

|  |
| --- |
| Azure AD Connect (POC) |
| Made for Coretech Christmas Blog 2015 |
| **Author:** Bjørn Studsgaard Voss |
| **Create date:** 15 December 2015 |
| **Change date:** 15 December 2015 |
| **Document revision:** 1.0 |
|  |
|  |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Author/Editor** | **Date** | **Revision** | **Notes** |
| bsv@coretech.dk | 16-12-2015 | 1.0 | Simple documentation on how to sync On-Premise AD to Azure. |
|  |  |  |  |

Contents

[Revision History 2](#_Toc438039037)

[Introduction 3](#_Toc438039038)

[Pre-requisites 4](#_Toc438039039)

[Create Azure Subscription (Part 1) 5](#_Toc438039040)

[Verify domain in Azure (Part 2) 8](#_Toc438039041)

[Create Azure Sync user (Part 3) 12](#_Toc438039042)

[Configure on-premise users (Part 4) 16](#_Toc438039043)

[Install Azure AD Connect (Part 5) 17](#_Toc438039044)

[Verify that configuration works (Part 6) 23](#_Toc438039045)

# Introduction

This document is a Step by Step guide showing how to setup a simple POC for Azure AD.

Document will demonstrate how to connect On-Premise AD to Azure AD with a limited set of Users using Azure AD Connect.

Azure AD can be used to validate users against Office 365 or Azure services.

Document is very detailed, with screen capture of all steps and most customers will be able to execute all parts of the process them self.

Feel free to share. Made for Coretech Yearly Christmas Blog 2015.

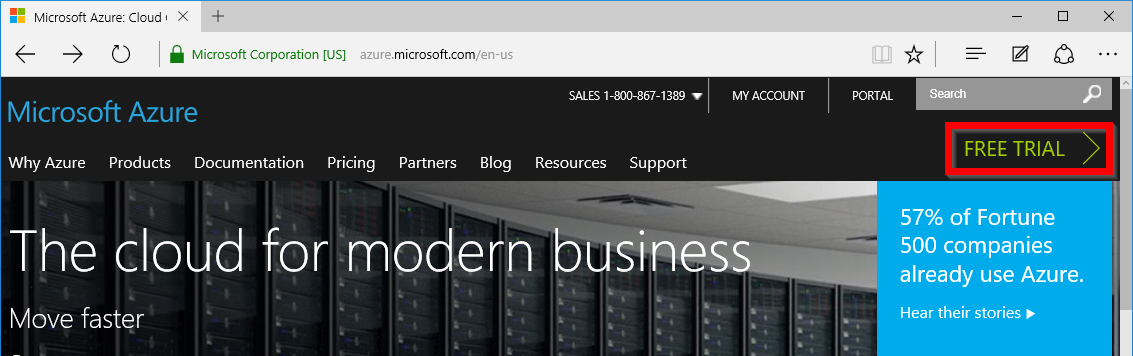
# Pre-requisites

**Below are pre-requisites that should be created prior to complete this installation**

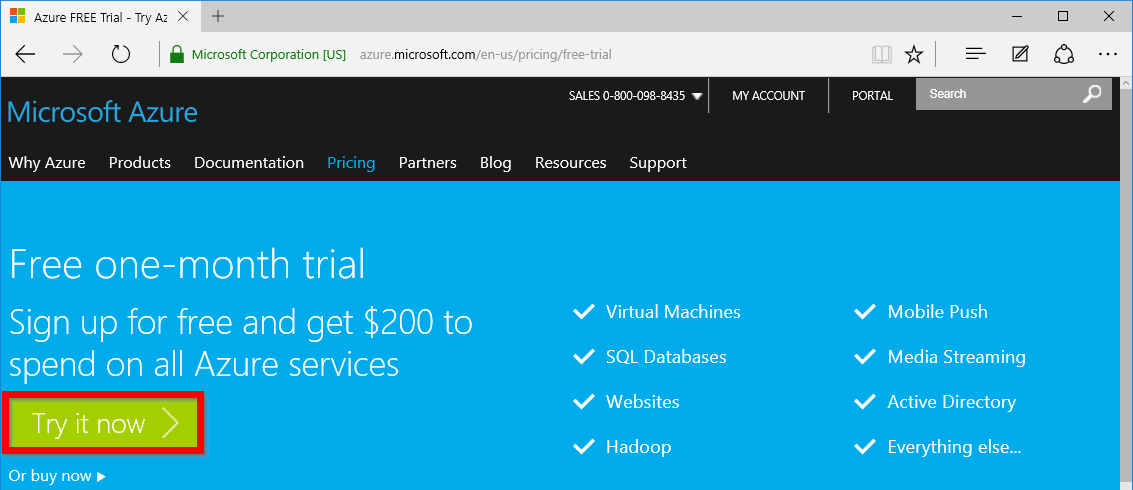
|  |  |  |
| --- | --- | --- |
| **Type** | Settings | Remarks |
| **Public Domain Name** | **Name:** Sandbx.dk | Access to change DNS records on a public domain name.Sandbx.dk used as example throughout this documentation |
| **On-Premise Service Account** | **Name:** SVC-ON-PREM-AZ-SYNC  **Rights:** Enterprise Admin (Important)    Machine generated alternative text: SVC-ON-PREM-AZ-SYNC properties  SW.I r ty  Nemee Üesktop Services Profile  Generzl k&ess A:count  Published c  control  Editor  Profile Tdepbones Orgarization  Replic&ion Cbject  Doman LISES  Services  AD SandBX | Service account is used to create/read settings from On-Premise AD. |
| **On-Premise Group** | **Name:** Azure-Synced-Users  **Type:** Global, Security    Machine generated alternative text: Create in :  Group name:  An -S ynced  Group name  Azu re-Synced4Jses  Group  @Global  O  New Object - Grou  AD. San&X .«Sardbx/Groeos  Gr•OLP | Group is used to identify users that should be synced to Azure AD. |
| **On-Premise Server** | **OS:** Windows Server2012 R2 (Recommended)<https://azure.microsoft.com/da-dk/documentation/articles/active-directory-aadconnect-prerequisites/#component-prerequisites>    **Hardware:** 2 vCPU, 4 GB Ram and 70 GB disk (Recommended) <https://azure.microsoft.com/da-dk/documentation/articles/active-directory-aadconnect-prerequisites/#hardware-requirements-for-azure-ad-connect> | Server will host “Azure AD Connect” and handle synchronization of users and passwords HASHs.  “Azure AD Connect” can co-exist with other services. But we recommend that a dedicated server is created for this POC. |

# Create Azure Subscription (Part 1)

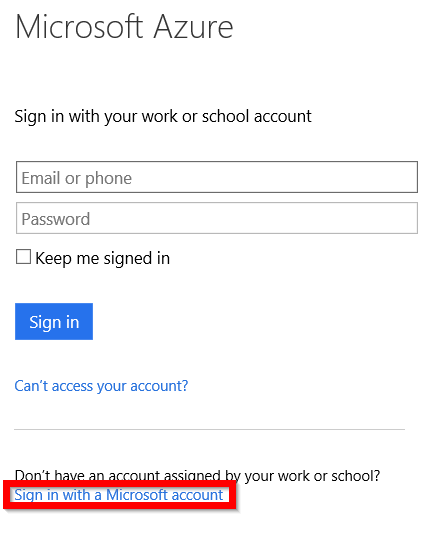
First step is to create an Azure subscription to contain the Azure AD.

