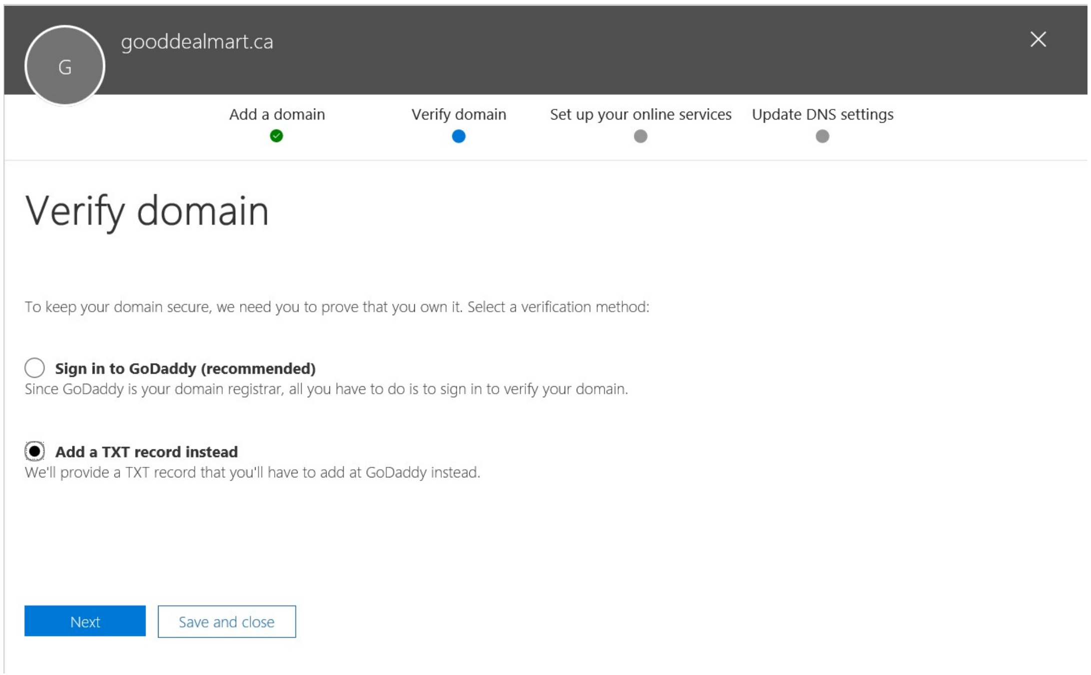
Add a domain

Enter a domain you own.

gooddealmart.ca

Your users' email addresses will look like this: username@gooddealmart.ca

4. On the **Verify domain** page, select Add a TXT record instead (if you own domain was not register with GoDaddy), click **Next**.



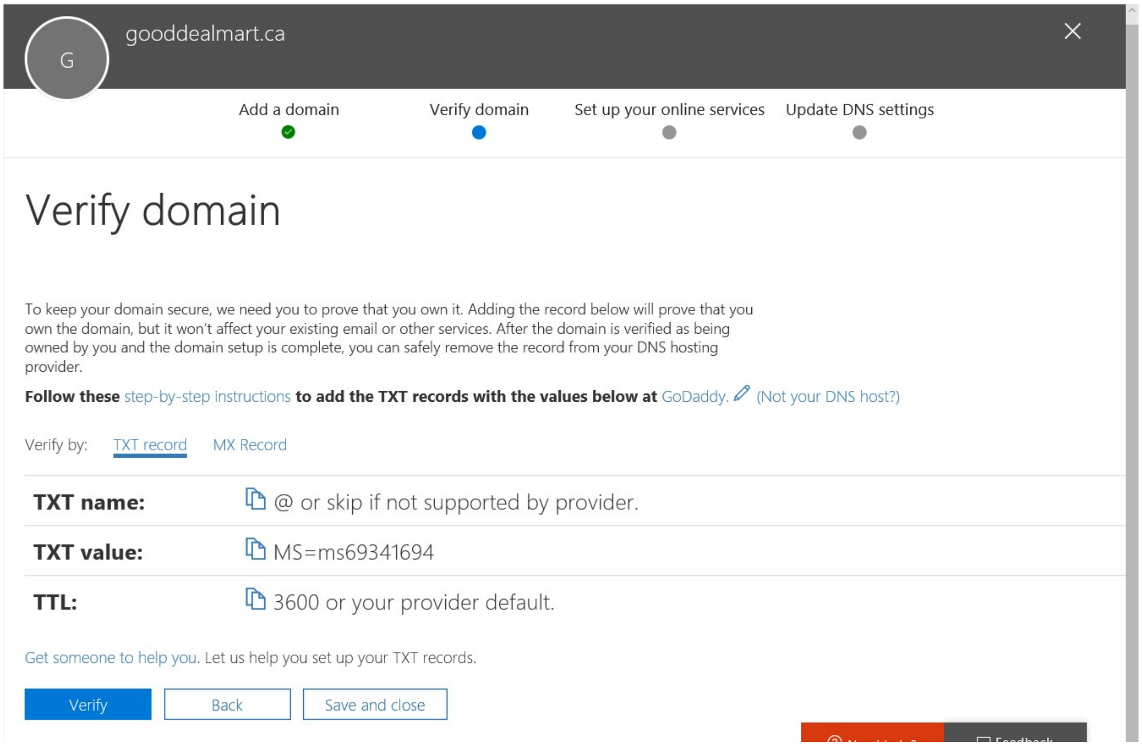
Verify domain

To keep your domain secure, we need you to prove that you own it. Select a verification method:

○ **Sign in to GoDaddy (recommended)**
Since GoDaddy is your domain registrar, all you have to do is to sign in to verify your domain.

● **Add a TXT record instead**
We'll provide a TXT record that you'll have to add at GoDaddy instead.

5. Add the TXT records to your DNS hosting and then click **Verify**.



Verify domain

To keep your domain secure, we need you to prove that you own it. Adding the record below will prove that you own the domain, but it won't affect your existing email or other services. After the domain is verified as being owned by you and the domain setup is complete, you can safely remove the record from your DNS hosting provider.

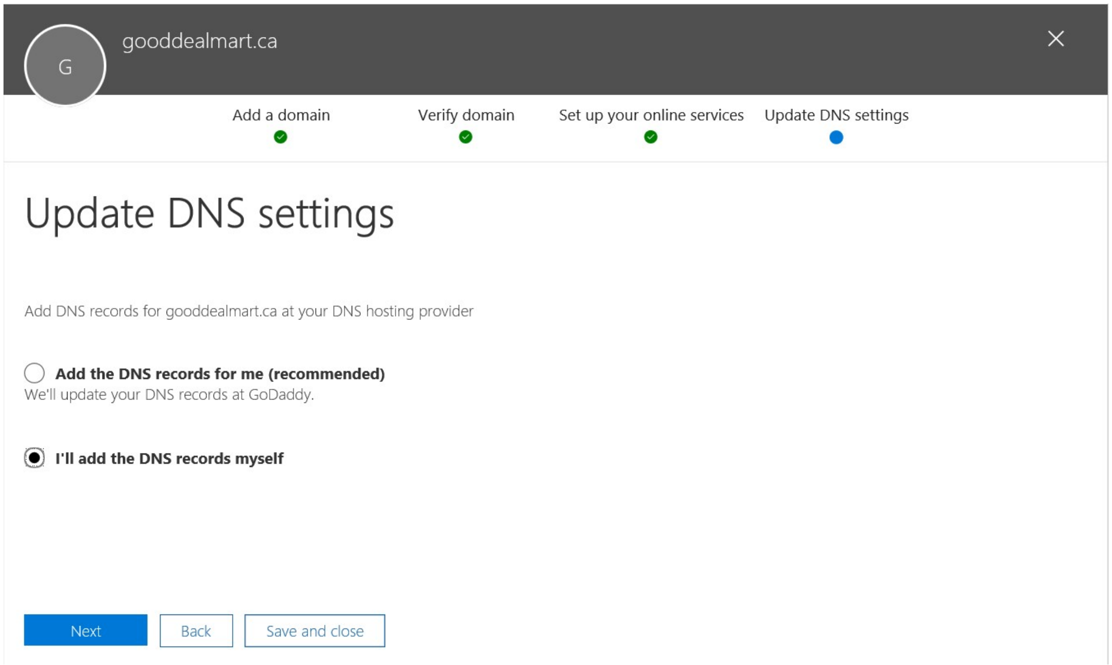
Follow these step-by-step instructions **to add the TXT records with the values below at** GoDaddy. (Not your DNS host?)

Verify by: TXT record MX Record

TXT name:	@ or skip if not supported by provider.
TXT value:	MS=ms69341694
TTL:	3600 or your provider default.

Get someone to help you. Let us help you set up your TXT records.

6. Select I'll add the DNS records myself, click Next.



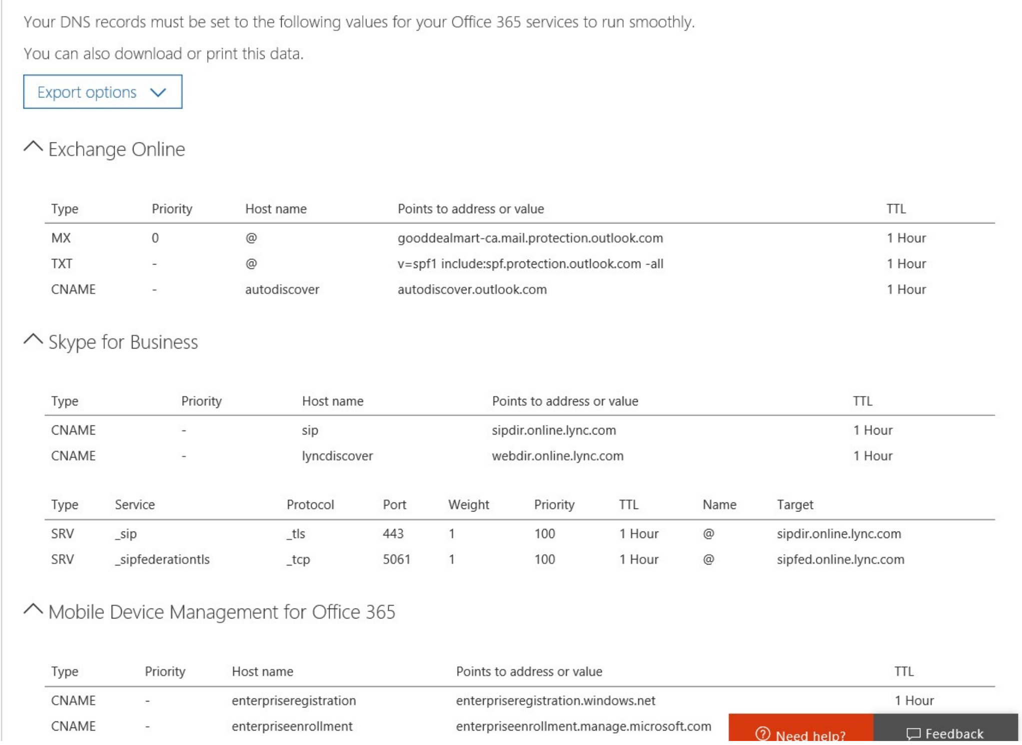
Update DNS settings

Add DNS records for gooddealmart.ca at your DNS hosting provider

○ **Add the DNS records for me (recommended)**
We'll update your DNS records at GoDaddy.

● **I'll add the DNS records myself**

7. Add all records and to your DNS hosting and then click Verify.



Your DNS records must be set to the following values for your Office 365 services to run smoothly.

You can also download or print this data.

Exchange Online

Type	Priority	Host name	Points to address or value	TTL
MX	0	@	gooddealmart-ca.mail.protection.outlook.com	1 Hour
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour

Skype for Business

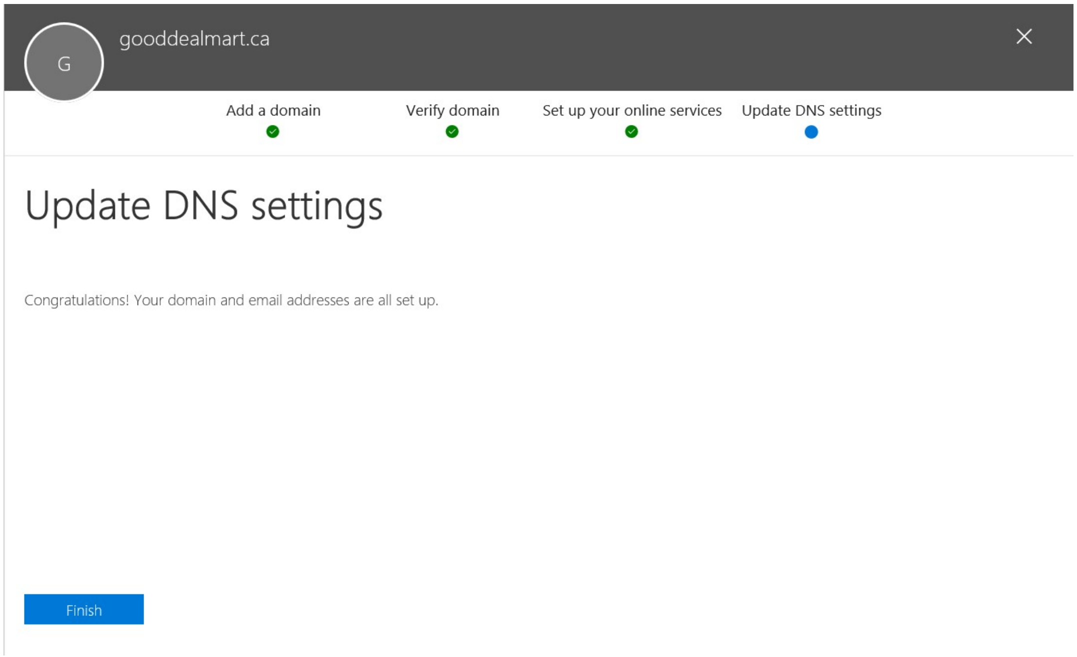
Type	Priority	Host name	Points to address or value	TTL
CNAME	-	sip	sipdir.online.lync.com	1 Hour
CNAME	-	lyncdiscover	webdir.online.lync.com	1 Hour

Type	Service	Protocol	Port	Weight	Priority	TTL	Name	Target
SRV	_sip	_tls	443	1	100	1 Hour	@	sipdir.online.lync.com
SRV	_sipfederationtls	_tcp	5061	1	100	1 Hour	@	sipfed.online.lync.com

Mobile Device Management for Office 365

Type	Priority	Host name	Points to address or value	TTL
CNAME	-	enterpriseregistration	enterpriseregistration.windows.net	1 Hour
CNAME	-	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	

8. Make sure all settings are correct and click Finish.



Update DNS settings

Congratulations! Your domain and email addresses are all set up.

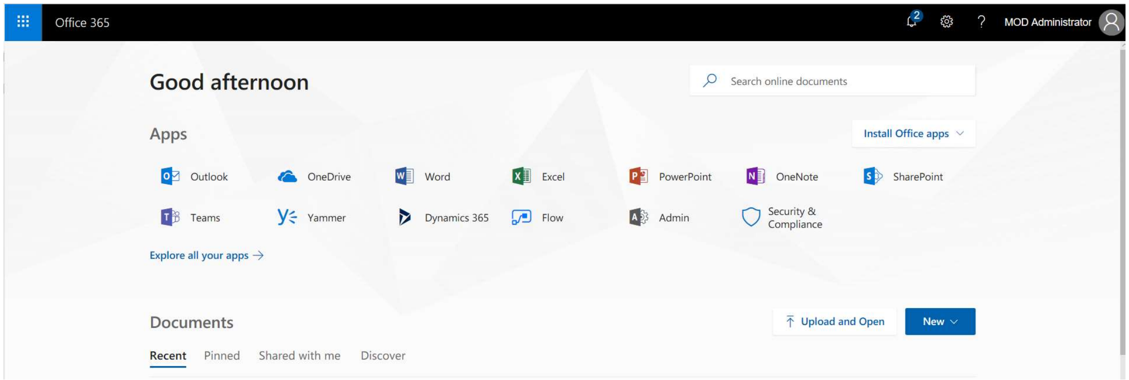
Chapter 3

Configuring Hybrid Identity with Office 365

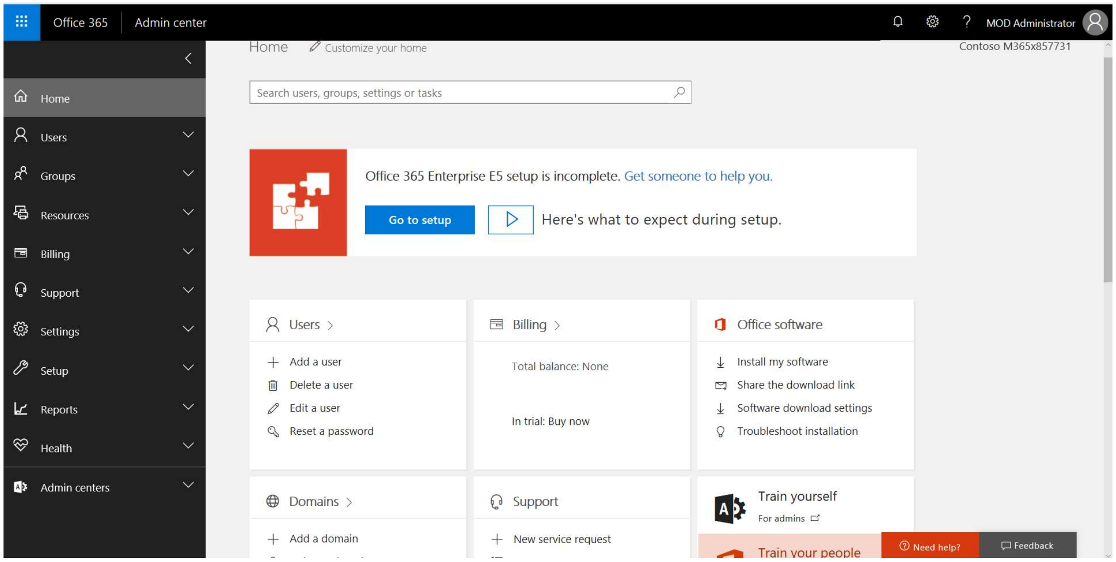
Add and verify the on-premise domain in Azure AD (Office 365)

We need to connect on-premise domain with office 365.