****

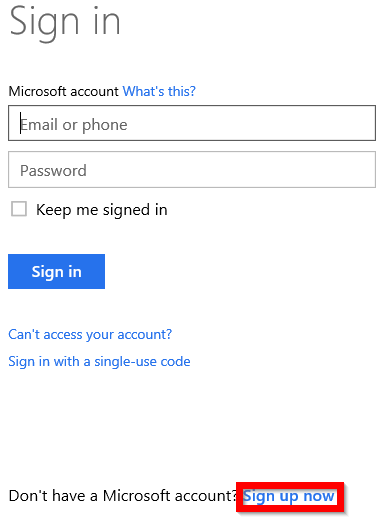
To create a Azure subscription go to [www.azure.com](http://www.azure.com) and press “FREE TRIAL >”

****

Press “Try it now >”

****

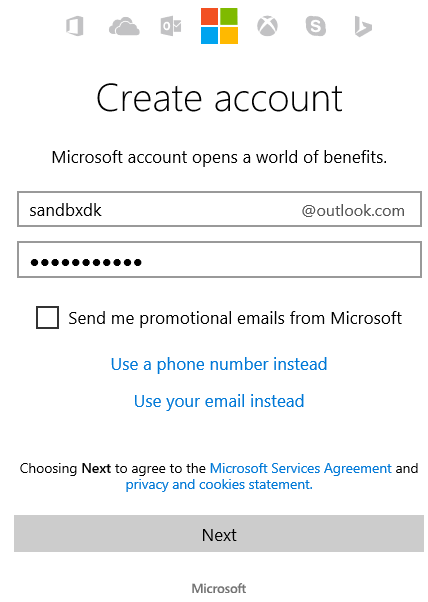
Press “Sign in with a Microsoft account”

****

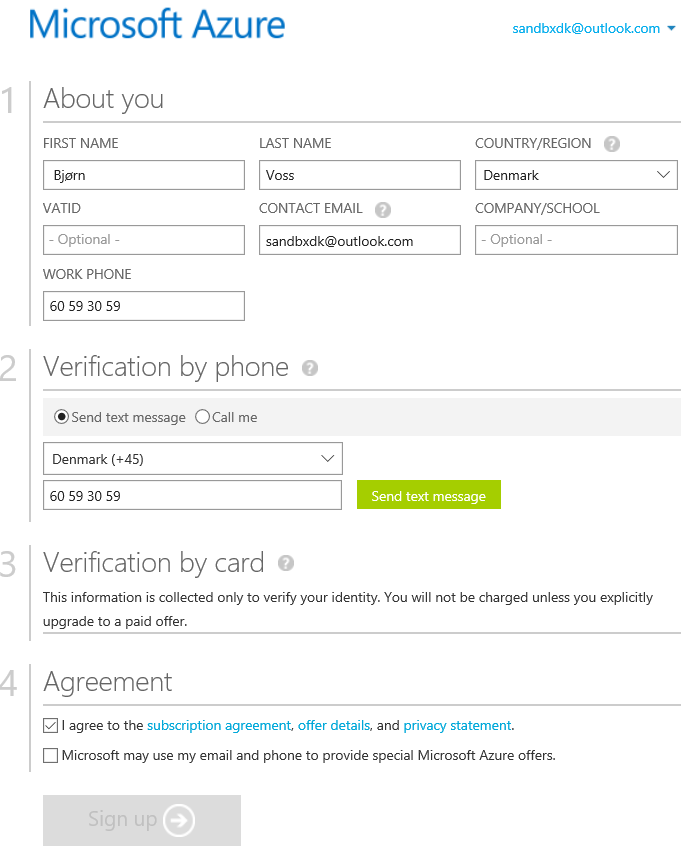
We recommend creating a dedicated account for this purpose, but since this only is a POC, then an existing Microsoft Account can be used.

Press “Sign up now”.

Notice that if an On-Premise account is use, then make sure that the account is not synced to Azure AD. If account to synched to Azure AD then issues might occur.

****

Fill in the login name that you wish to use for the account. Validation can be done by either email or phone.

****

Above is example of verification by phone.

Fill in all information and press “Send text message”.

Text message will now be received on the phone and should be entered.

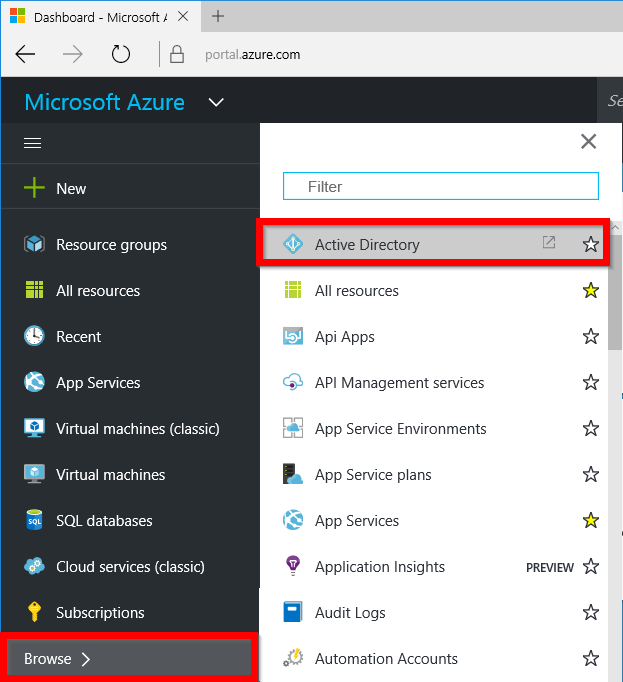
Once validation is completed, “Verification by card” will appear (This can take up to 1 minute)

Fill in card information and complete by pressing “Sign up ->”.

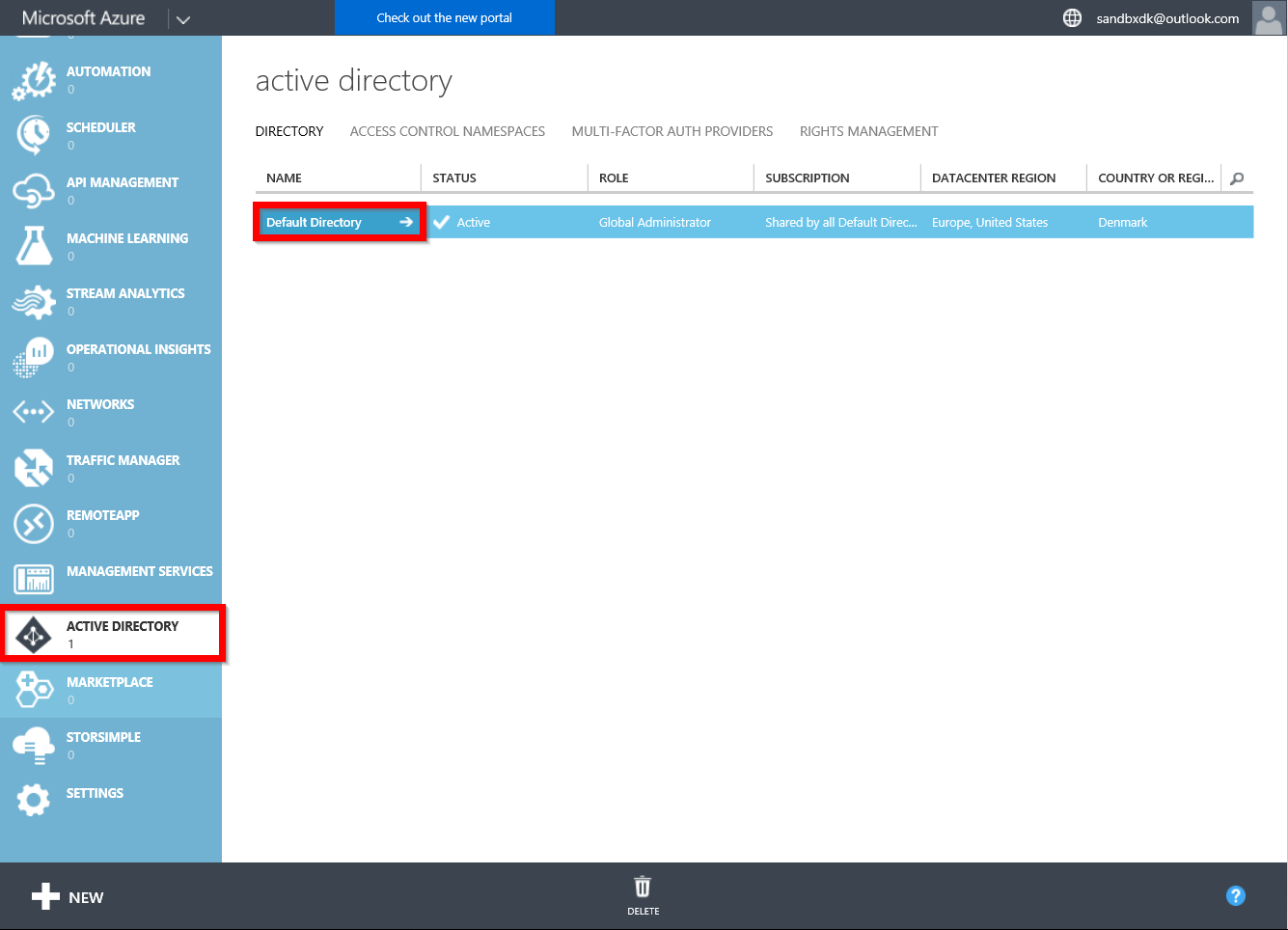
An Azure subscription will now be created. (App. 5 minutes)

# Verify domain in Azure (Part 2)

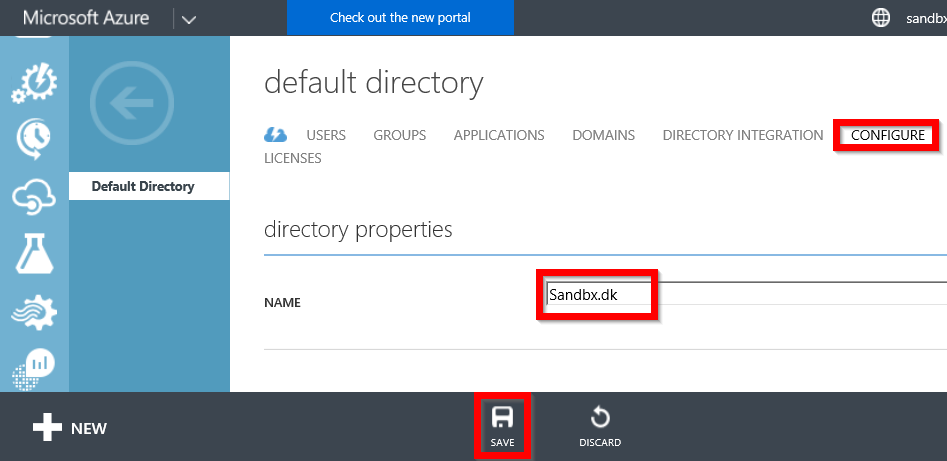
The previously created Microsoft Account will automatically be logged in.

****

Choose “Browse >” followed by “Active Directory”. (Page will be redirected to a new portal.)

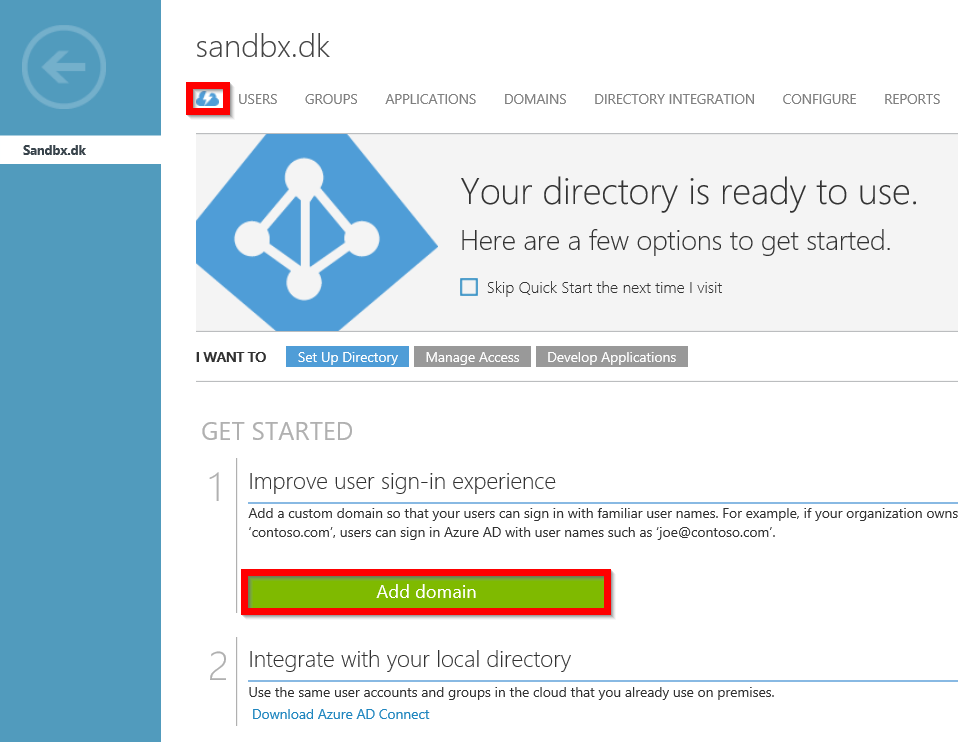
****

Choose “ACTIVE DIRECTORY” on the left side, followed by “Default Directory”.

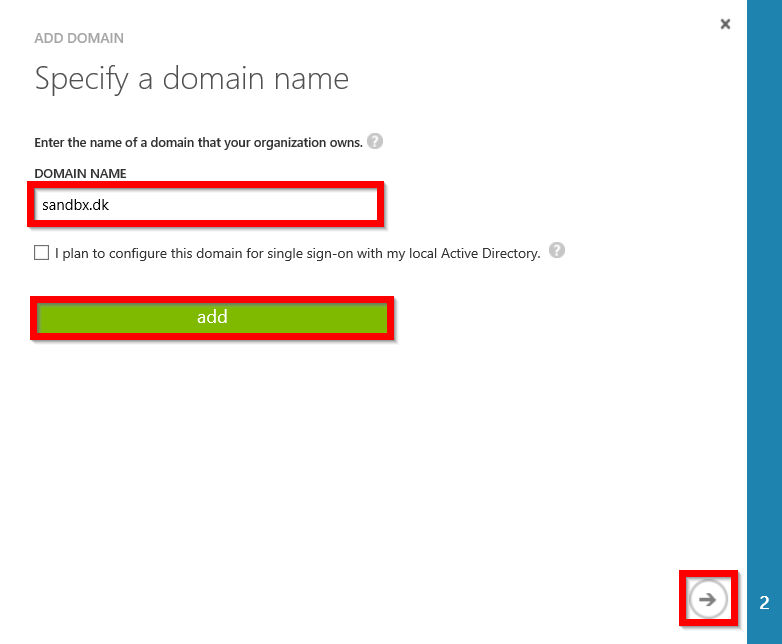
****

Rename “Default Directory” to the public domain name and complete by pressing “Save”.