1. Login to office 365 tenant and then click **Admin**.



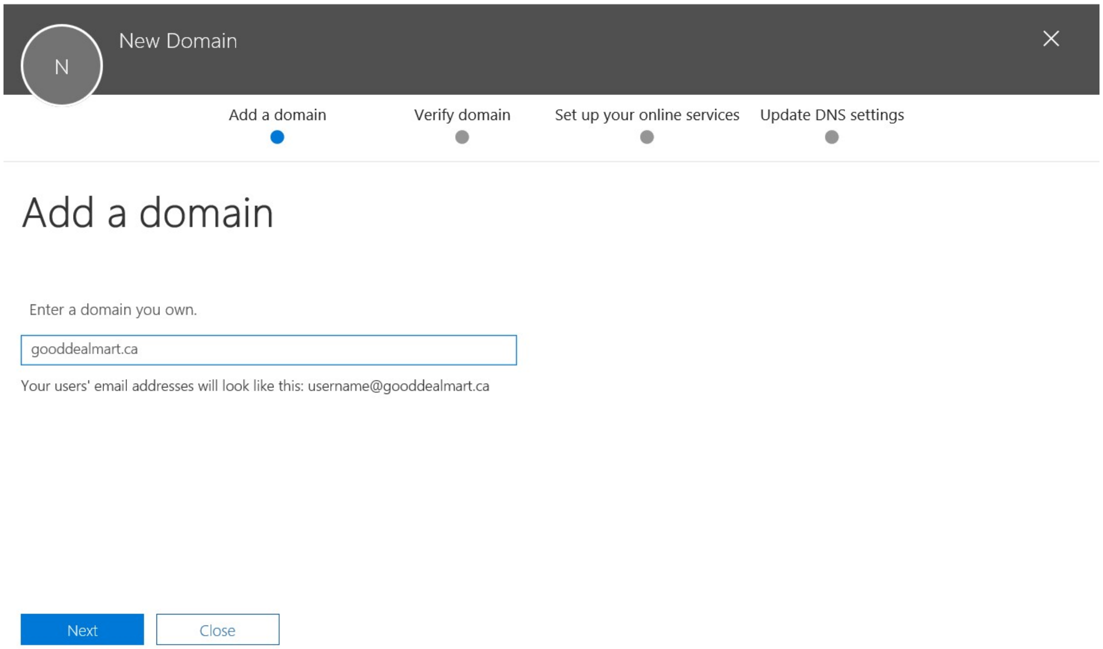
2. On the **Home** Page, click **Add a domain**.



Office 365 Enterprise E5 setup is incomplete. Get someone to help you.

Here's what to expect during setup.

3. Enter on-premise domain name to **Enter a domain you own**, click **Next**.



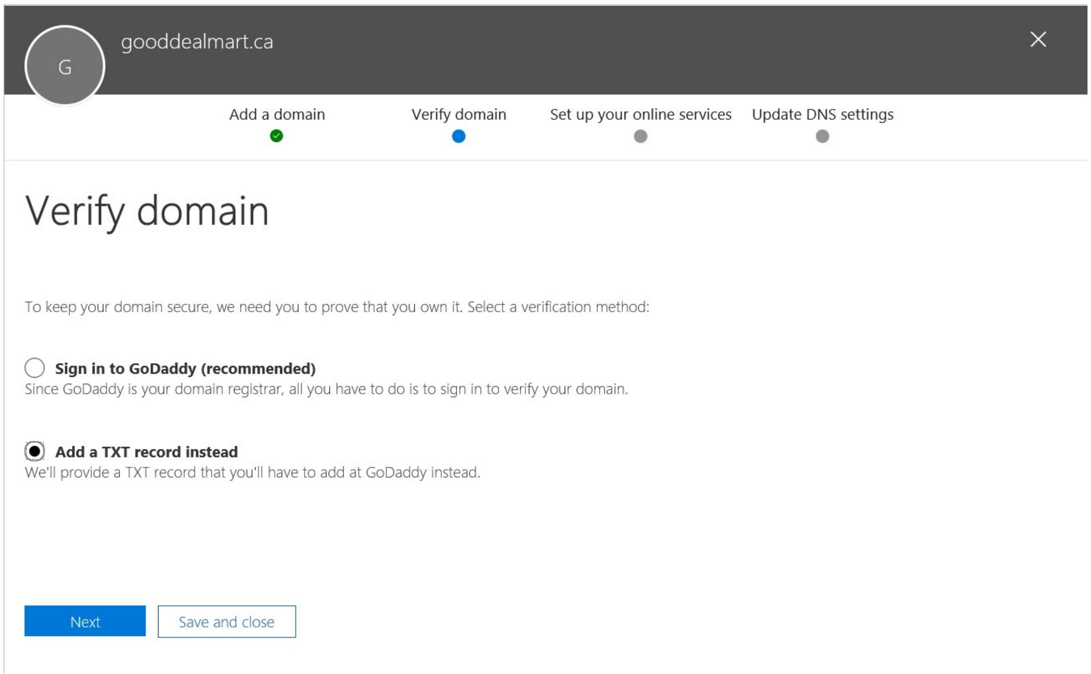
Add a domain

Enter a domain you own.

gooddealmart.ca

Your users' email addresses will look like this: username@gooddealmart.ca

4. On the **Verify domain** page, select Add a TXT record instead (if you own domain was not register with GoDaddy), click **Next**.



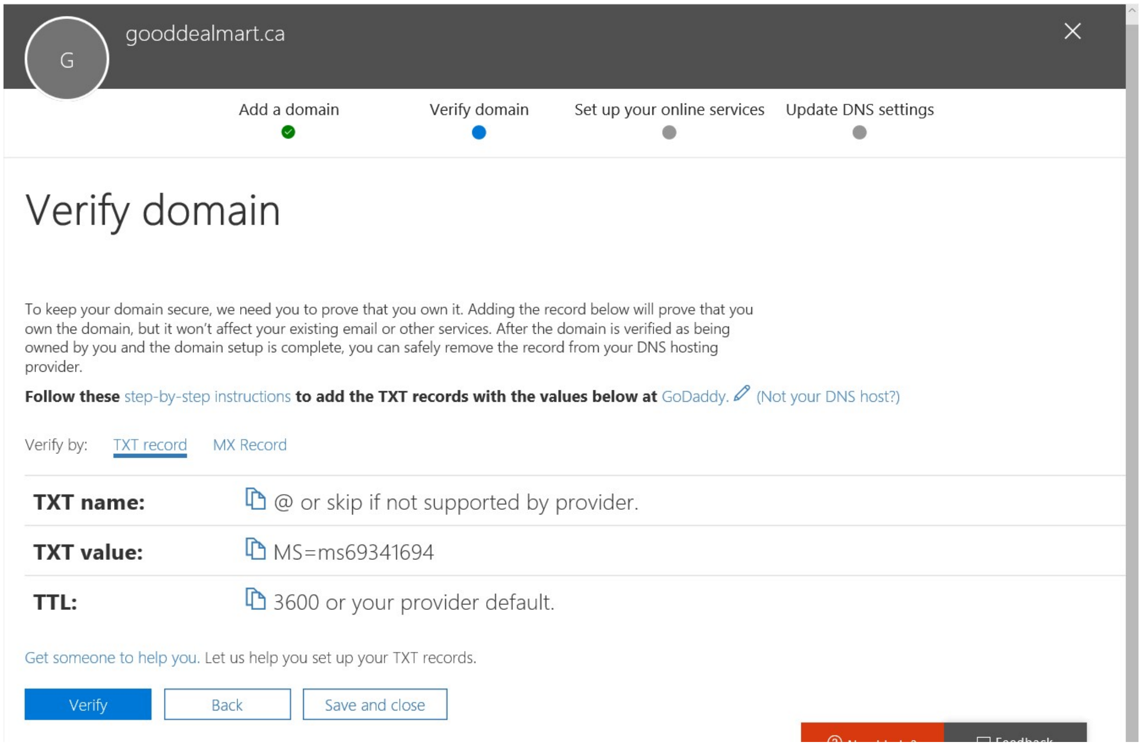
Verify domain

To keep your domain secure, we need you to prove that you own it. Select a verification method:

○ **Sign in to GoDaddy (recommended)**
Since GoDaddy is your domain registrar, all you have to do is to sign in to verify your domain.

● **Add a TXT record instead**
We'll provide a TXT record that you'll have to add at GoDaddy instead.

5. Add the TXT records to your DNS hosting and then click **Verify**.



Verify domain

To keep your domain secure, we need you to prove that you own it. Adding the record below will prove that you own the domain, but it won't affect your existing email or other services. After the domain is verified as being owned by you and the domain setup is complete, you can safely remove the record from your DNS hosting provider.

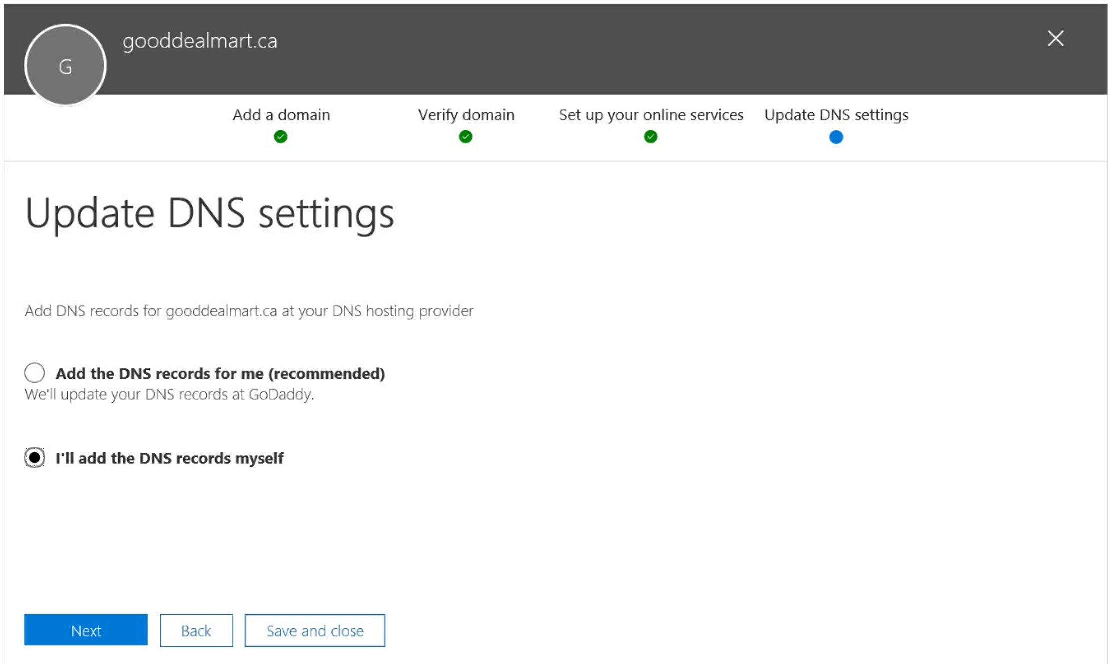
Follow these step-by-step instructions **to add the TXT records with the values below at** GoDaddy. (Not your DNS host?)

Verify by: TXT record MX Record

TXT name:	@ or skip if not supported by provider.
TXT value:	MS=ms69341694
TTL:	3600 or your provider default.

Get someone to help you. Let us help you set up your TXT records.

6. Select I'll add the DNS records myself, click Next.



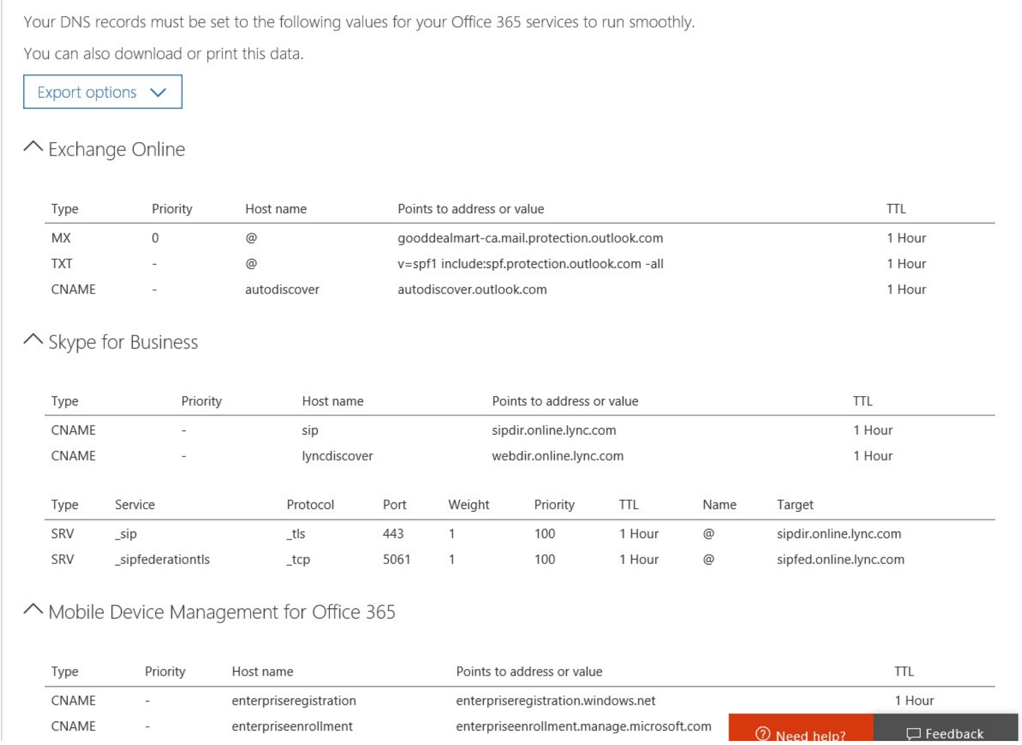
Update DNS settings

Add DNS records for gooddealmart.ca at your DNS hosting provider

○ **Add the DNS records for me (recommended)**
We'll update your DNS records at GoDaddy.

● **I'll add the DNS records myself**

7. Add all records and to your DNS hosting and then click Verify.



Your DNS records must be set to the following values for your Office 365 services to run smoothly.

You can also download or print this data.

Exchange Online

Type	Priority	Host name	Points to address or value	TTL
MX	0	@	gooddealmart-ca.mail.protection.outlook.com	1 Hour
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour

Skype for Business

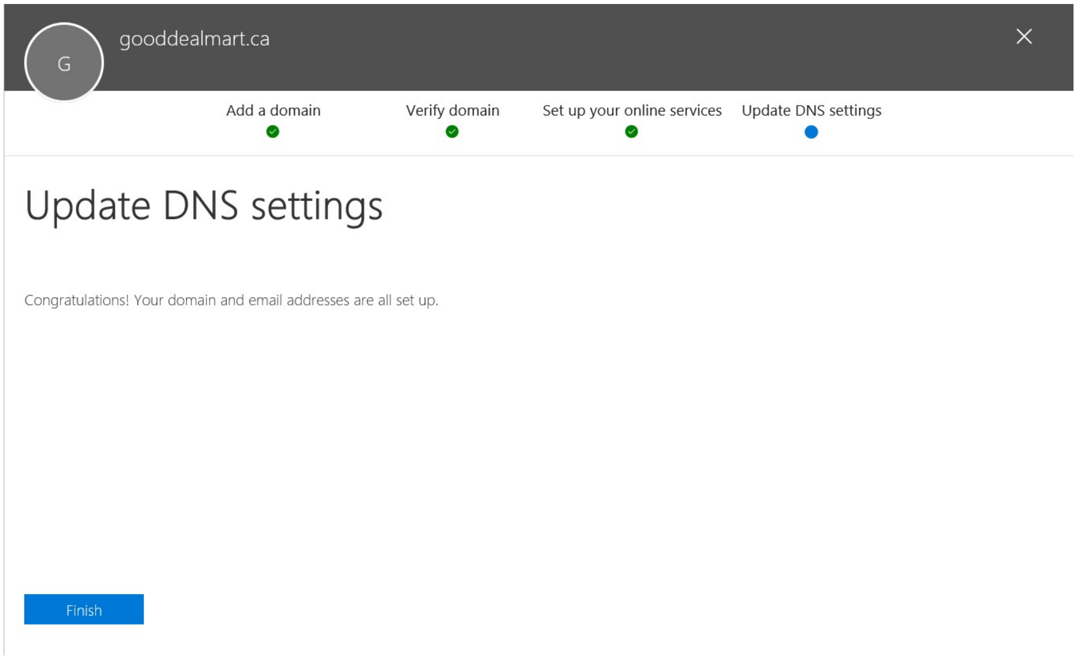
Type	Priority	Host name	Points to address or value	TTL
CNAME	-	sip	sipdir.online.lync.com	1 Hour
CNAME	-	lyncdiscover	webdir.online.lync.com	1 Hour

Type	Service	Protocol	Port	Weight	Priority	TTL	Name	Target
SRV	_sip	_tls	443	1	100	1 Hour	@	sipdir.online.lync.com
SRV	_sipfederationtls	_tcp	5061	1	100	1 Hour	@	sipfed.online.lync.com

Mobile Device Management for Office 365

Type	Priority	Host name	Points to address or value	TTL
CNAME	-	enterpriseregistration	enterpriseregistration.windows.net	1 Hour
CNAME	-	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	

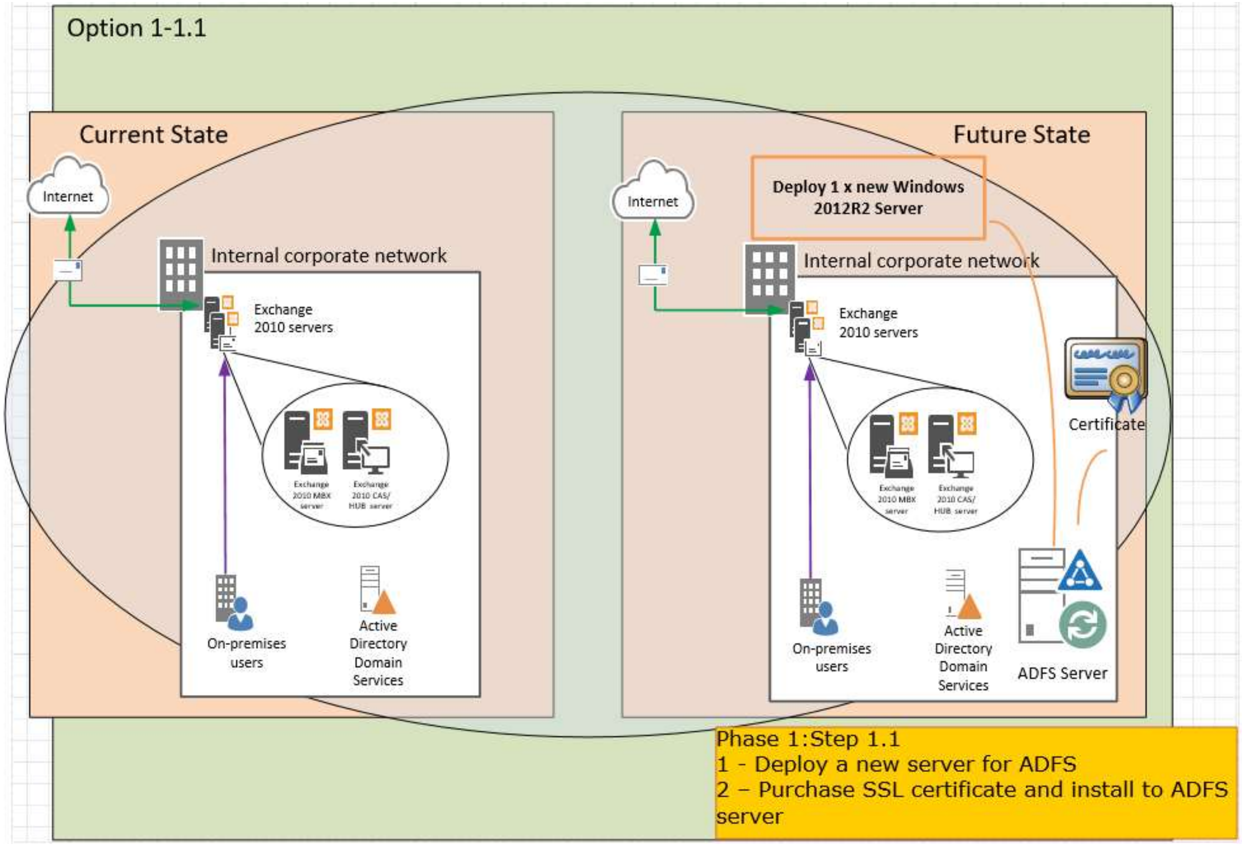
8. Make sure all settings are correct and click Finish.