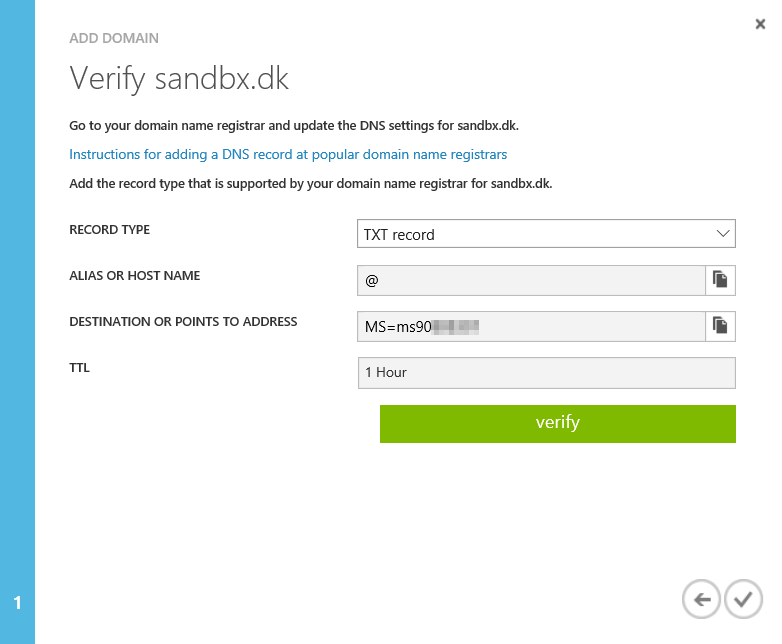
(This step is not mandatory but makes it easier to identify domains when having multiple accounts).

****

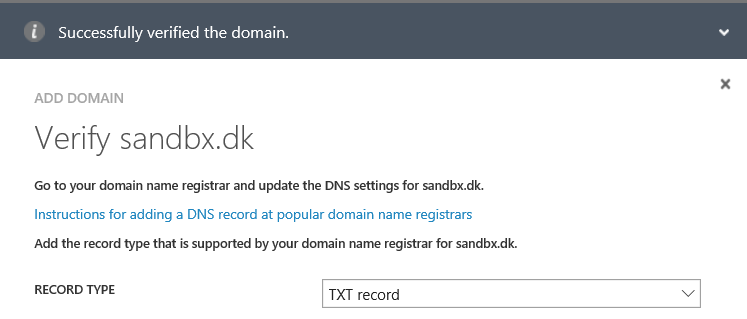
Choose the “Cloud Icon” in the top left, followed by “Add domain”.

****

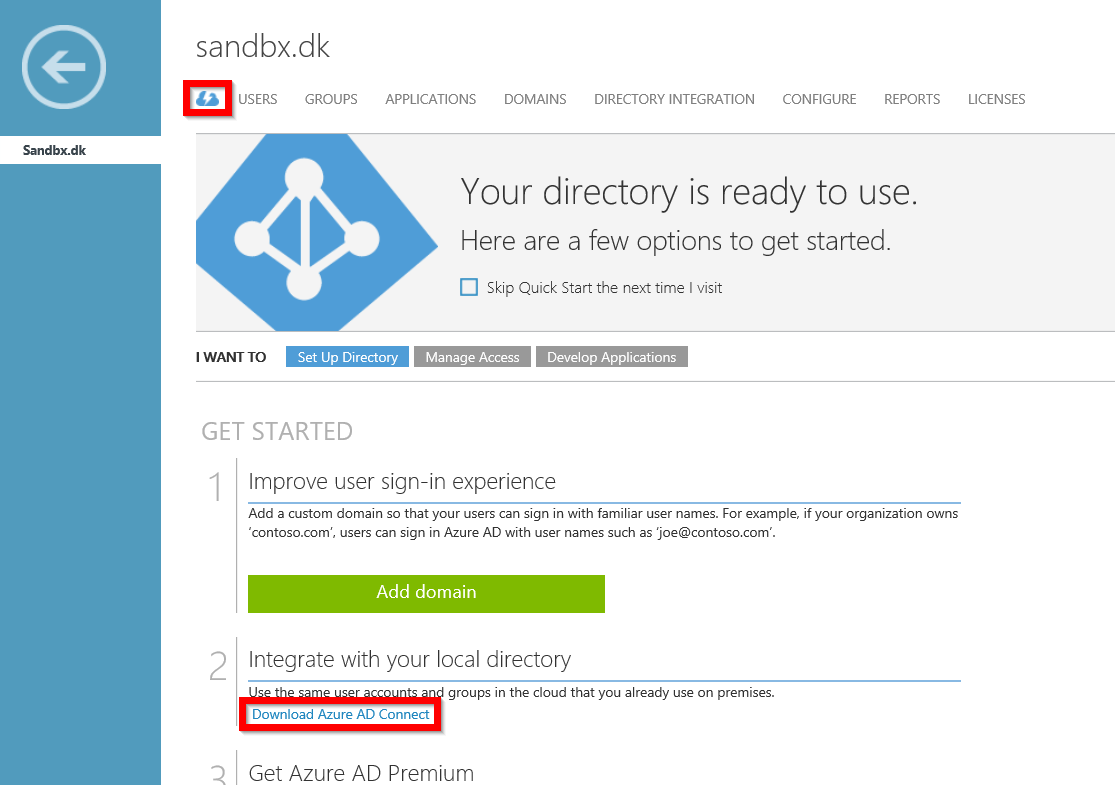
Fill in the public domain name, followed by pressing “add” and “->”.

****

To verify the public domain an TXT or MX record will have to be added to the public DNS. This process is individual depending on where the domain is hosted. Guides can be found in the link on the page.

****

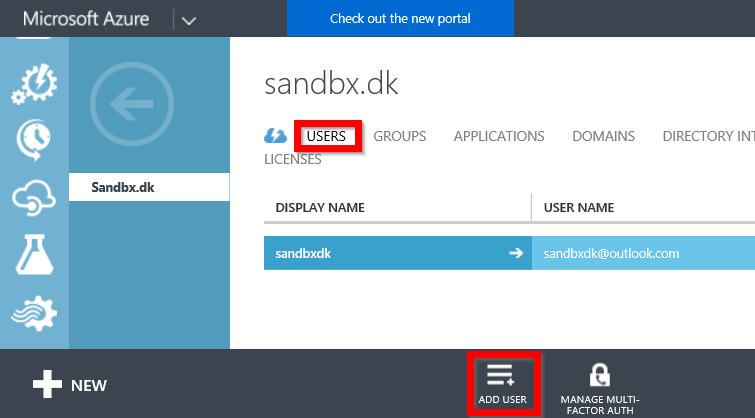
It can take up to 72 hours before TXT/MX records are replicated worldwide. But normally it only takes 10-20 minutes.

****

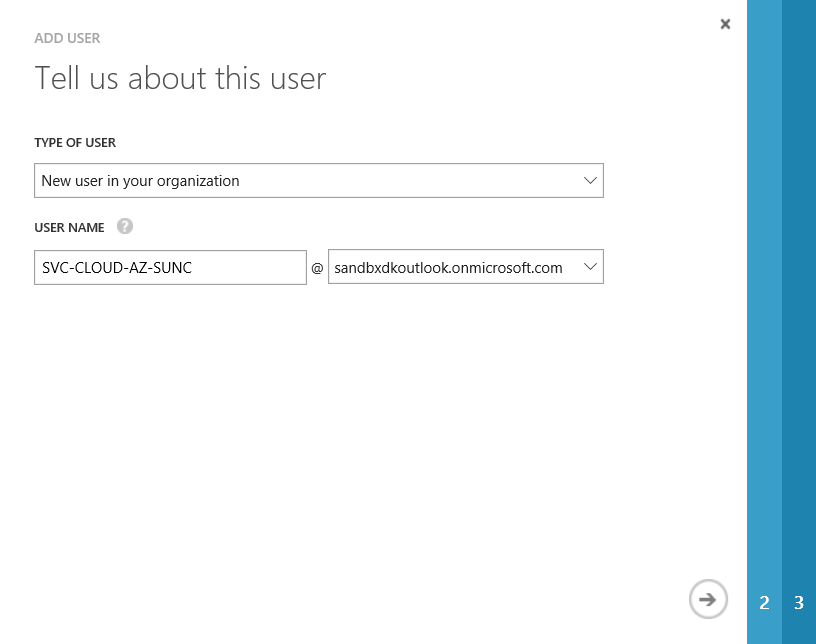
When the domain is validated, press “Download Azure AD Connect” and download latest   
version of Azure AD Connect. Copy the installation file to the newly created server, that will be used as sync server.

# Create Azure Sync user (Part 3)

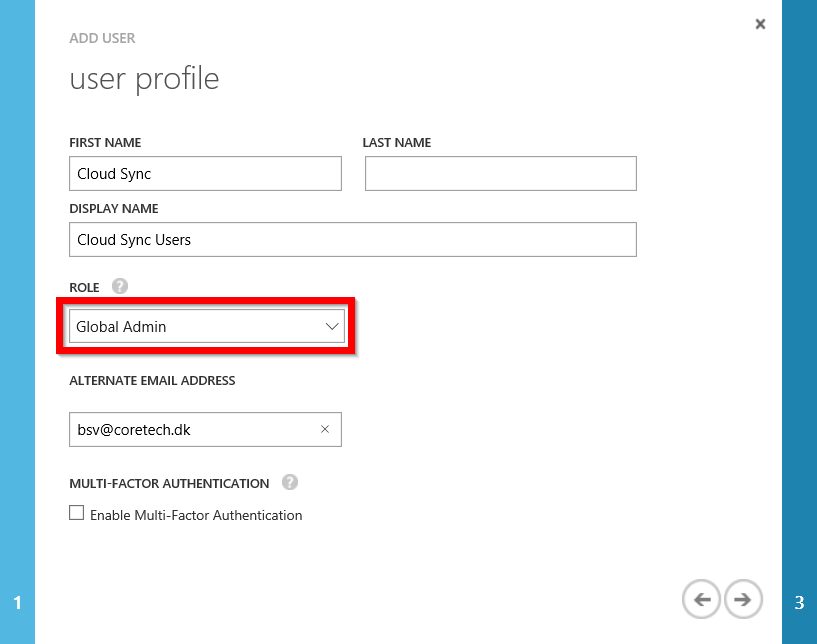
A dedicated user is needed in Azure AD to add users. The sync users should be “Global Administrator”.

****

Choose “Users” and press “ADD USER”.

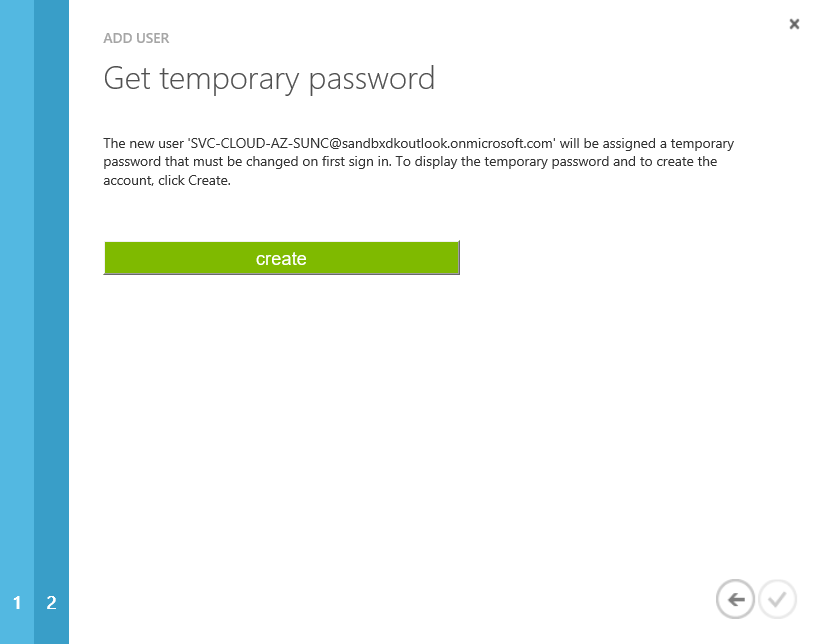
****

Type in name of sync user and press “->” (next)

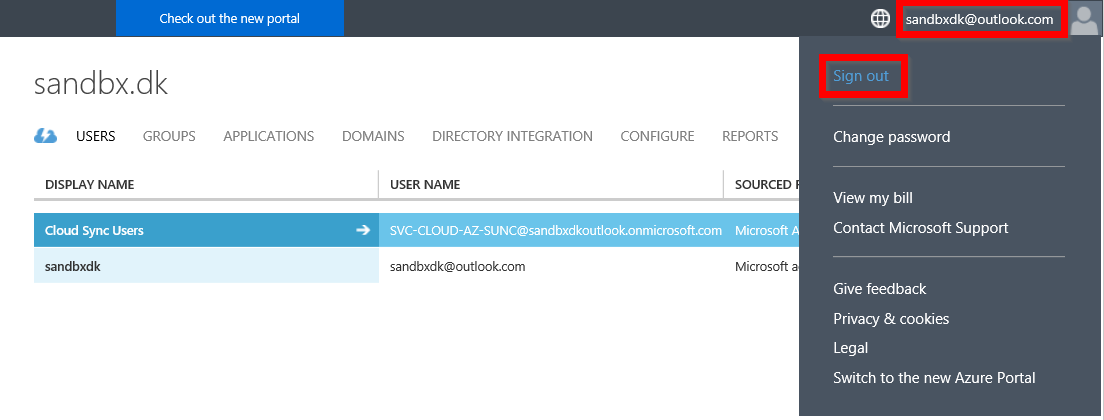
****

Change ROLE to “Global Admin” and fill in ALTERNATIVE EMAIL ADDRESS.

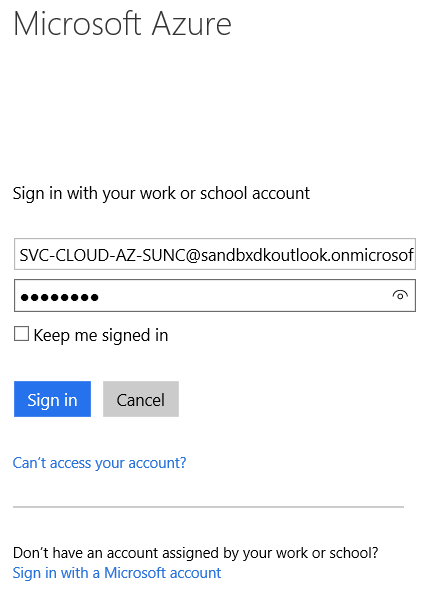
Complete by pressing “->” (Next).

****

Press “create” and note down username and temporary password.

****

A new password is needed to the newly created sync user. Sign out existing user by pressing “Sign out” in the user profile.