Update DNS settings

Congratulations! Your domain and email addresses are all set up.

Deployment Certificate (If Active Directory Federation Services is being deployed)


Option 1-1.1
Current State
Internet
Internal corporate network
Exchange 2010 servers
Exchange 2010 MBX server
Exchange 2010 CAS/ HUB server
On-premises users
Active Directory Domain Services
Future State
Deploy 1 x new Windows 2012R2 Server
Internet
Internal corporate network
Exchange 2010 servers
Exchange 2010 MBX server
Exchange 2010 CAS/ HUB server
Certificate
On-premises users
Active Directory Domain Services
ADFS Server

Phase 1:Step 1.1
1 - Deploy a new server for ADFS
2 – Purchase SSL certificate and install to ADFS server

We need certificate for ADFS to configure DirSync and Single Sign-On.

1. Logon to ADFS Server.
2. In the **Windows** start menu, type **Internet Information Services (IIS) Manager** and open it.
3. In the **Connections** menu tree (left pane), locate and click the **server name**.

4. On the server name Home page (center pane), in the IIS section, double-click **Server Certificates**.

5. On the Server Certificates page (center pane), in the **Actions** menu (right pane), click the **Create Certificate Request…** link.

6. In the Request Certificate wizard, on the Distinguished Name Properties page, provide the information and then click **Next**.

7. On the Cryptographic Service Provider Properties page, provide the information below and then click **Next.**

   Cryptographic service provider - In the drop-down list, select **Microsoft RSA SChannel...**, unless you have a specific cryptographic provider.

Bit length - In the drop-down list, select **2048** (or higher).

8. On the File Name page, under Specify a file name for the certificate request, click the … box to browse to a location where you want to save your CSR and then click **Finish**.

9. Use a text editor (such as Notepad) to open the file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags, and paste it into the third-party certificate providers order form**.**

10. After you receive your SSL Certificate from third-party providers, you can install it.

11. Use certificate you've purchased from third-party to import onto the ADFS server virtual machine.

12. Click **Complete Certificate Request** from the Actions panel.

13. Locate to your certificate, and enter **Friendly** name. Select **Personal**.

14. Verify the certificate you just installed.

15. On the **Start** menu click Run and then type **mmc**.

16. Click **File**, select **Add/Remove Snap-in**.

17. Click **Certificates** and then select **Add**.

18. Select **Computer Account** and then click **Next**.
19. Select **Local Computer** and then click **Finish**.
20. Click the **+** to expand the certificates (local computer) console tree and look for the personal directory/folder. Expand the certificates folder.
21. Right-click on the certificate you want to backup and select ALL TASKS and then click **Export**.
22. Choose **Yes, export the private key and include all certificates in certificate path if possible**.
23. Leave the default settings and then enter your password if required and then click **Finish**.
24. Imported certificates to all virtual machines which are required to connect to Microsoft Office 365.

Configure UPN suffix

You need to configure UPN suffix if the internal domain name doesn't match the domain to federate with office 365. Membership in Domain Admins or Enterprise Admins, or equivalent, is the minimum required to complete this procedure.

1. Logon to Domain control server
2. From the **Start** menu, click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
3. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**.
4. On the **UPN Suffixes** tab, type an alternative UPN suffix suffixes field the domain name to match the external domain used to federate with Office 365, and then click **Add.**
5. Click **OK** and close Active Directory Domain and Trust window.

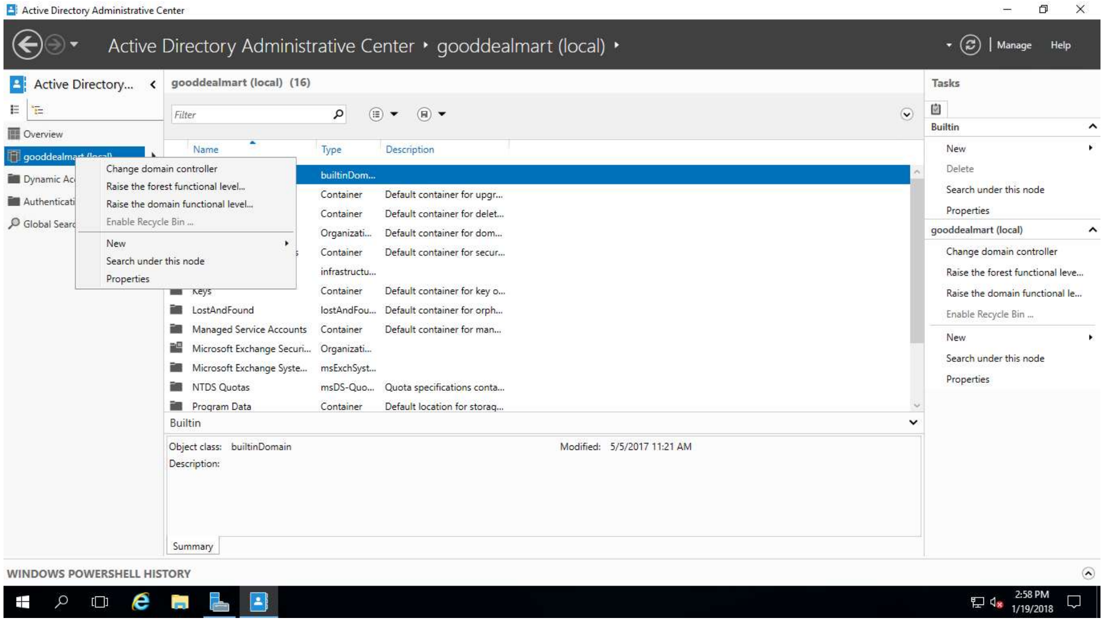
Note

a custom **UPN suffix** must match the external name space, The new UPN suffix must be assigned to the users before **perform the authentication** with federated domain

6. From the **Start** menu, click **Administrative Tools**, and then click **Active Directory Users and Computers**.
7. Select the users, right click the selection and choose **Properties** option.
8. Thick **UPN suffix**, select the external domain name and click **OK.**
9. Check the user's **Properties**, the **User logon name** field is now set with the UPN suffix just configured.

Enable Active Directory Recycle Bin

1. Logon Domain control server.
2. Open the **Active Directory Administrative Center**.
3. Right-click your domain.
4. Select **Enable Recycle Bin…..**



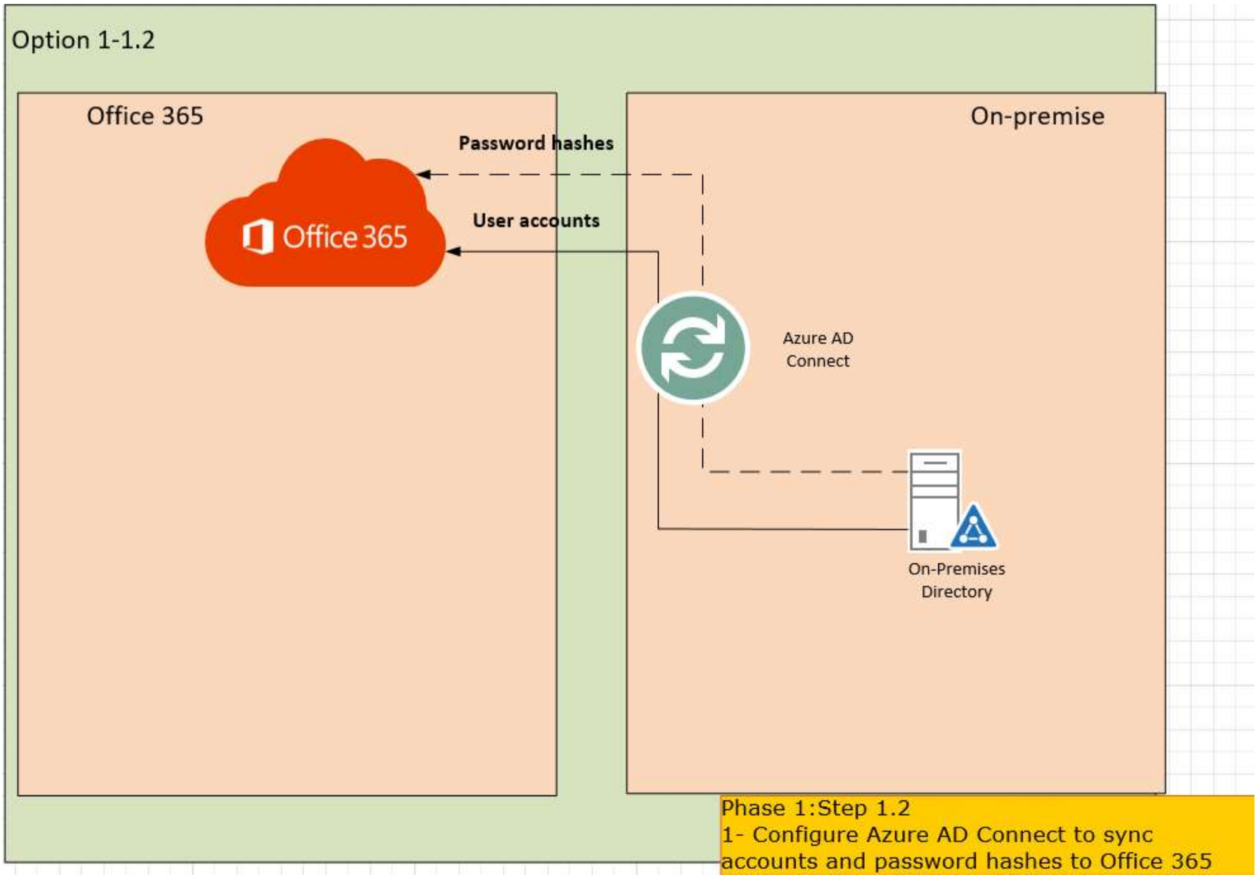
gooddealmart (local) (16)

Name	Type	Description
	builtinDom...	
	Container	Default container for upgr...
	Container	Default container for delet...
	Organizati...	Default container for dom...
	Container	Default container for secur...
	infrastructu...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
Microsoft Exchange Securi...	Organizati...	
Microsoft Exchange Syste...	msExchSyst...	
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...

Builtin

Object class: builtinDomain
Modified: 5/5/2017 11:21 AM
Description:

Deployment Azure AD Connect



If you need a tool to connect your on-premises directory with Azure AD and Office 365, Azure AD Connect is the best way to do it. Azure AD Connect has two installation types for new installation: Express and customized.

Note

Windows Azure Active Directory Sync (DirSync) or Azure AD Sync as these tools are now deprecated and will reach end of support on April 13, 2017

Prerequisites

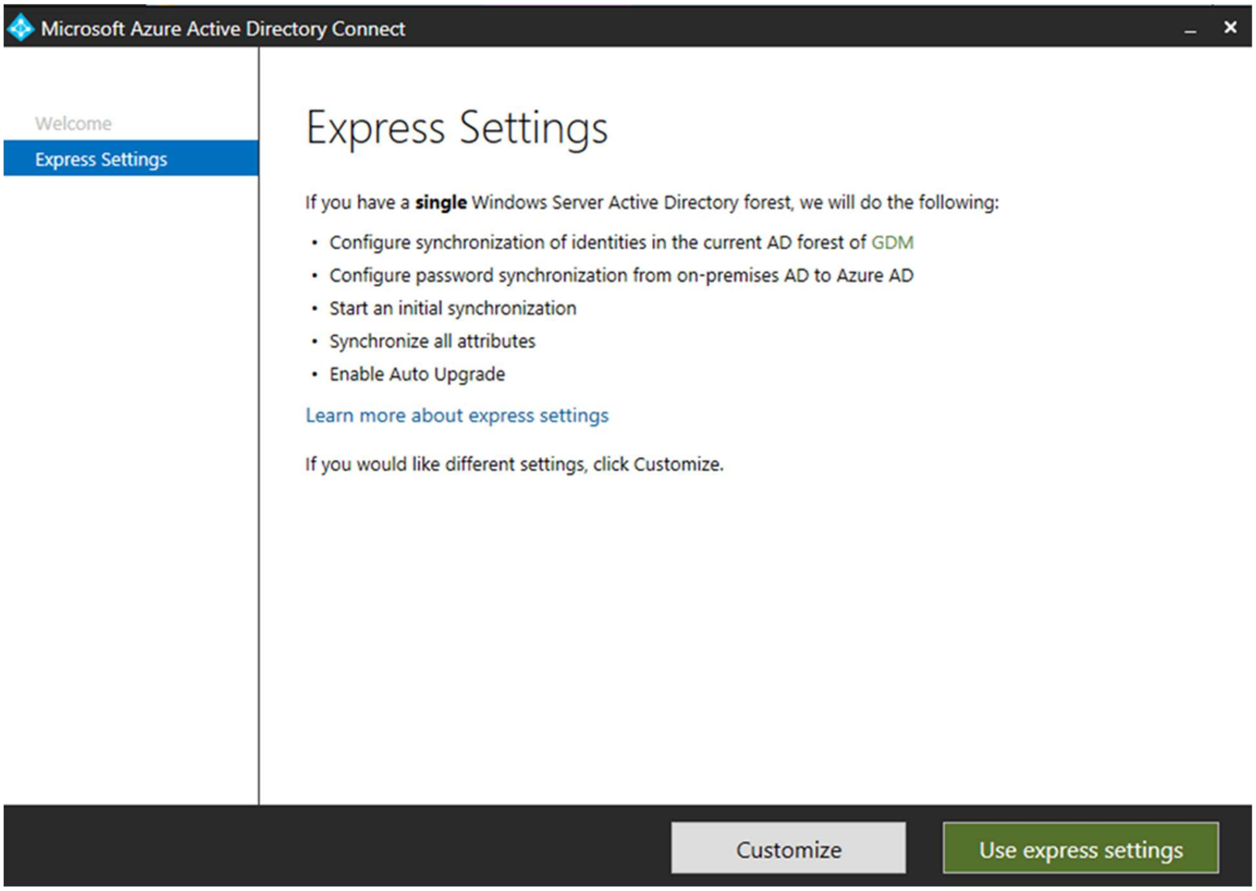
- It must be installed on Windows Server standard or better.
- It supports full GUI installed only.
- Azure AD Connect must be installed on Windows Server 2008 or later. This server may be a domain controller or a member server when using express settings. If you use custom settings, then the server can also be stand-alone and does not have to be joined to a domain.
- If you plan to use the feature **password synchronization**, then the Azure AD Connect server must be on Windows Server 2008 R2 SP1 or later.
- If you plan to use a **group managed service account**, then the Azure AD Connect server must be on Windows Server 2012 or later.
- Disable PowerShell Transcription Group Policy.
- .NET Framework 4.5.1 or later and Microsoft PowerShell 3.0 or later installed.
- If Active Directory Federation Services is being deployed, the servers where AD FS or Web Application Proxy are installed must be Windows Server 2012 R2 or later. Windows remote management must be enabled on these servers for remote installation.
- You need SSL Certificates if Active Directory Federation Services is being deployed
- An Azure AD Global Administrator account for the Azure AD tenant you wish to integrate with. This account must be a **school or organization account** and cannot be a **Microsoft account**.
- Create a A record for AD FS federation service name on both intranet and internet.
- Check the link for https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-ports if you have firewalls on your intranet.

Note

Please review the latest prerequires before Install.

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-prerequisites

Install Azure AD Connect with Express settings



Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of GDM
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

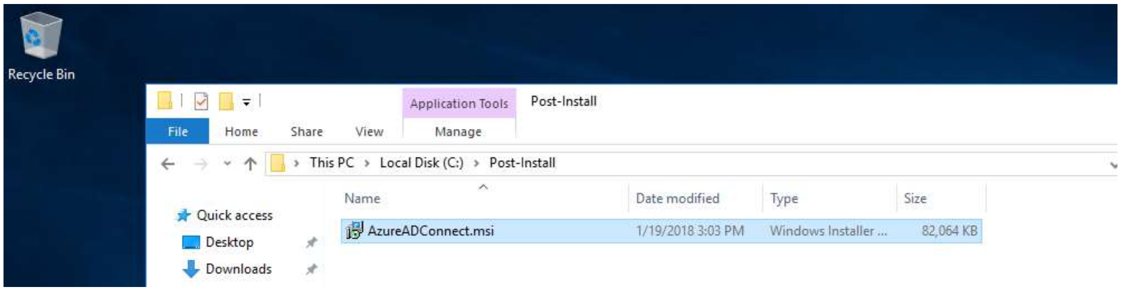
If you would like different settings, click Customize.

If you have a signal forest AD or User sign with the same password using password synchronization, then this is the recommended option to use.

Azure AD Connect **Express Settings** is used when you have a single-forest topology and password synchronization for authentication.

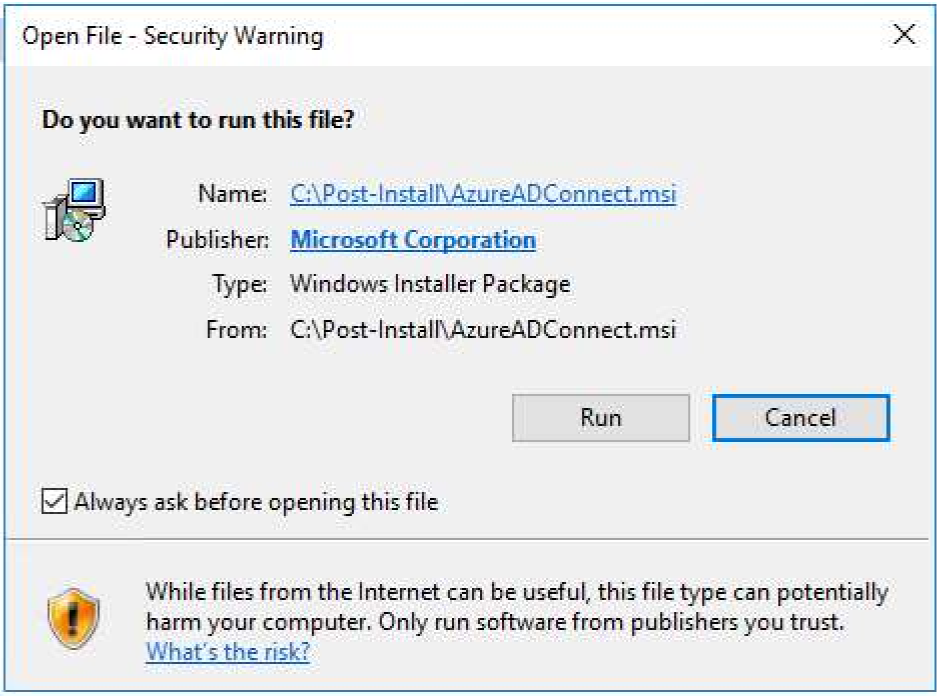
Before you start installing Azure AD Connect, make sure to download Azure AD Connect and complete the pre-requisite steps in Azure AD Connect: Hardware and prerequisites.

1. Sign in as a local Administrator to Azure AD Connect Server.
2. Navigate to and double-click **AzureADConnect.msi**.



Name	Date modified	Type	Size
AzureADConnect.msi	1/19/2018 3:03 PM	Windows Installer ...	82,064 KB

3. On the Security Warning page, click Run.



Open File - Security Warning

Do you want to run this file?

Name: C:\Post-Install\AzureADConnect.msi

Publisher: Microsoft Corporation

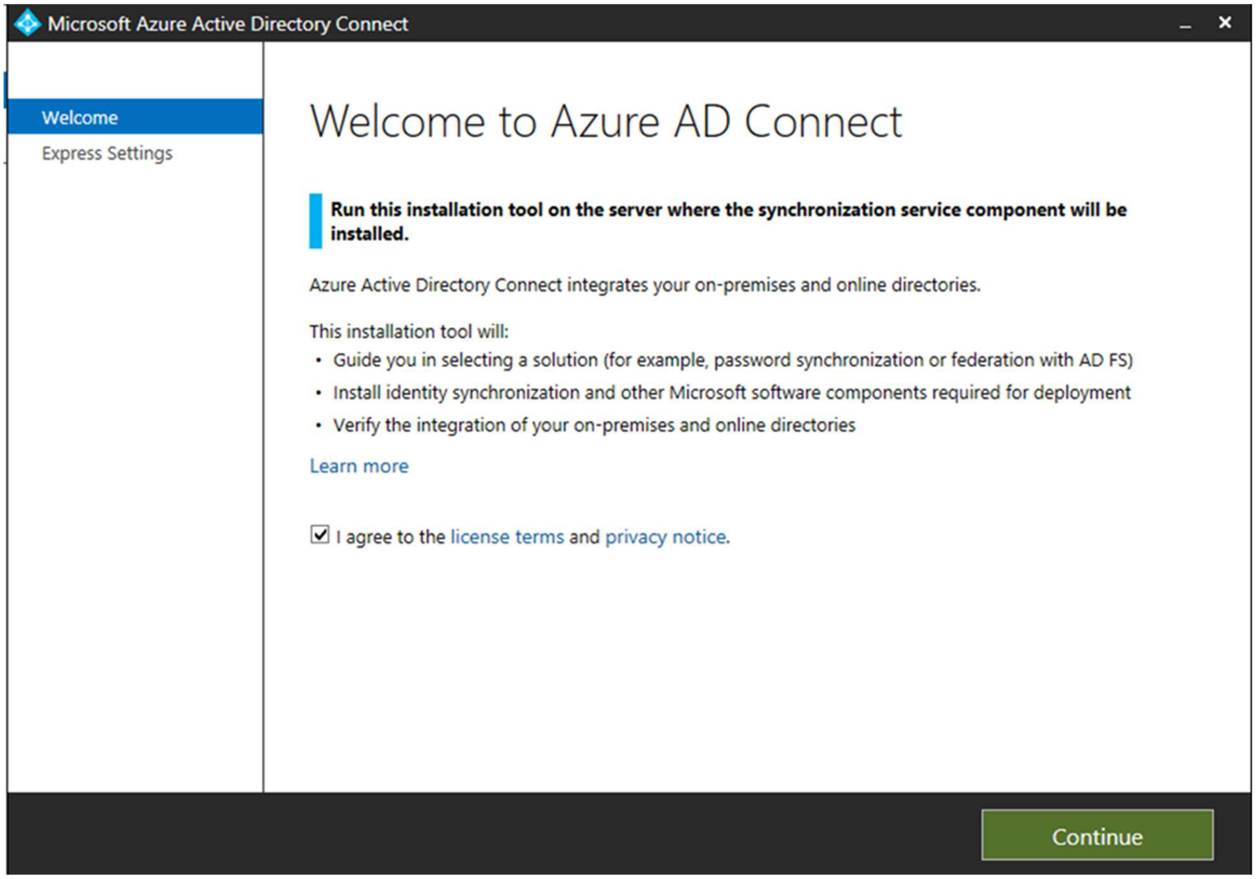
Type: Windows Installer Package

From: C:\Post-Install\AzureADConnect.msi

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

4. On the **Welcome** screen, select the box agreeing to the licensing terms and click **Continue**.



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

Azure Active Directory Connect integrates your on-premises and online directories.

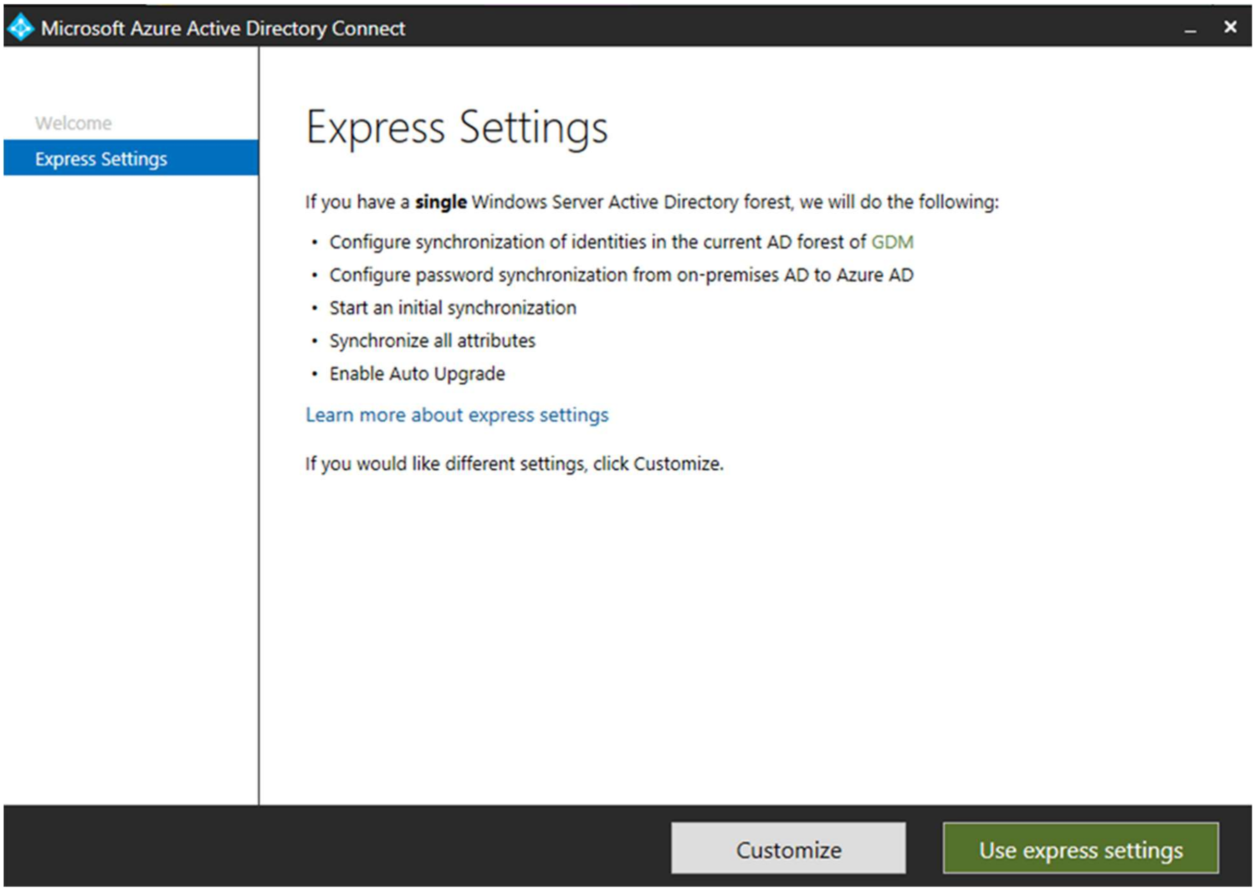
This installation tool will:

- Guide you in selecting a solution (for example, password synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Verify the integration of your on-premises and online directories

Learn more

☑ I agree to the license terms and privacy notice.

5. On the Express settings screen, click **Use express settings**.



Express Settings

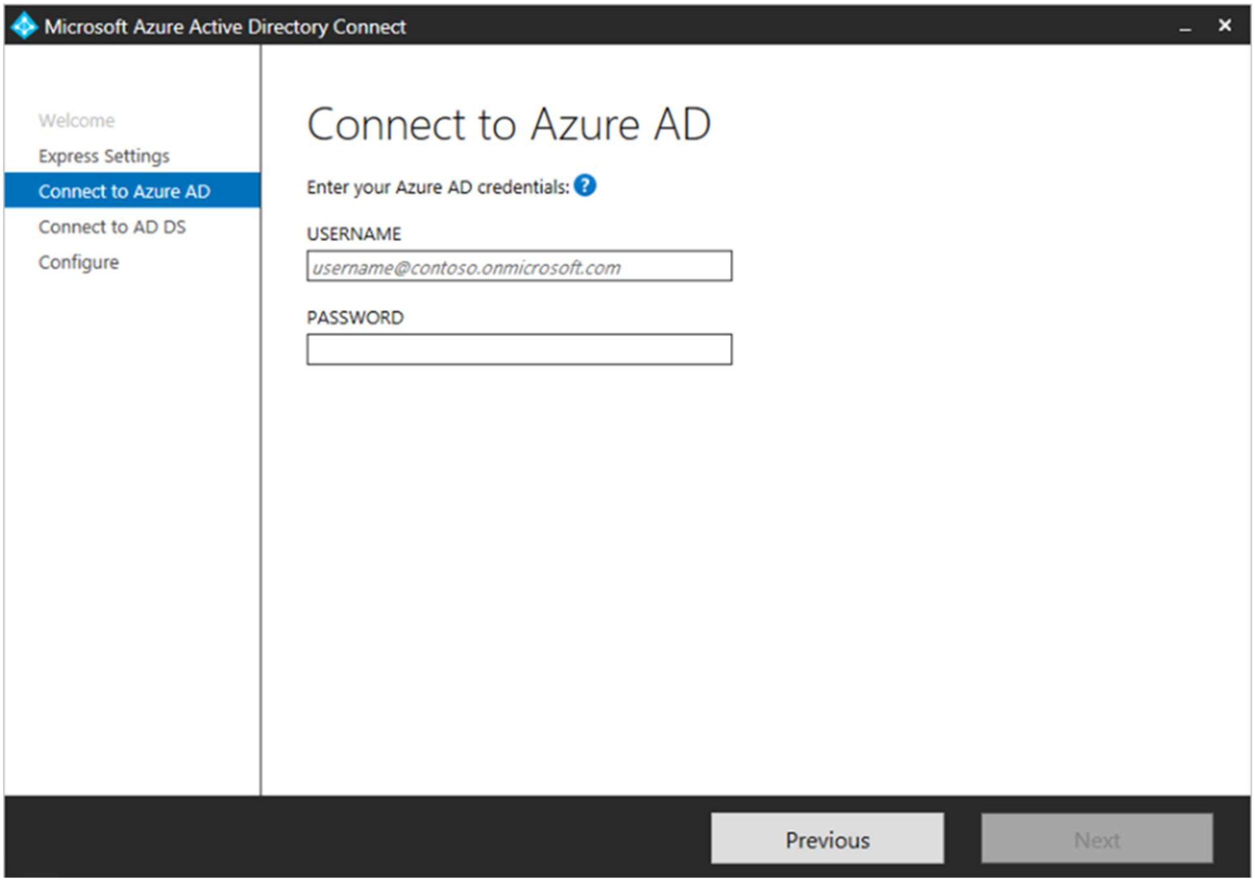
If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of GDM
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

6. On the **Enter your Azure AD credentials page**, enter the username and password of a **global administrator** for your Azure AD. Click **Next**.



Connect to Azure AD

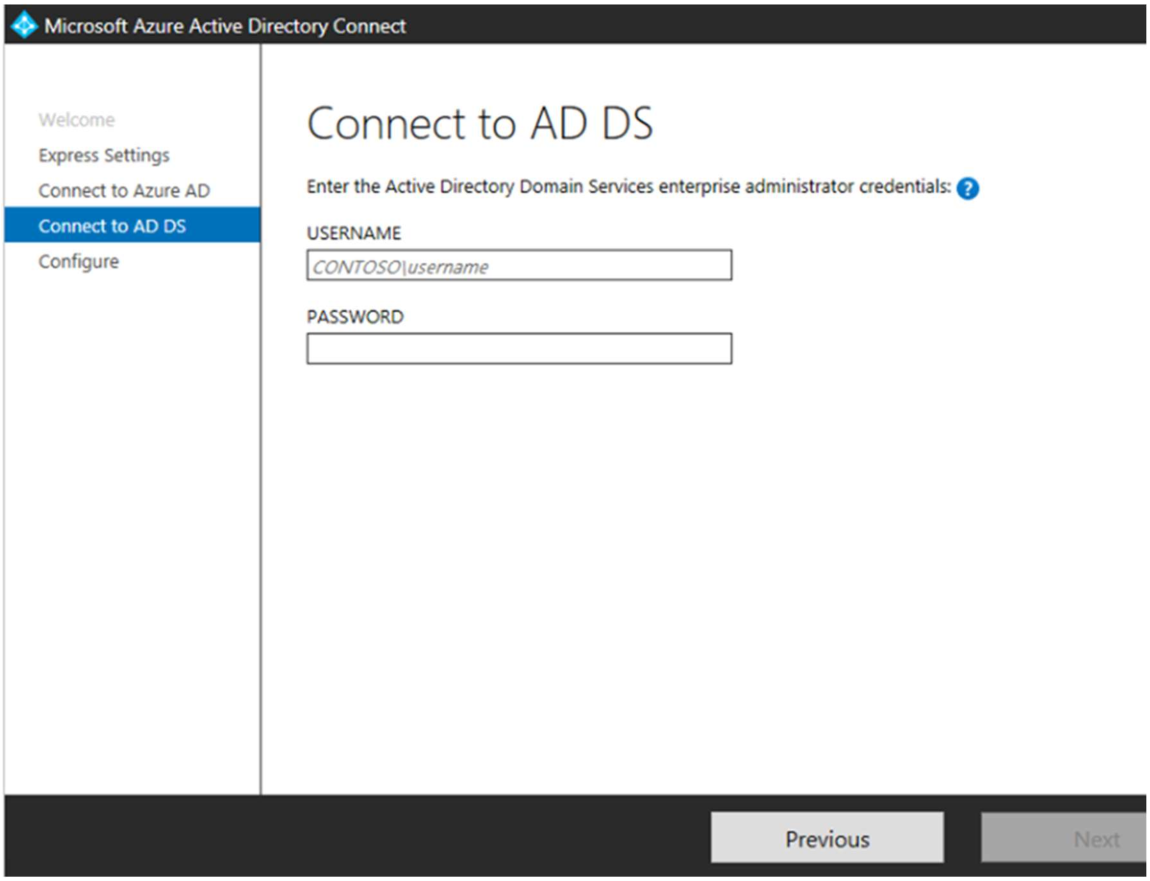
Enter your Azure AD credentials:

USERNAME

username@contoso.onmicrosoft.com

PASSWORD

7. On the **Enter the Active Directory Services enterprise administrator credentials page**, enter the username and password for an **enterprise admin account**. You can enter the domain part in either NetBIOS or FQDN format, Click **Next**.



Connect to AD DS

Enter the Active Directory Domain Services enterprise administrator credentials:

USERNAME

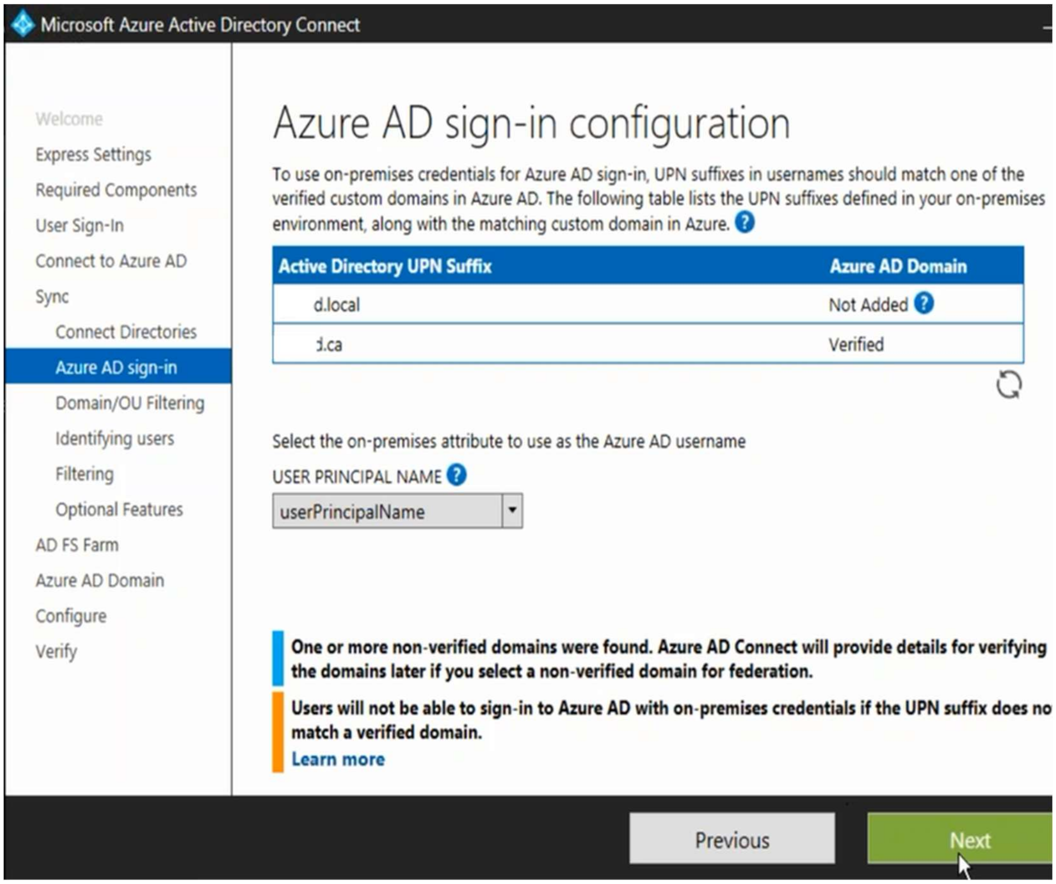
CONTOSO\username

PASSWORD

Note

The Azure AD sign-in configuration page only shows if you did not complete verify your domains in the prerequisites.