****

Enter credential and password for the sync user and press “Sign in”.

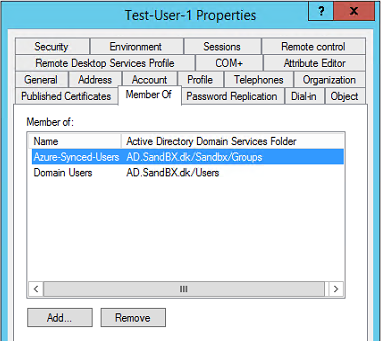
****

Create new password.

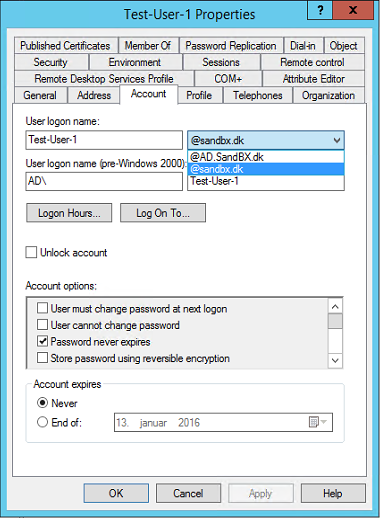
Once signed in, Azure will inform that the user does not have any subscription assigned.

Since the sync user do not require any subscription choose “Sign out” to complete the process.

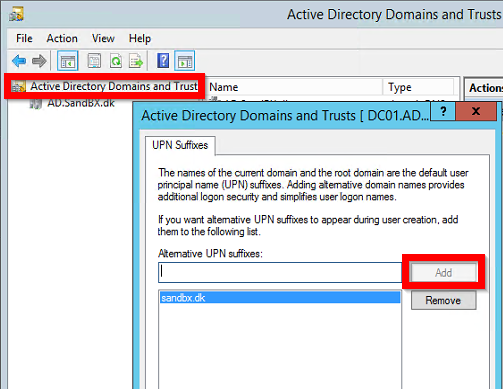
# Configure on-premise users (Part 4)



Add users that should have their credentials synchronized to Azure AD to the group mentioned in the pre-requisites.

****

Ensure that their UPN is set to public domain name in their Account page.

  
If the public domain name is not visible in UPN on the Account profile. Then it can be added in “Active Directory Domain and Trusts”.

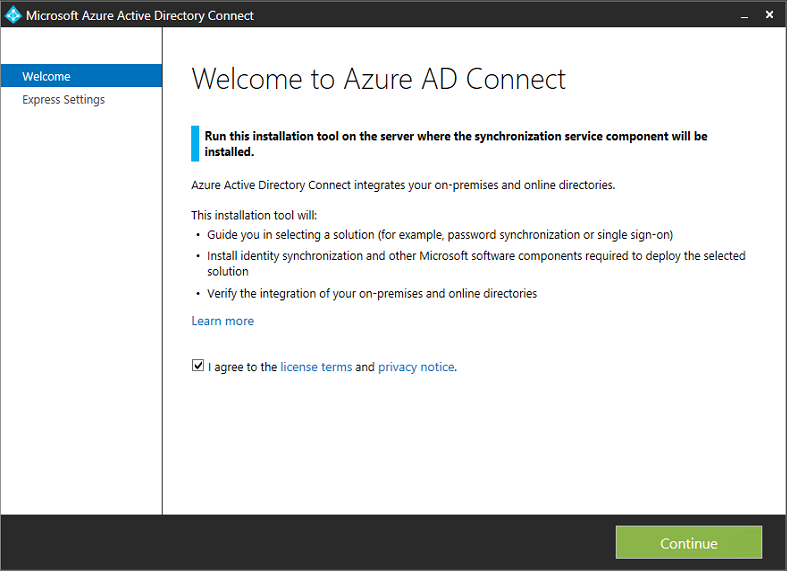
Right click “Active Directory Domains and Trust” and choose “Properties”.

Add in the public domain name in “Alternative UPN suffixes”. Complete by pressing “Add” and “Done”.

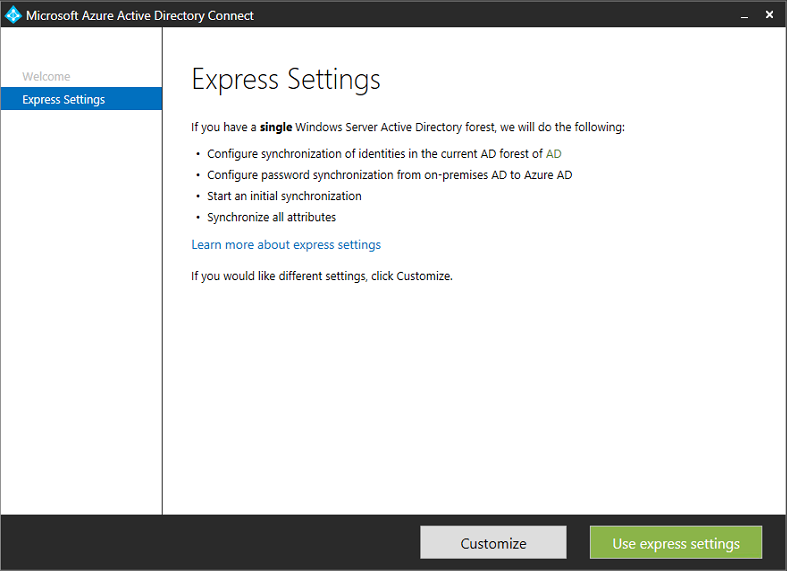
# Install Azure AD Connect (Part 5)

Login to the on-premise sync server and start the installation by executing the previously downloaded “Azure AD Connect” installation package.

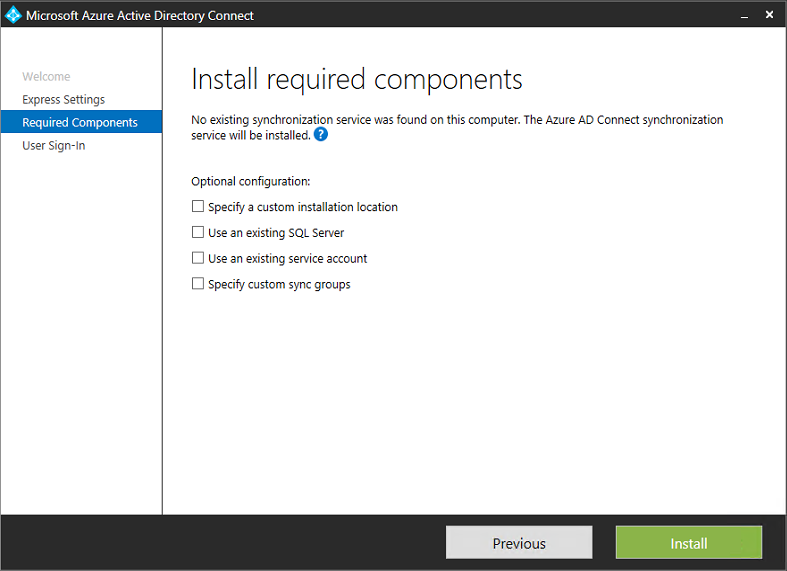
(Local server administrator rights needed)