If you see this page, then review every domain marked **Not Added** and **Not Verified**. Make sure those domains you use have been verified in Azure AD. Click the Refresh symbol when you have verified your domains.



Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes in usernames should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Azure AD Domain
d.local	Not Added
d.ca	Verified

Select the on-premises attribute to use as the Azure AD username

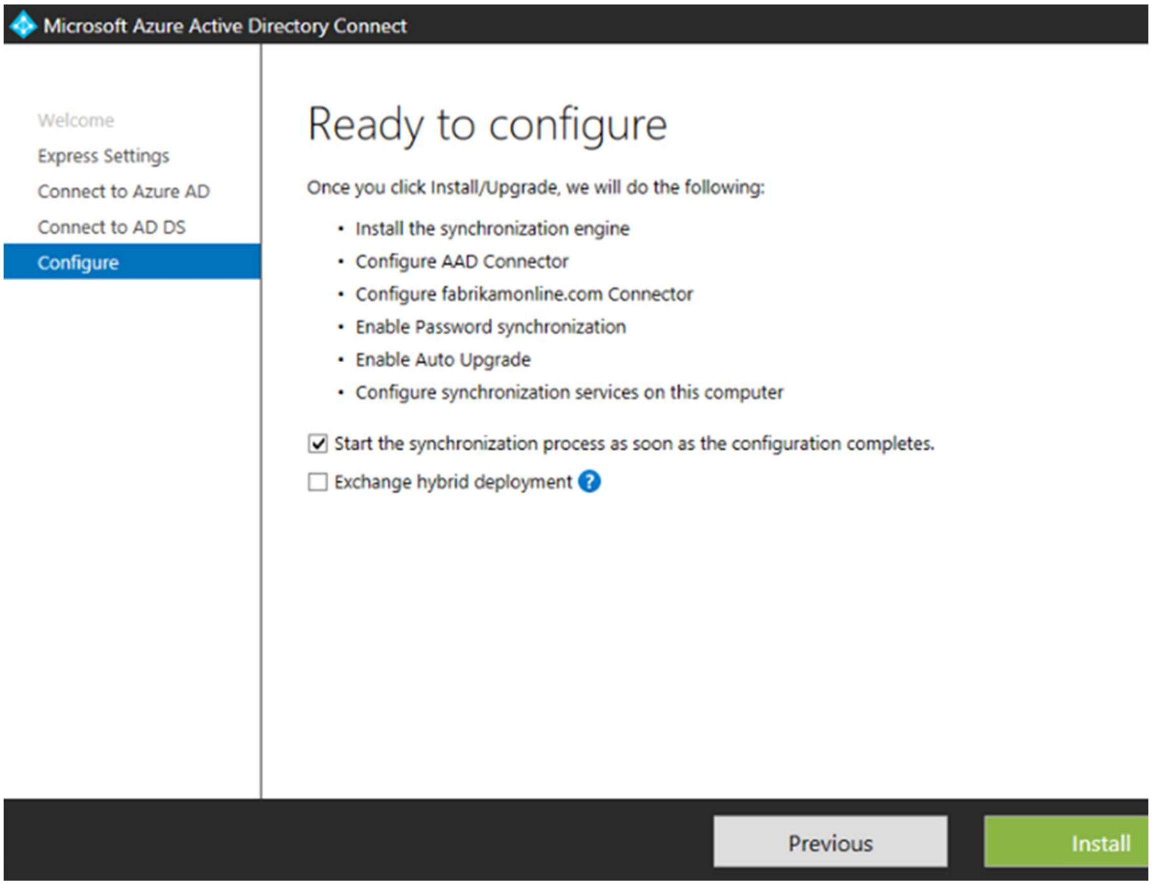
USER PRINCIPAL NAME: userPrincipalName

One or more non-verified domains were found. Azure AD Connect will provide details for verifying the domains later if you select a non-verified domain for federation.

Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does no match a verified domain.

Learn more

8. On the **Ready to configure** screen, click **Install**.



Ready to configure

Once you click Install/Upgrade, we will do the following:

- Install the synchronization engine
- Configure AAD Connector
- Configure fabrikamonline.com Connector
- Enable Password synchronization
- Enable Auto Upgrade
- Configure synchronization services on this computer

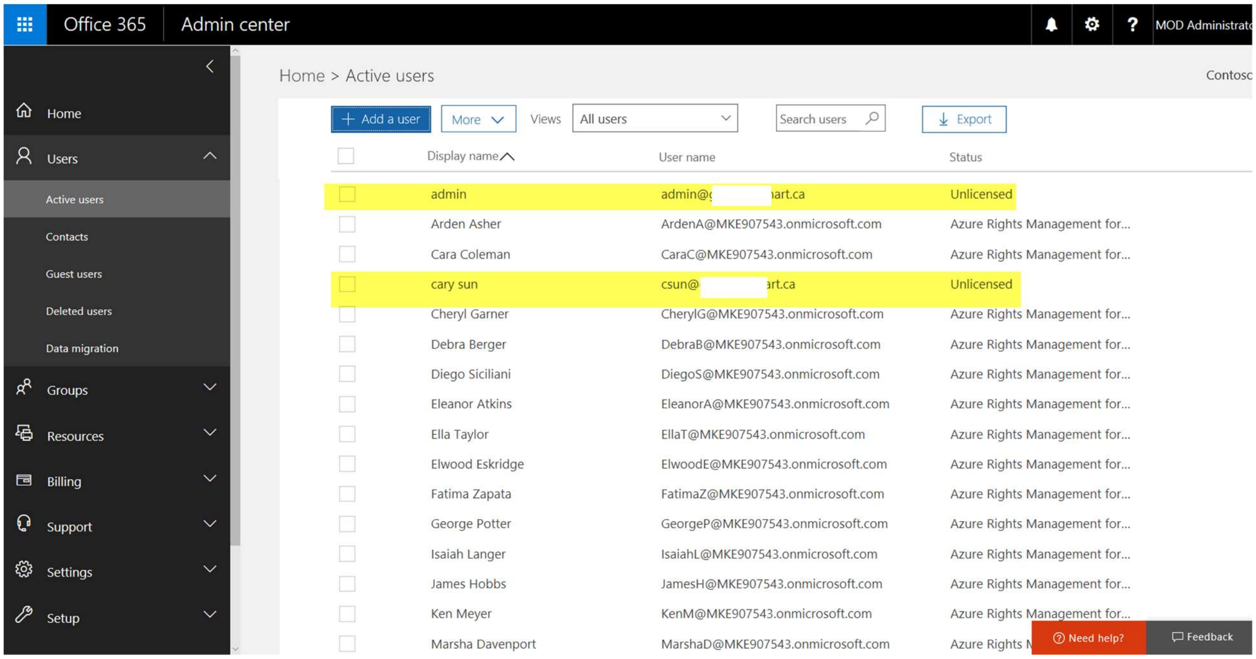
☑ Start the synchronization process as soon as the configuration completes.

□ Exchange hybrid deployment

Note

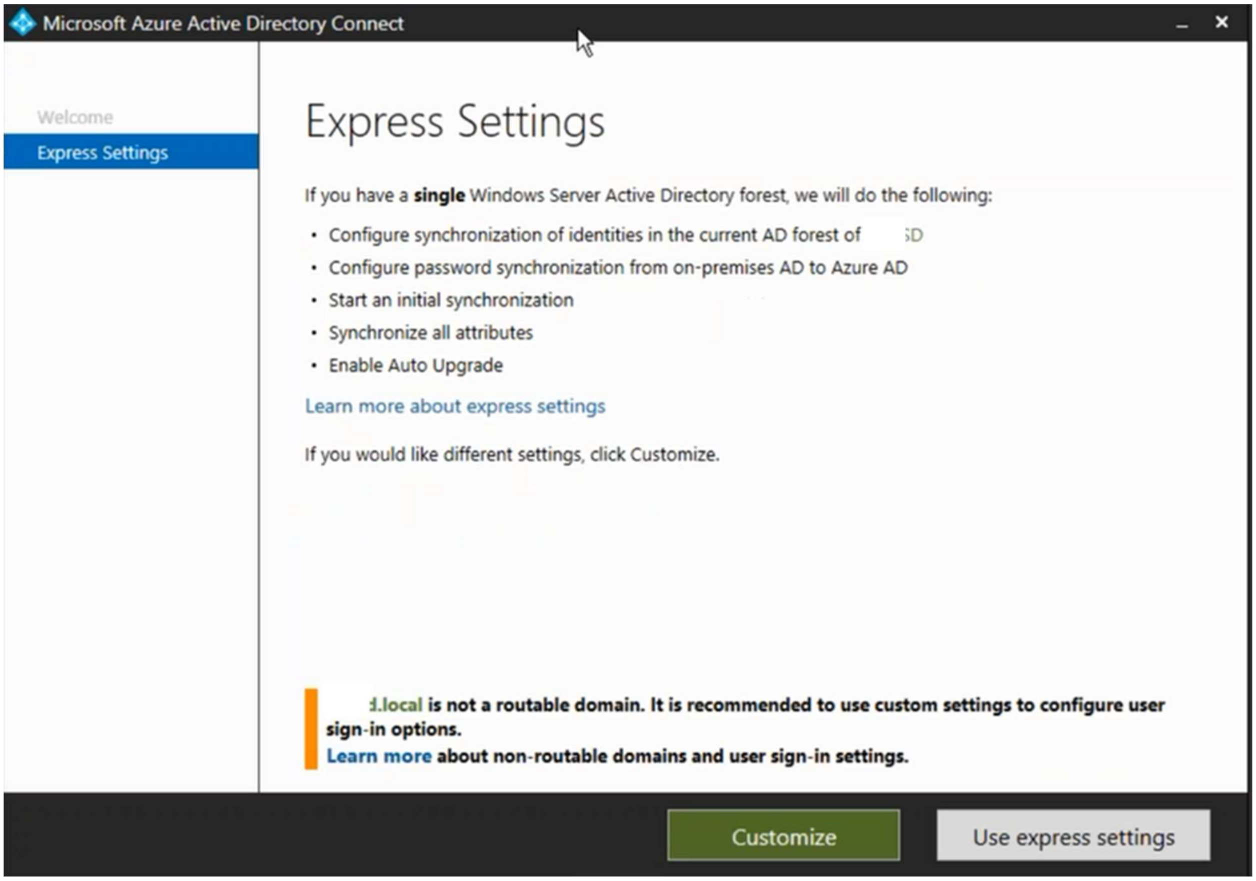
If you have Exchange in your on-premises Active Directory, then you also have an option to enable Exchange Hybrid deployment. Enable this option if you plan to have Exchange mailboxes both in the cloud and on-premises at the same time.

9. When the installation completes, click **Exit**.
10. After the installation has completed, sign off and sign in again before you use Synchronization Service Manager or Synchronization Rule Editor.



	Display name	User name	Status
□	admin	admin@[redacted]art.ca	Unlicensed
□	Arden Asher	ArdenA@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Cara Coleman	CaraC@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	cary sun	csun@[redacted]art.ca	Unlicensed
□	Cheryl Garner	CherylG@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Debra Berger	DebraB@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Diego Siciliani	DiegoS@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Eleanor Atkins	EleanorA@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Ella Taylor	EllaT@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Elwood Eskridge	ElwoodE@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Fatima Zapata	FatimaZ@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	George Potter	GeorgeP@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Isaiah Langer	IsaiahL@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	James Hobbs	JamesH@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Ken Meyer	KenM@MKE907543.onmicrosoft.com	Azure Rights Management for...
□	Marsha Davenport	MarshaD@MKE907543.onmicrosoft.com	Azure Rights M

Install Azure AD Connect with Customized settings



Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of SD
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

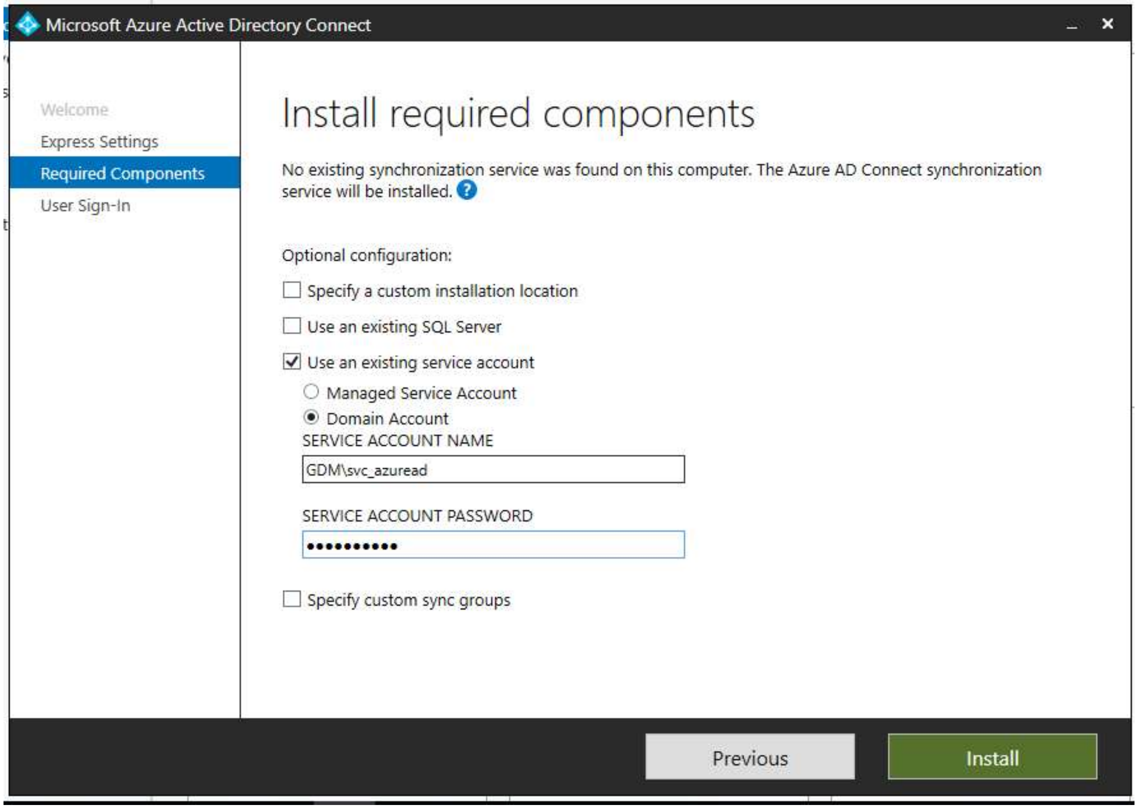
If you would like different settings, click Customize.

d.local is not a routable domain. It is recommended to use custom settings to configure user sign-in options.
Learn more about non-routable domains and user sign-in settings.

If you have multiple forests or you need to customized your sign-in option or customize synchronization feature, then this is the recommended option to use.

1. If your internal domain is not a routable domain, you need to select the customization settings to configure user sign-in.

2. On the **Install required components** page, check **Use an existing service account** and type service account name and password, click **Install**.



Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.

Optional configuration:

□ Specify a custom installation location

□ Use an existing SQL Server

☑ Use an existing service account

○ Managed Service Account

● Domain Account

SERVICE ACCOUNT NAME: GDM\svc_azuread

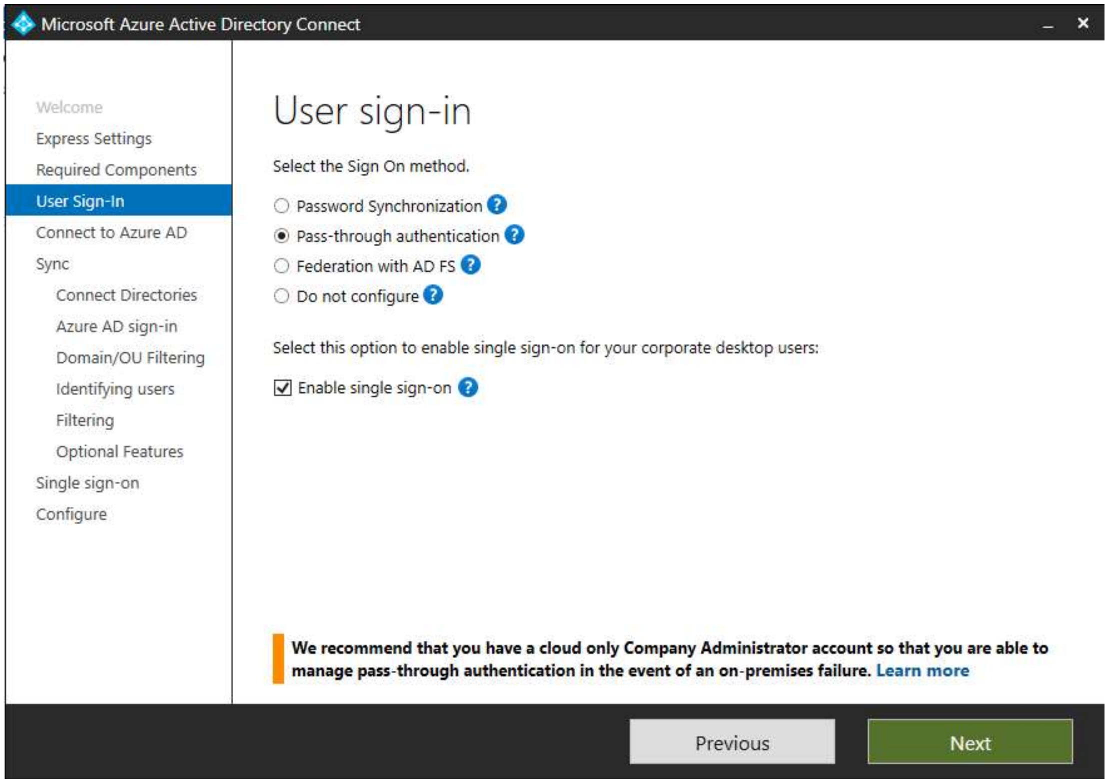
SERVICE ACCOUNT PASSWORD: ••••••••••

□ Specify custom sync groups

Note

By default, Azure AD Connect uses a virtual service account for the synchronization services to use. If you use a remote SQL server or use a proxy that requires authentication, you need to use a **managed service account** or use a service account in the domain and know the password. In those cases, enter the account to use. Make sure the user running the installation is an SA in SQL so a login for the service account can be created

3. On **User sign-in** page, select **pass-through authentication** to be the Sign On method, users can sign in to Office 365 using the same password as on-premises network, also, select **Enable sign sign-on** and then click **Next**.



User sign-in

Select the Sign On method.

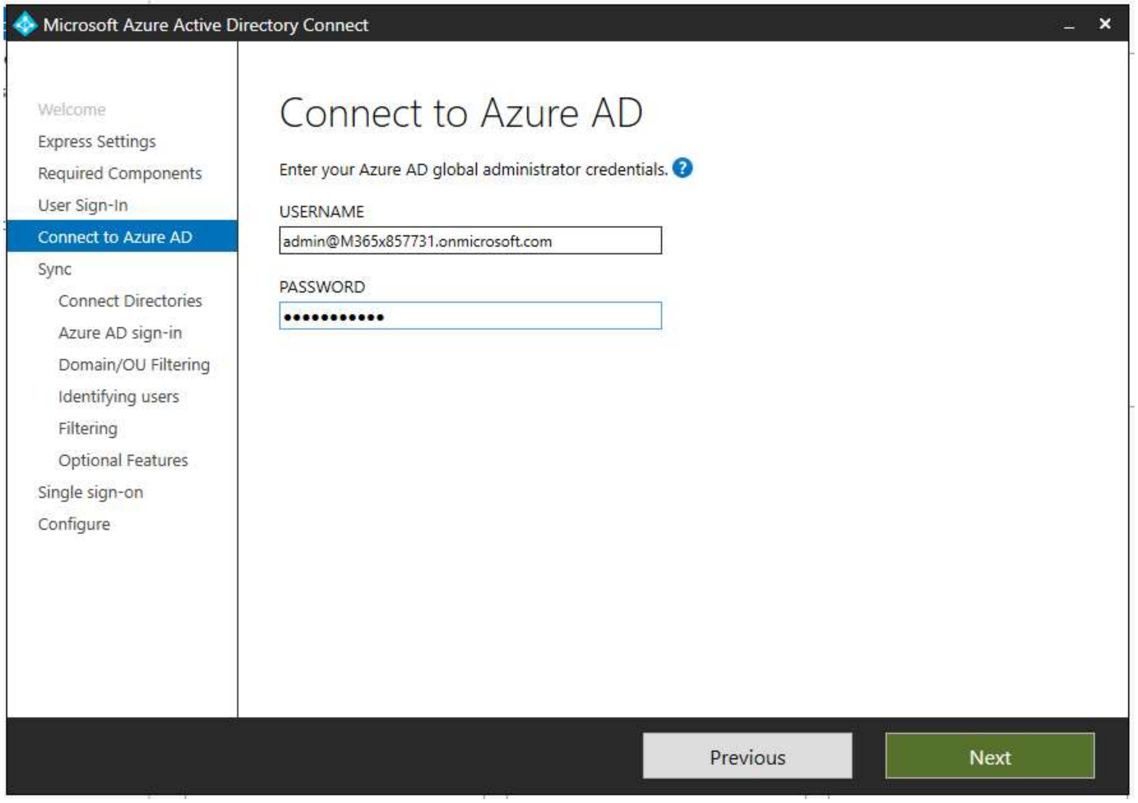
○ Password Synchronization
● Pass-through authentication
○ Federation with AD FS
○ Do not configure

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

☑ Enable single sign-on

We recommend that you have a cloud only Company Administrator account so that you are able to manage pass-through authentication in the event of an on-premises failure. Learn more

4. On **Connect to Azure AD** page, enter global admin account and password, click **Next**.



Connect to Azure AD

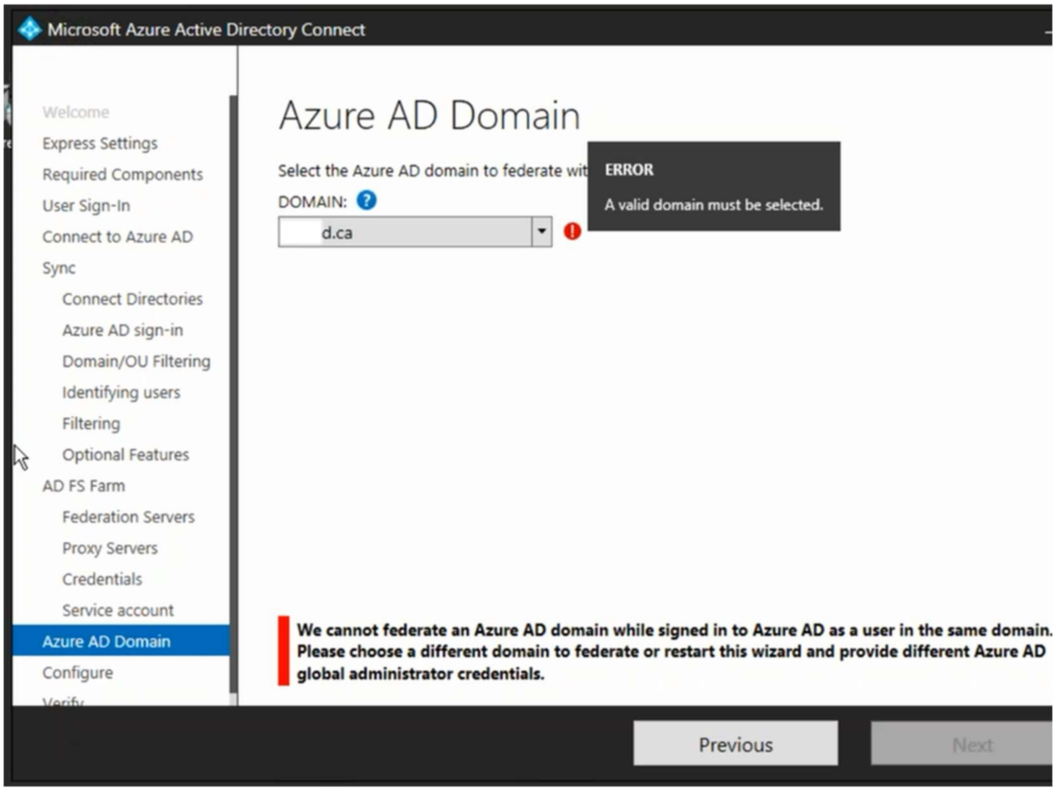
Enter your Azure AD global administrator credentials.

USERNAME
admin@M365x857731.onmicrosoft.com

PASSWORD
••••••••••••

Note

Please use an account in the default **onmicrosoft.com** domain, it will happen error if using the federation domain account.



Azure AD Domain

Select the Azure AD domain to federate wit

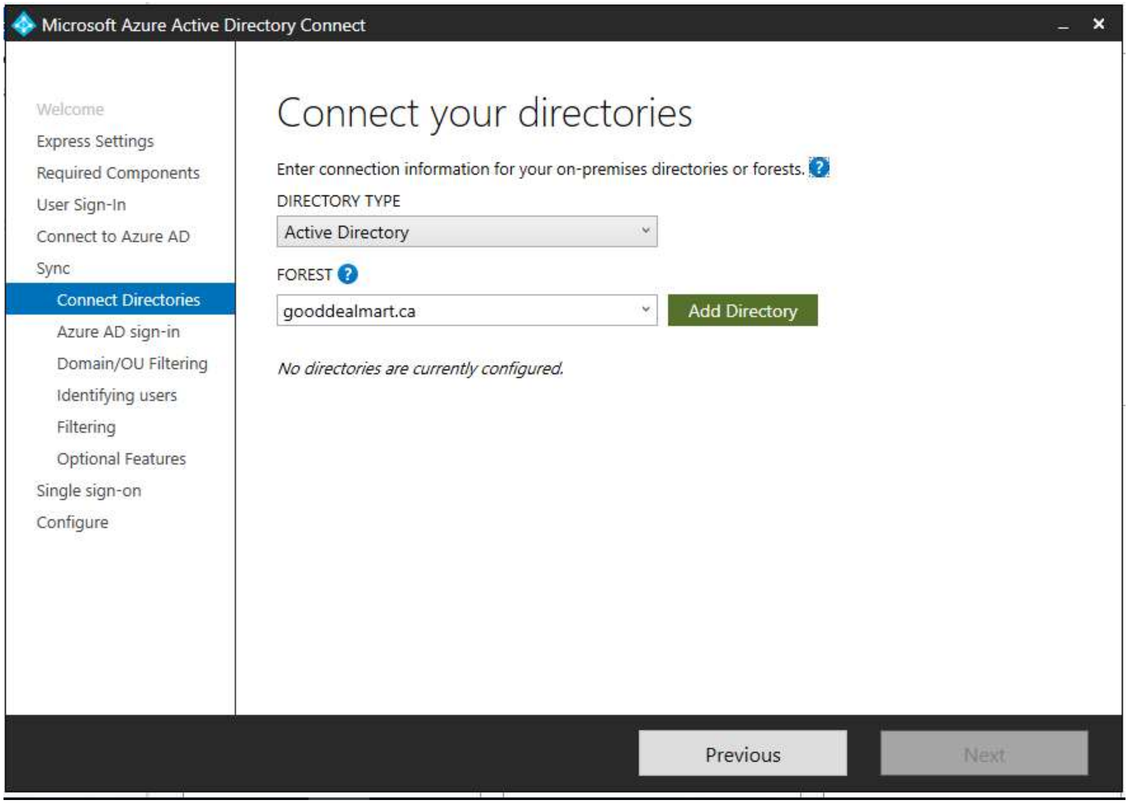
DOMAIN: d.ca

ERROR

A valid domain must be selected.

We cannot federate an Azure AD domain while signed in to Azure AD as a user in the same domain. Please choose a different domain to federate or restart this wizard and provide different Azure AD global administrator credentials.

5. On **Connect your directories** page, select local domain and click **Add Directory**.



Connect your directories

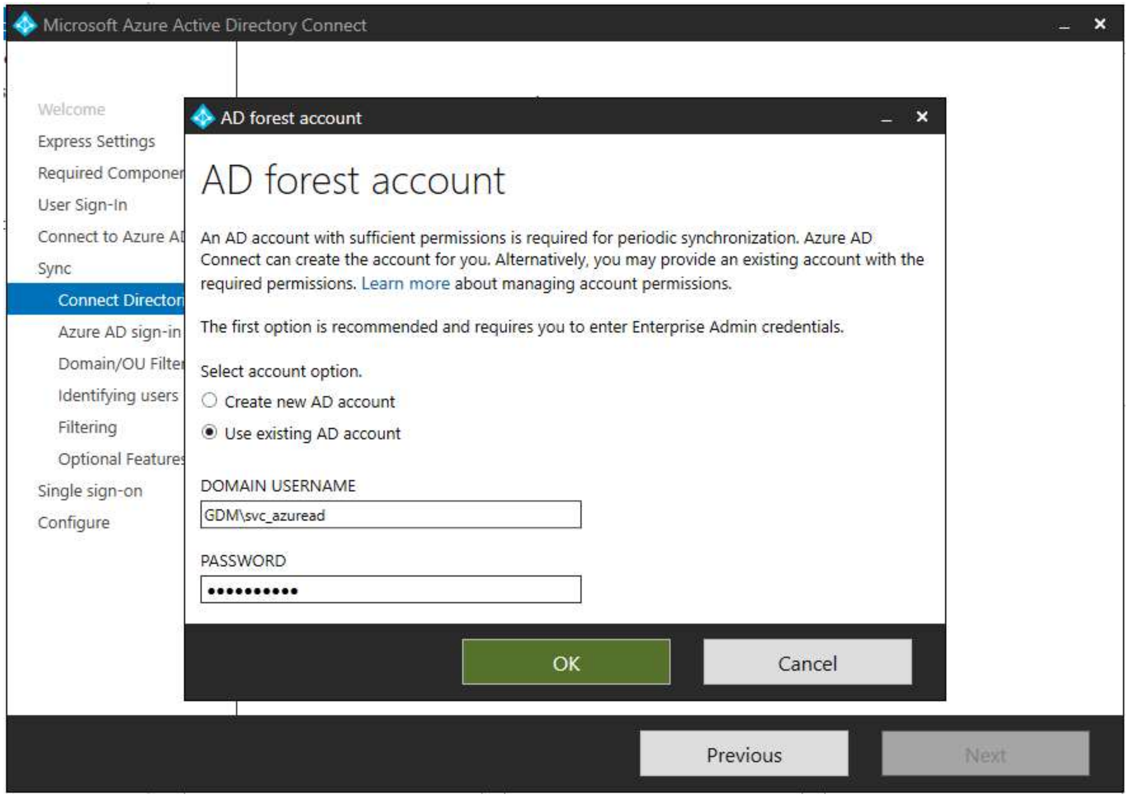
Enter connection information for your on-premises directories or forests.

DIRECTORY TYPE: Active Directory

FOREST: gooddealmart.ca

No directories are currently configured.

6. It will pop up **AD Forest account** page, select **Create new account** and enter the service account name and password, click **OK** and then click **Next**.



AD forest account

AD forest account

An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.

The first option is recommended and requires you to enter Enterprise Admin credentials.

Select account option.

○ Create new AD account

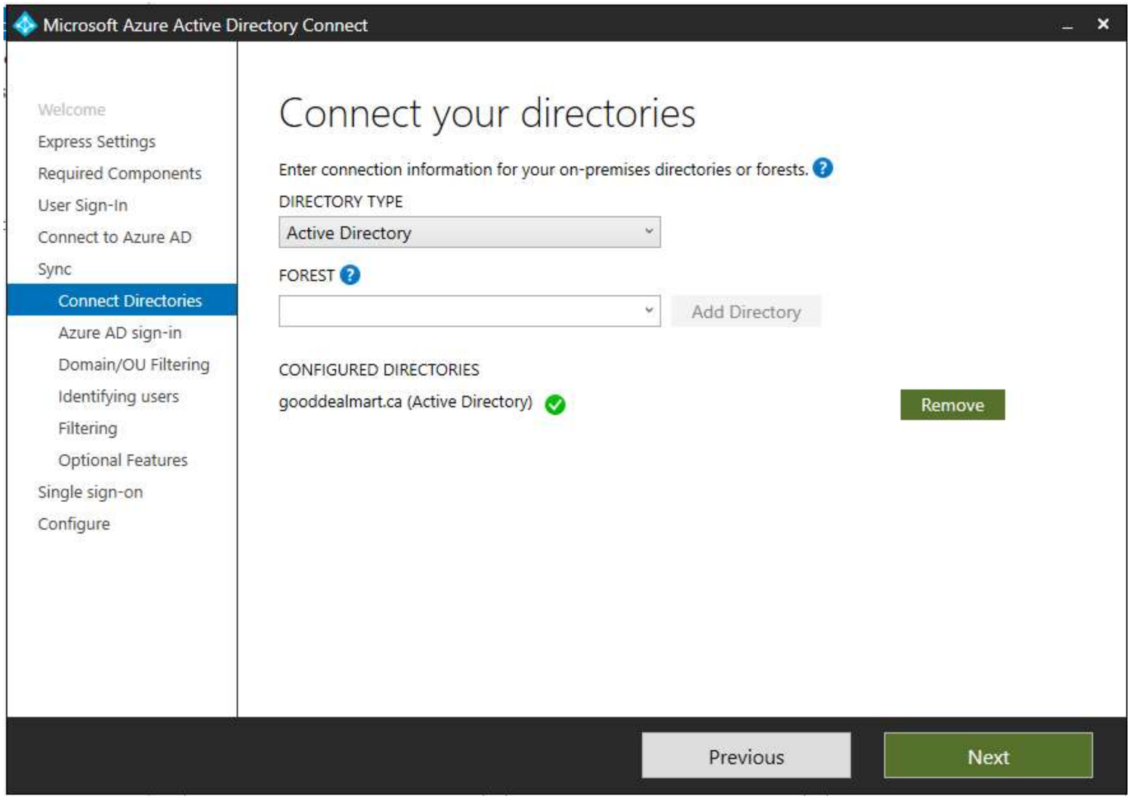
● Use existing AD account

DOMAIN USERNAME

GDM\svc_azuread

PASSWORD

•••••••••••



Connect your directories

Enter connection information for your on-premises directories or forests.

DIRECTORY TYPE

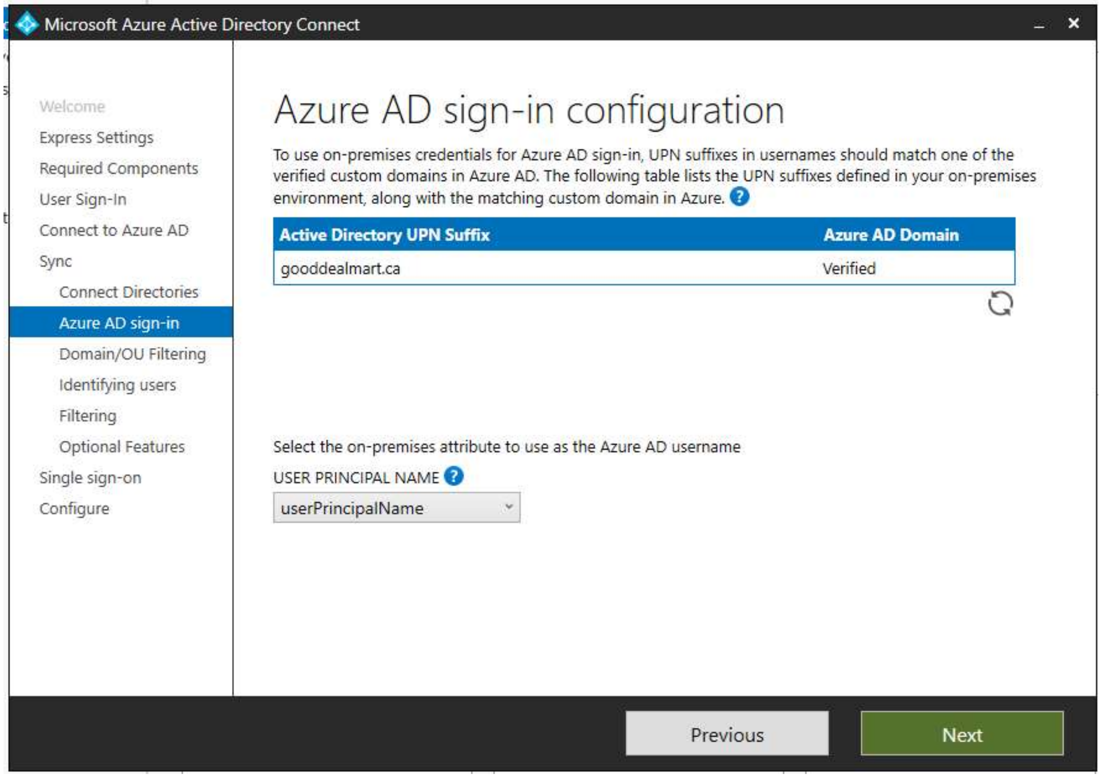
Active Directory

FOREST

CONFIGURED DIRECTORIES

gooddealmart.ca (Active Directory) ✓

7. On **Azure AD sign-in configuration** page, make sure the UPN domains present in on-premises AD DS and be verified in Azure AD, click **Next**.



Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes in usernames should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Azure AD Domain
gooddealmart.ca	Verified

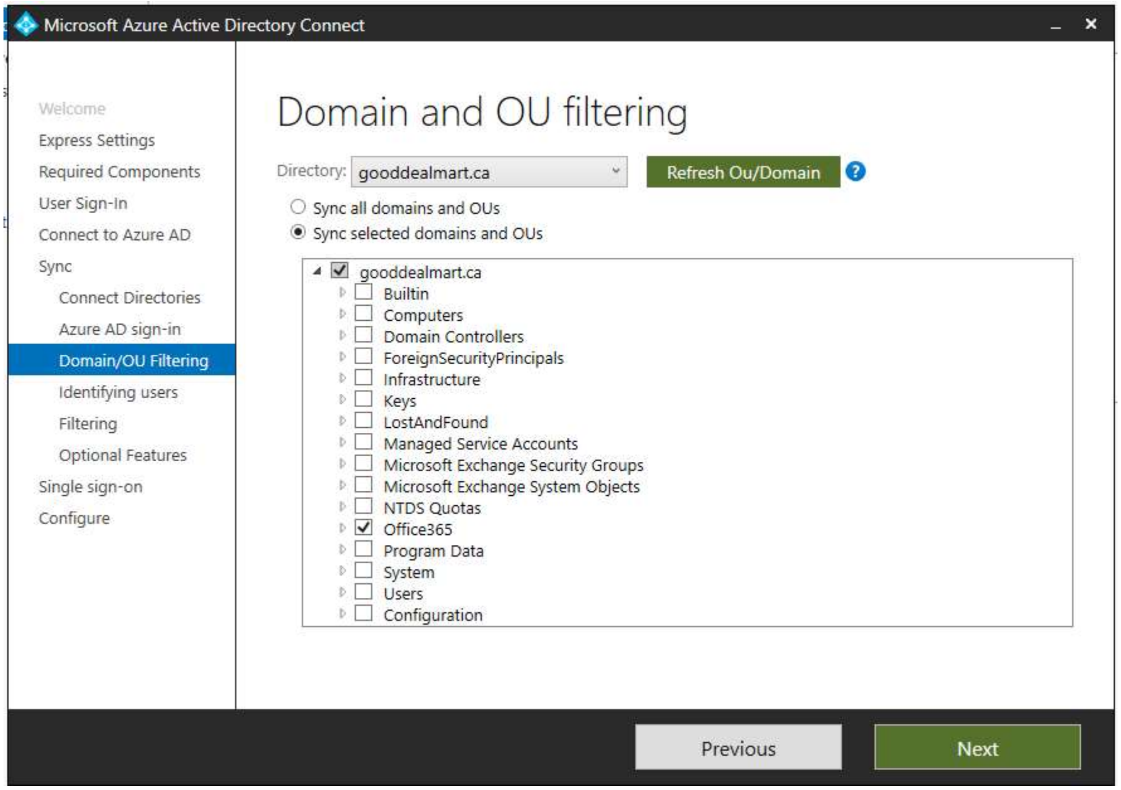
Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME

userPrincipalName

8. On **Domain and OU filtering** page, click **Sync selected domains and OUs**.

9. Select OUs you do want to synchronize to Azure AD, click **Next**.



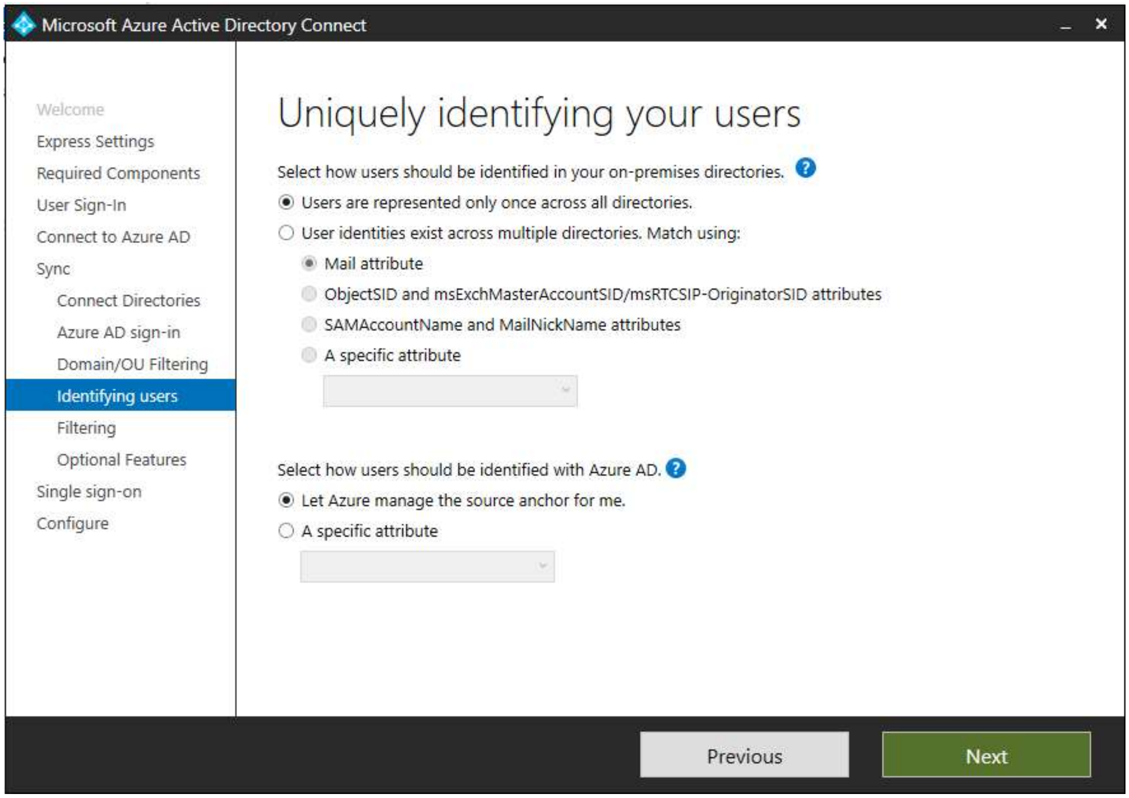
Domain and OU filtering

Directory: gooddealmart.ca

○ Sync all domains and OUs
● Sync selected domains and OUs

- ☑ gooddealmart.ca
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ Keys
  - □ LostAndFound
  - □ Managed Service Accounts
  - □ Microsoft Exchange Security Groups
  - □ Microsoft Exchange System Objects
  - □ NTDS Quotas
  - ☑ Office365
  - □ Program Data
  - □ System
  - □ Users
  - □ Configuration

10. Click **Next** on the **Uniquely identifying your users** page.



Uniquely identifying your users

Select how users should be identified in your on-premises directories.

● Users are represented only once across all directories.

○ User identities exist across multiple directories. Match using:

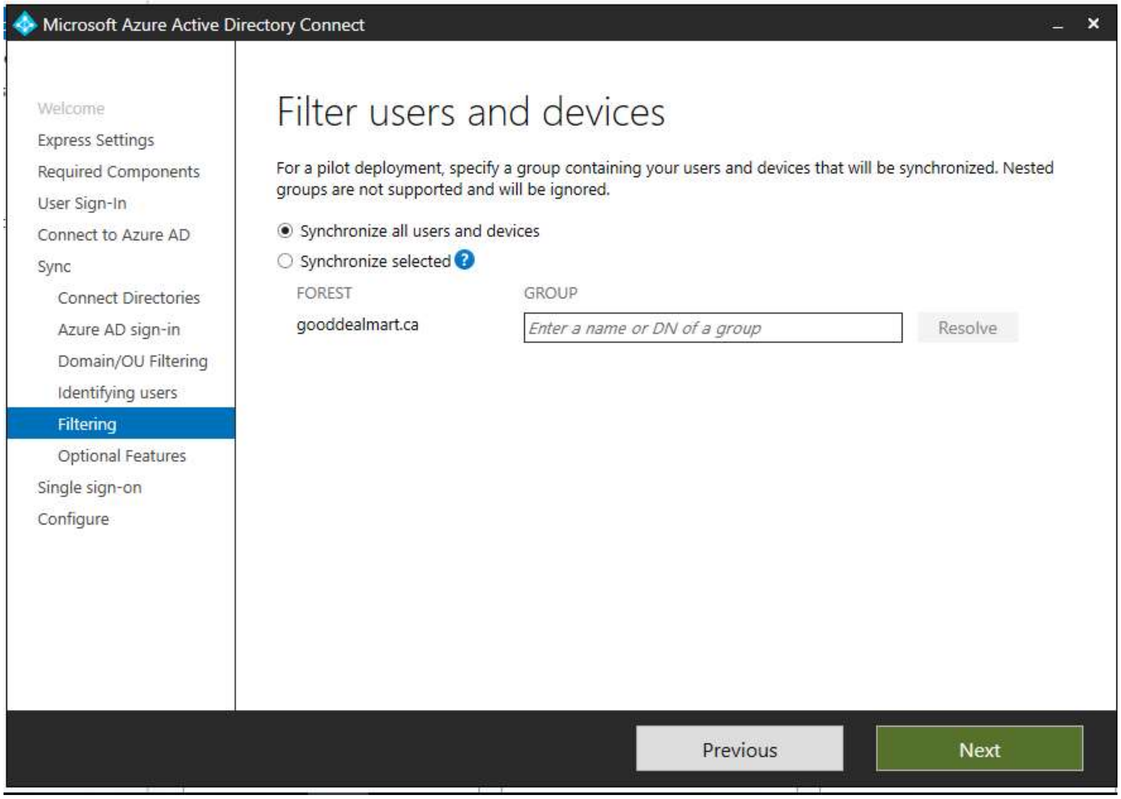
- ● Mail attribute
- ○ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
- ○ SAMAccountName and MailNickName attributes
- ○ A specific attribute

Select how users should be identified with Azure AD.

● Let Azure manage the source anchor for me.

○ A specific attribute

11. Click **Next** on the **Filter users and devices** page.



Filter users and devices

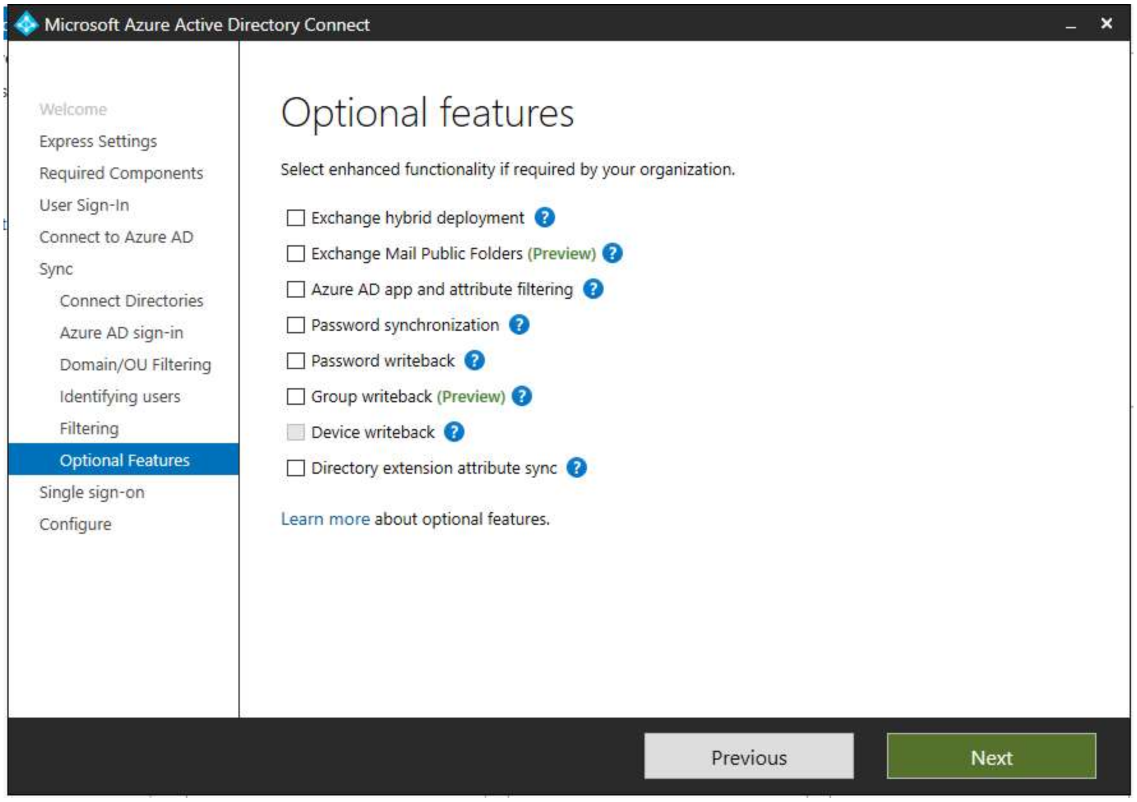
For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

● Synchronize all users and devices

○ Synchronize selected

FOREST	GROUP
gooddealmart.ca	*Enter a name or DN of a group*

12. On **Optional features** page, select **optional features if required**, click **Next**.



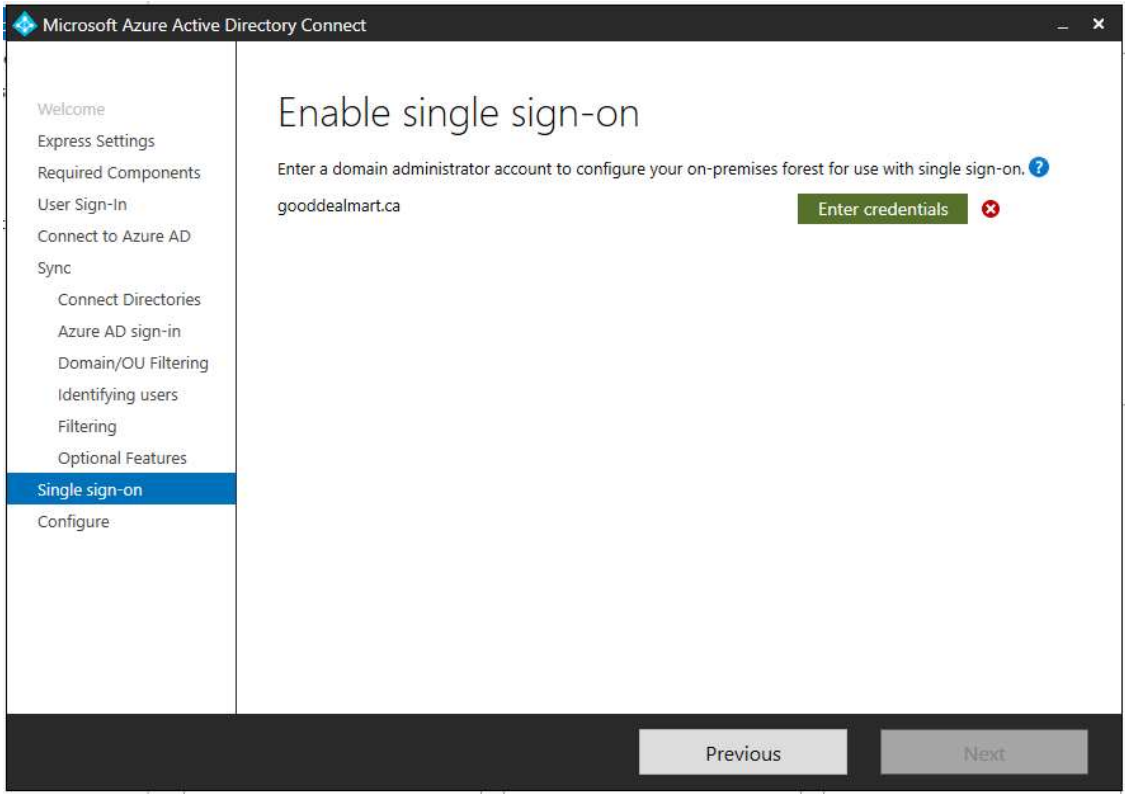
Optional features

Select enhanced functionality if required by your organization.

☐ Exchange hybrid deployment ?
☐ Exchange Mail Public Folders (Preview) ?
☐ Azure AD app and attribute filtering ?
☐ Password synchronization ?
☐ Password writeback ?
☐ Group writeback (Preview) ?
☐ Device writeback ?
☐ Directory extension attribute sync ?

Learn more about optional features.

13. On the Enable single sign-on page, click Enter credentials.

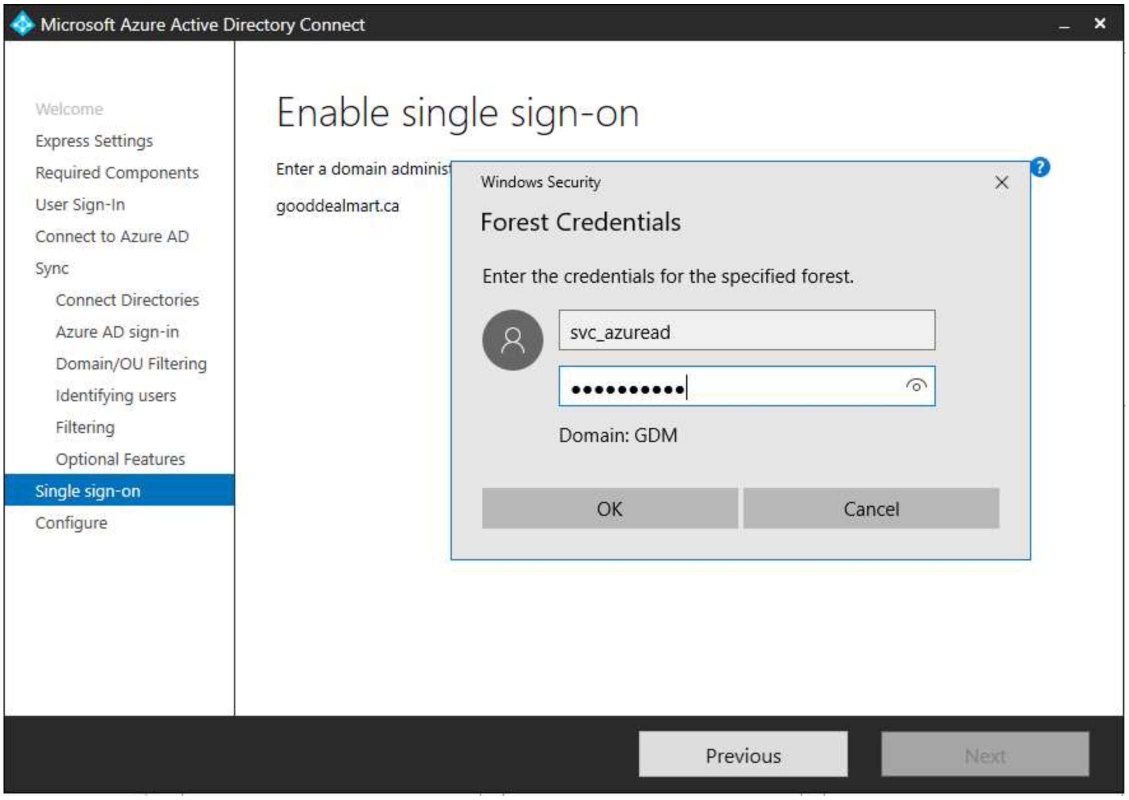


Enable single sign-on

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

gooddealmart.ca

14. Enter domain admin service account, click **OK** and then click **Next**.



Enable single sign-on

Enter a domain adminis

gooddealmart.ca

Windows Security

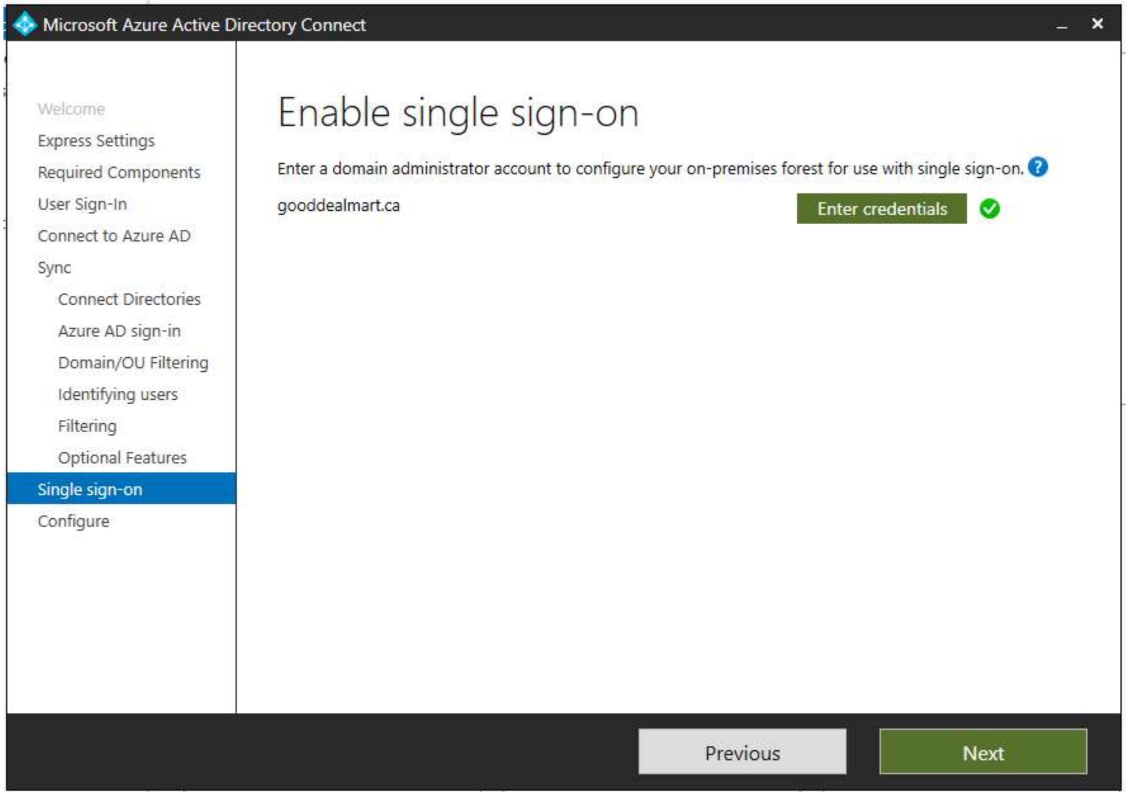
Forest Credentials

Enter the credentials for the specified forest.