****

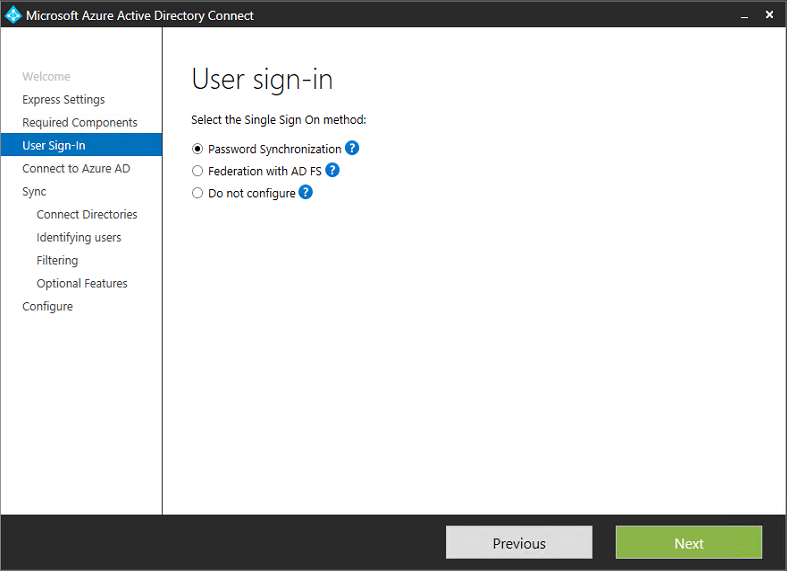
Press “Continue”.

****

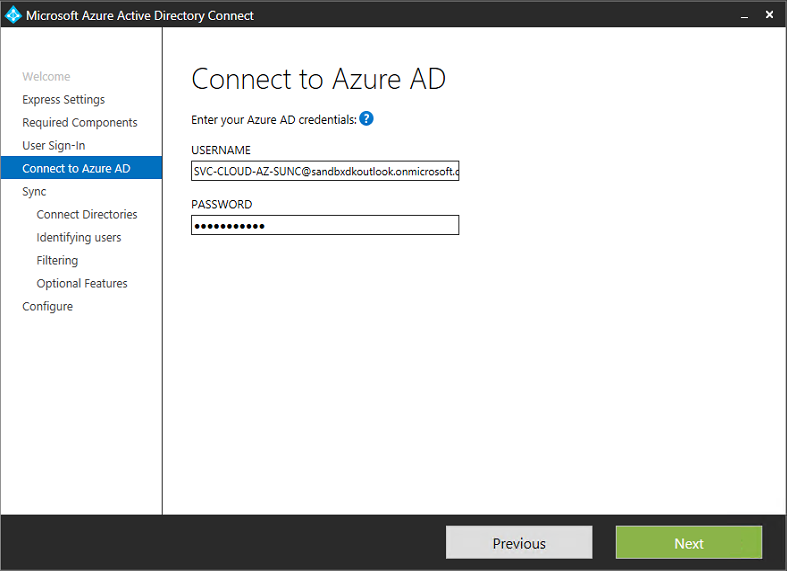
Choose “Customize”

****

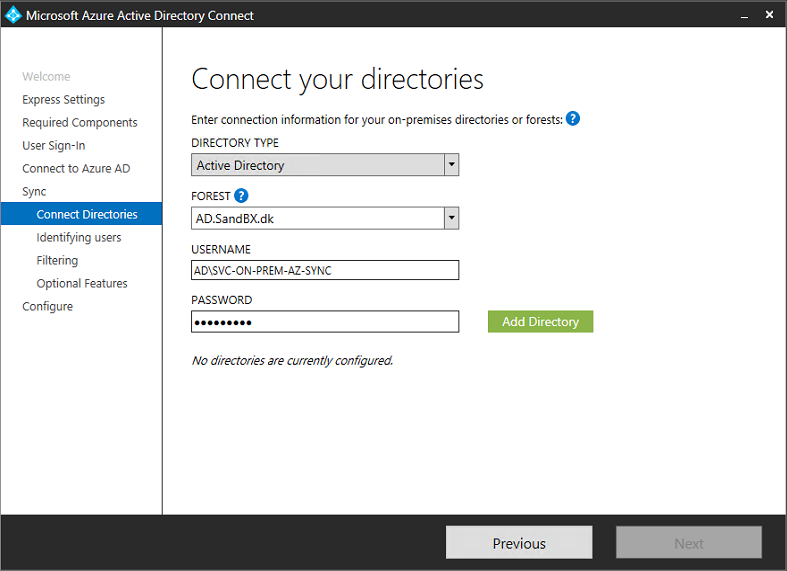
Choose “Install”.

****

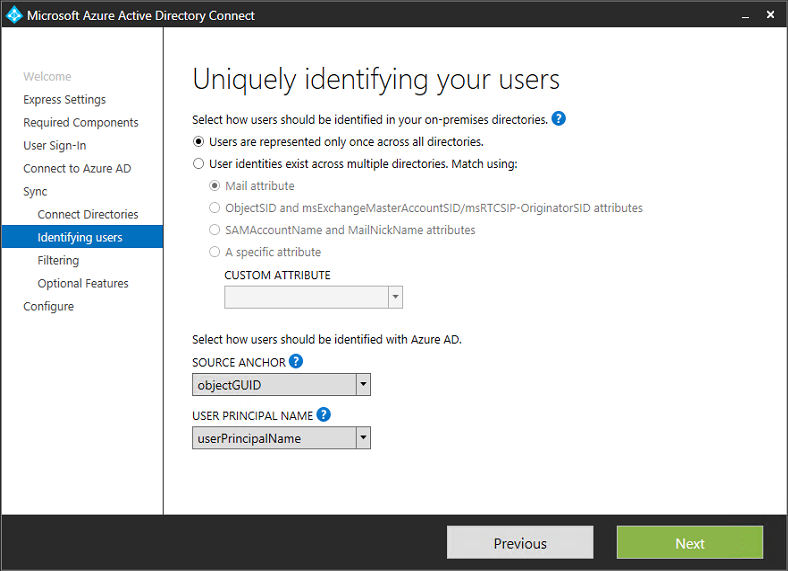
Choose “Next”.

****

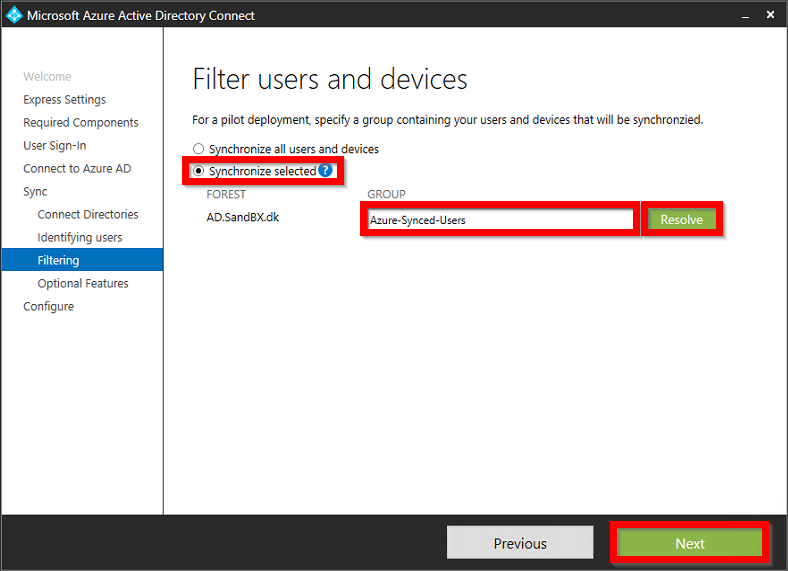
Fill in Azure Sync users USERNAME/PASSWORD and press “Next”.