svc_azuread

●●●●●●●●●●●

Domain: GDM

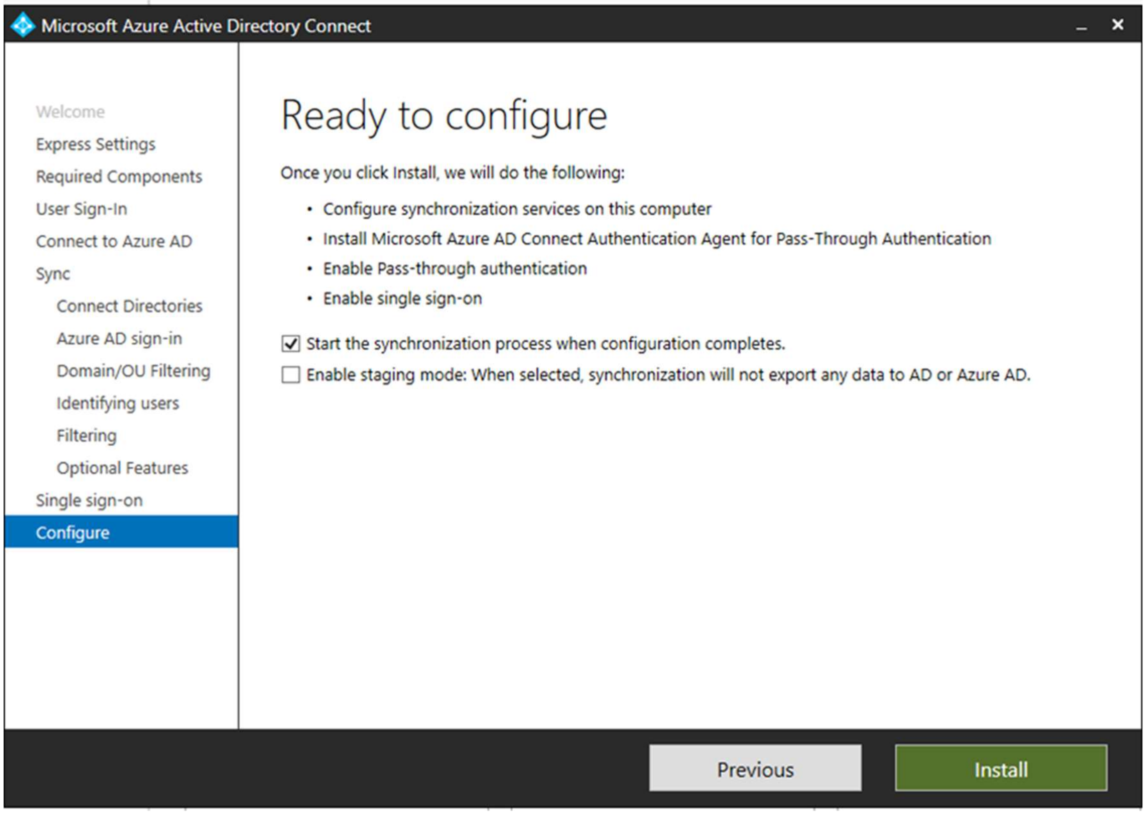


Enable single sign-on

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

gooddealmart.ca

15. Select **Start the synchronization process when configuration completes** on the **Ready to Configure** page, click **Install.**



Ready to configure

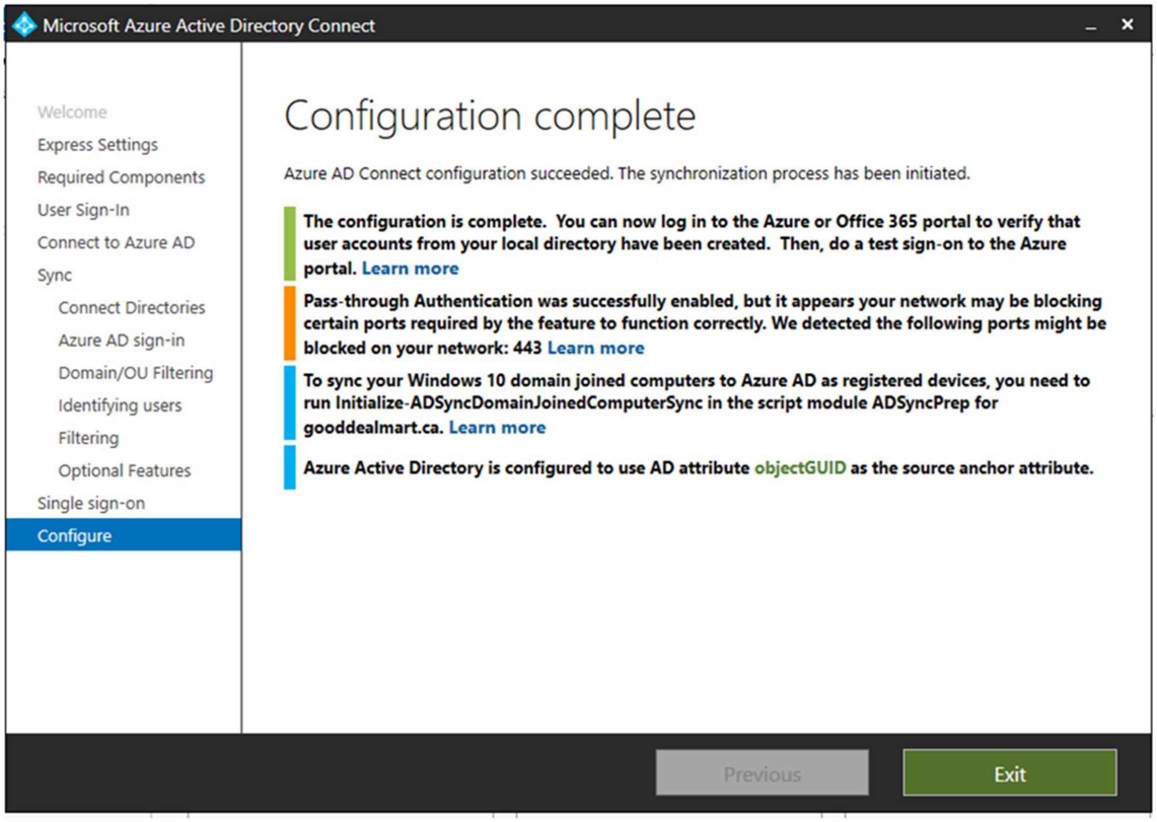
Once you click Install, we will do the following:

- Configure synchronization services on this computer
- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication
- Enable single sign-on

☑ Start the synchronization process when configuration completes.

□ Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

16. Click **Next** on **Configuration complete** page and then click **Exit**.



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

Pass-through Authentication was successfully enabled, but it appears your network may be blocking certain ports required by the feature to function correctly. We detected the following ports might be blocked on your network: 443 Learn more

To sync your Windows 10 domain joined computers to Azure AD as registered devices, you need to run Initialize-ADSyncDomainJoinedComputerSync in the script module ADSyncPrep for gooddealmart.ca. Learn more

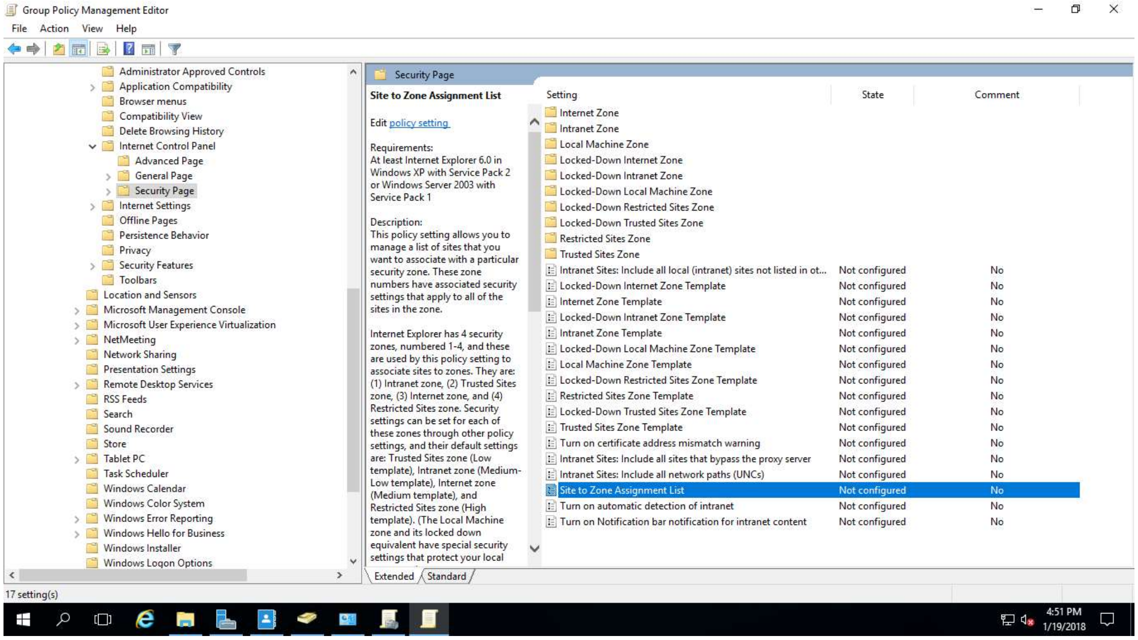
Azure Active Directory is configured to use AD attribute objectGUID as the source anchor attribute.

17. In order to allow Azure AD to accept Kerberos tickets you need to configure a client GPO. You need to publish these two URL's to your Internet Zone Settings.

    https://autologon.microsoftazureread-sso.com

    https://aadg.windows.net.nsatc.net

18. Open Group Policy Management Editor, go to **User Configuration→Policies→Administrative Templates→Windows Components→Internet Explorer→Internet Control Panel**, click **Security Page,** and then double click **Site to Zone Assignment List**.



Site to Zone Assignment List

Edit policy setting

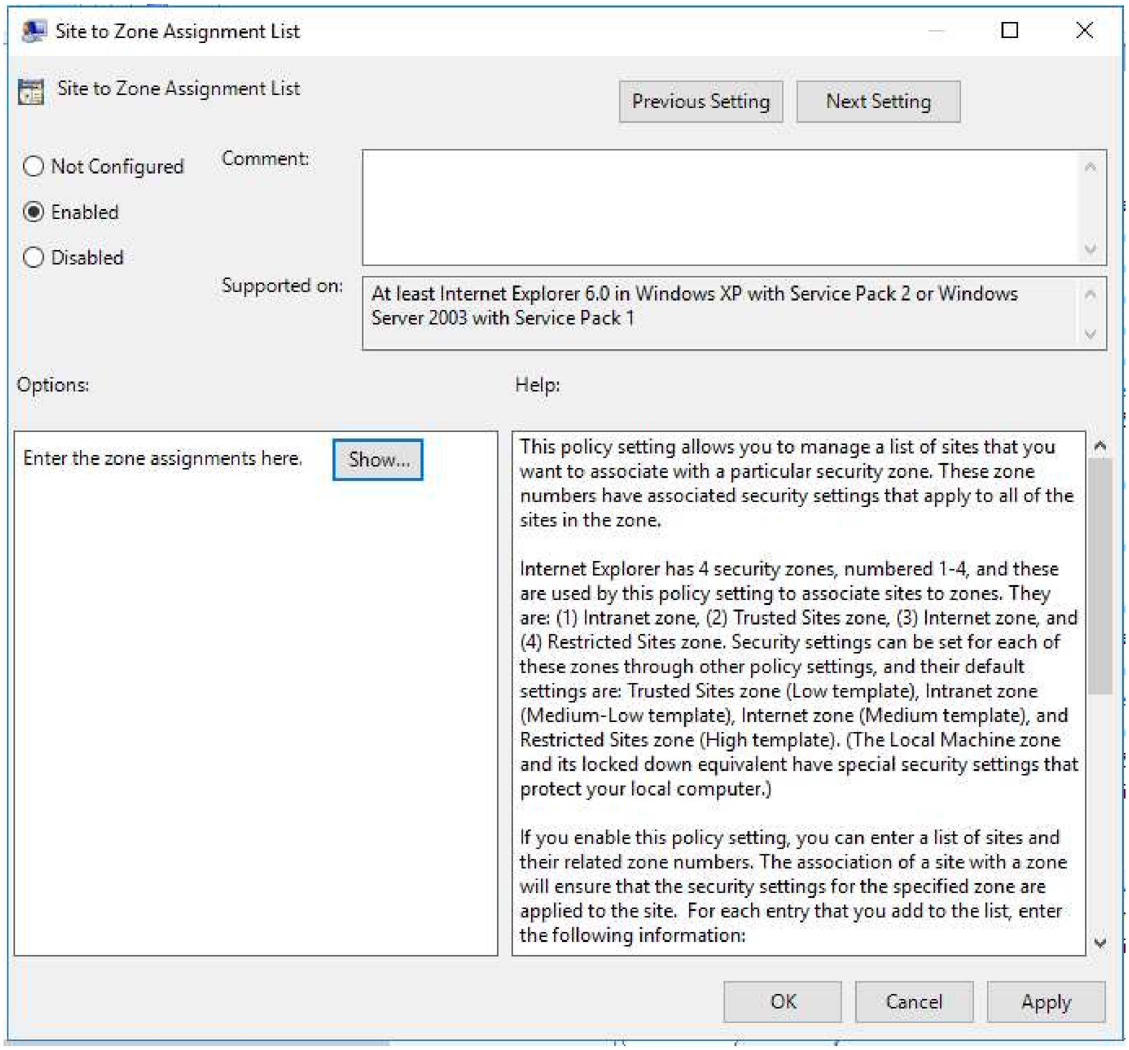
Requirements:
At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1

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

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 ot...	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

19. On the **Site to Zone Assignment List** page, click Enabled and then click **Show…**



○ Not Configured

● Enabled

○ Disabled

Comment:

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

Options:

Enter the zone assignments here.

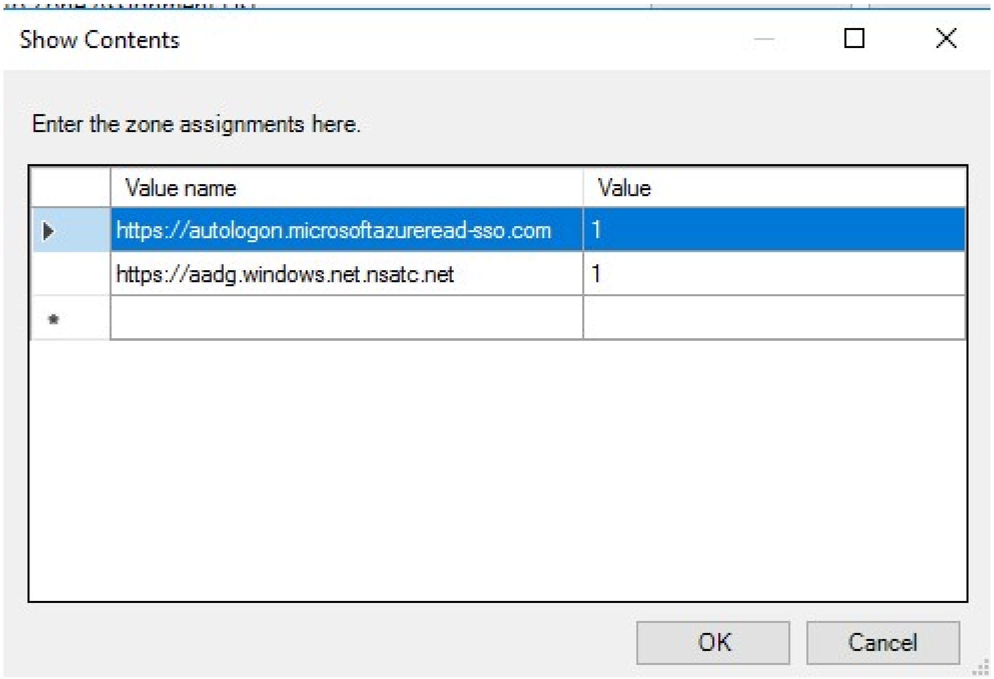
Help:

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.)

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 the following information:

20. Add two URLs as above and click OK.



Enter the zone assignments here.

Value name	Value
https://autologon.microsoftazureread-sso.com	1
https://aadg.windows.net.nsatc.net	1

21. Link this GPO to your domain.