****

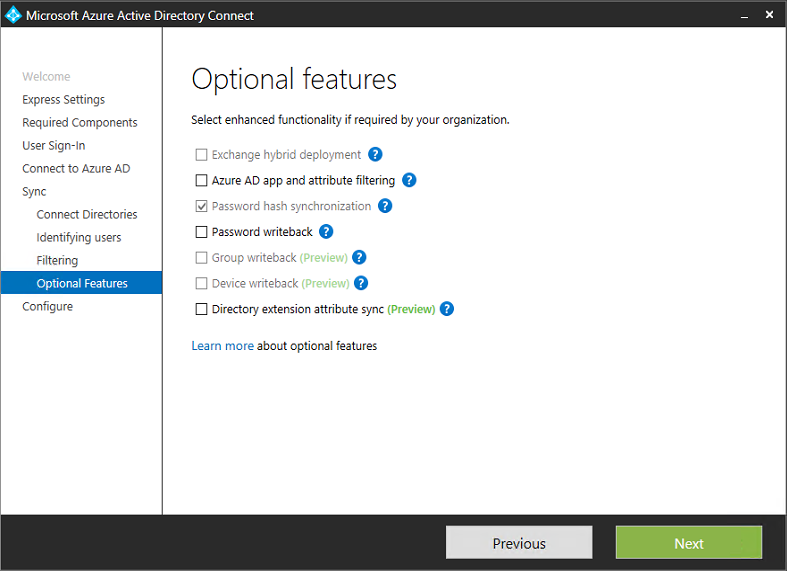
Choose FOREST and fill in USERNAME/PASSWORD of the On-Premise Service Account from the pre-requisites and press “Add Directory”. Complete by pressing “Next”.

****

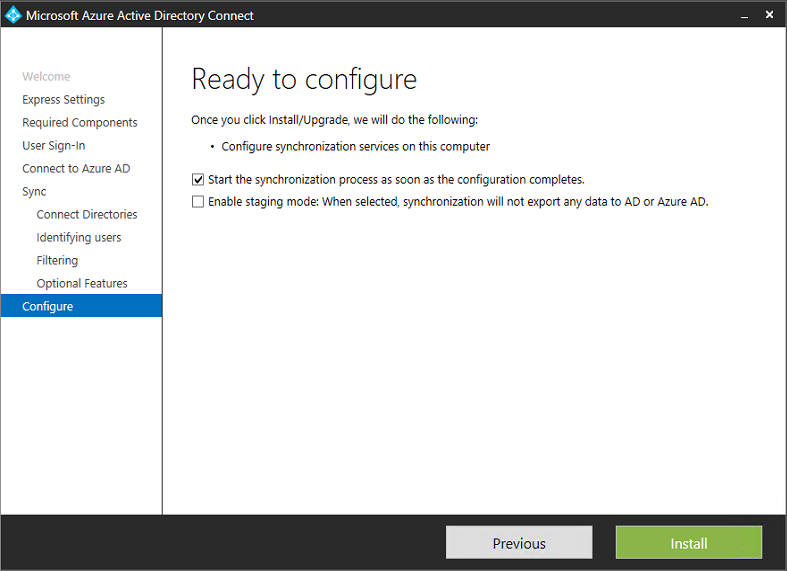
Press “Next”. (If settings are changed on this page, then some applications might not work correctly in Azure/Office365)

****

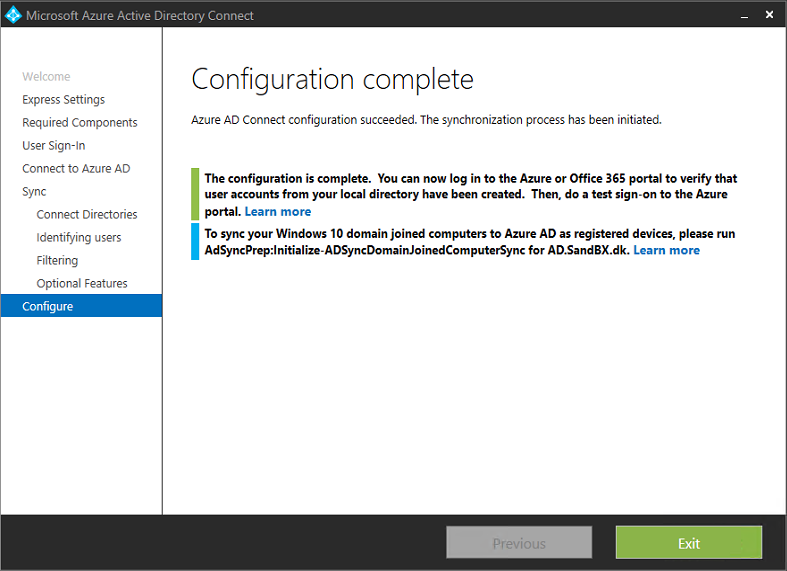
Choose “Synchronize selected” and enter GROUP from the pre-requisites and press “Resolve”. Complete by pressing “Next”.

****

Press “Next”.

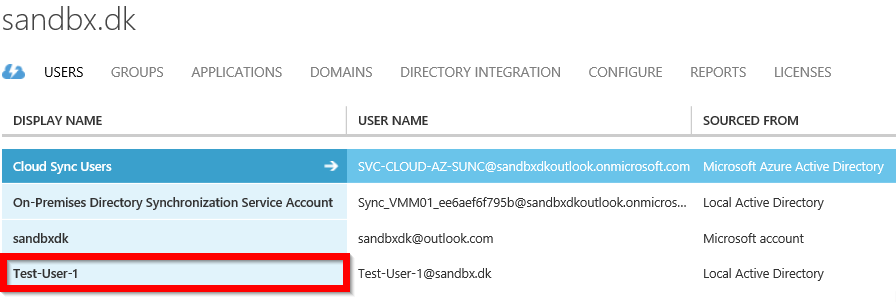
****

Press “Install” and synchronization of users joined to the defined group will begin.

****Check that everything is completed successfully and press “Exit”.

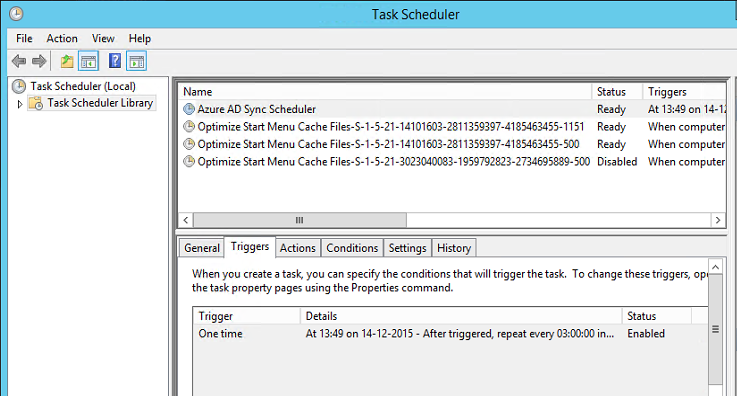
# Verify that configuration works (Part 6)

Login to Azure with the Microsoft Account.

****

Verify that users are now visible in the created Azure AD.

User can now login to Azure or Office 365 but have no subscriptions. Add in the needed products or the access rights that user requires.

****

Default Azure AD Connect sync every 3 hours. If needed this can be changed in “Azure AD Sync Scheduler” in the “Task Scheduler”.

**Azure AD Connect is now configured and sync with On-Premise AD.**

**This guide will be suitable for multiple environments and POCs. But there are many additional settings that can be configured during installation.**

**Feel free to contact us I you need assistance with special configuration (ADFS, SSO and so on)**

**Coretech wish all a Merry Christmas.**