IT Operating Manual

Q.4.xx - ITOM – Azure AD Connect

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Main IT Service Catalogue Service** | Q.4.xx |
| **Related IT Service Catalogue Service(s)** | <Service Catalogue ID : X.0.0 > |
|  | <Service Catalogue ID : X.0.0 > |
|  |  |
| **Prepared by** | J |
| **Date** |  |
| **Version** | v.1.0 |
| **Status** | Final |
|  |  |
|  |  |

Content

[Administration 2](#_Toc384718139)

[1 Introduction 2](#_Toc384718140)

[2 Context 3](#_Toc384718141)

[3 Internal Key User / Business Application Owner 3](#_Toc384718142)

[4 External Support 3](#_Toc384718143)

[5 Service responsibilities / Operational Modell 3](#_Toc384718144)

[5.1 GUS 3](#_Toc384718145)

[5.2 GITO 3](#_Toc384718146)

[5.3 GAD 3](#_Toc384718147)

[5.4 Business 3](#_Toc384718148)

Administration

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Change ID | Changes |
| <ver | <dd.mm.yyyy> | <author> | <USU change number stated as CID\_xxxx > | <changes> |

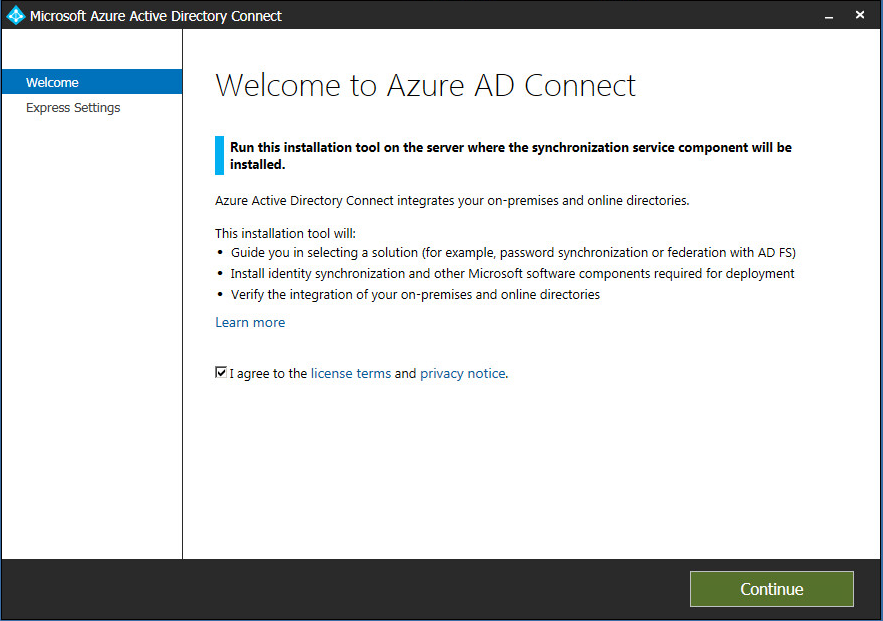
# Introduction

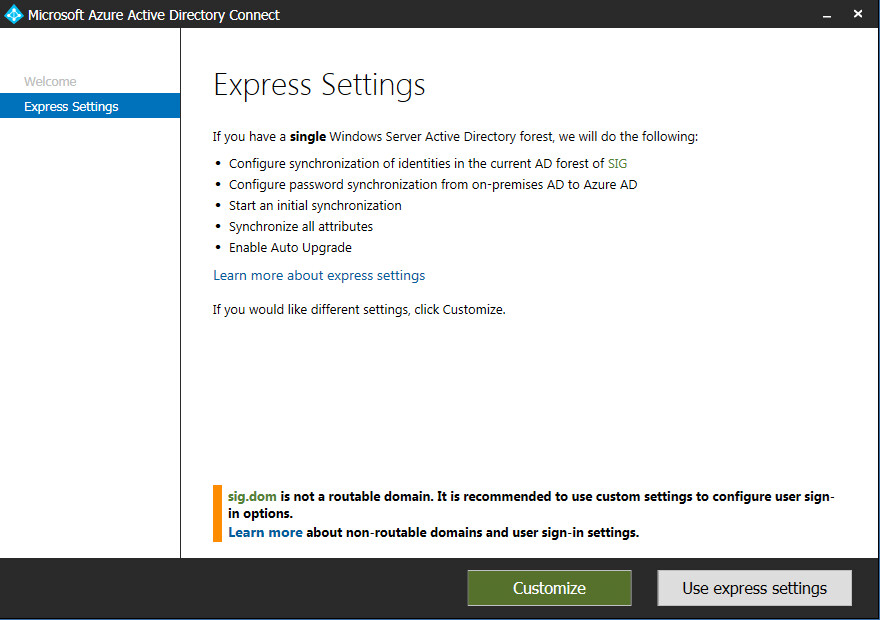
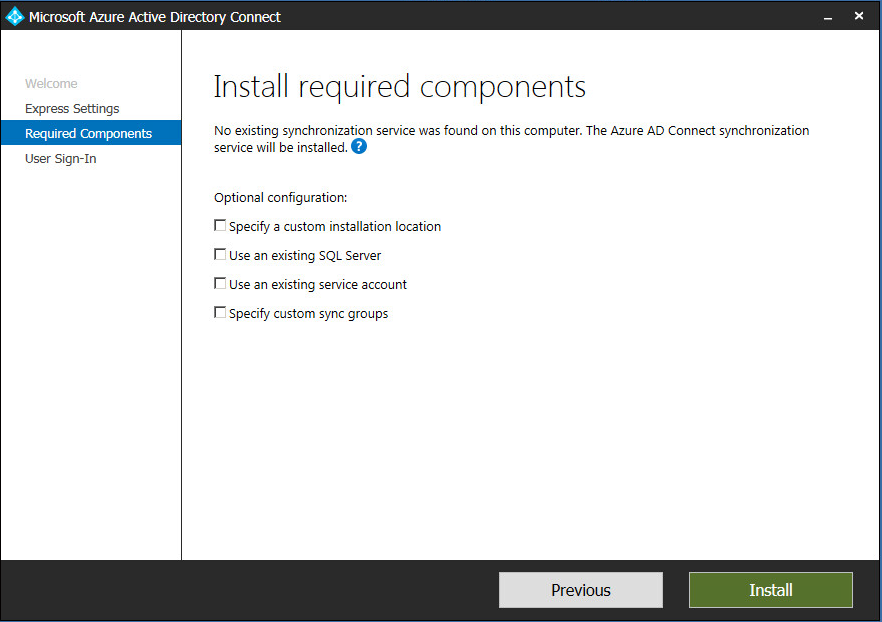
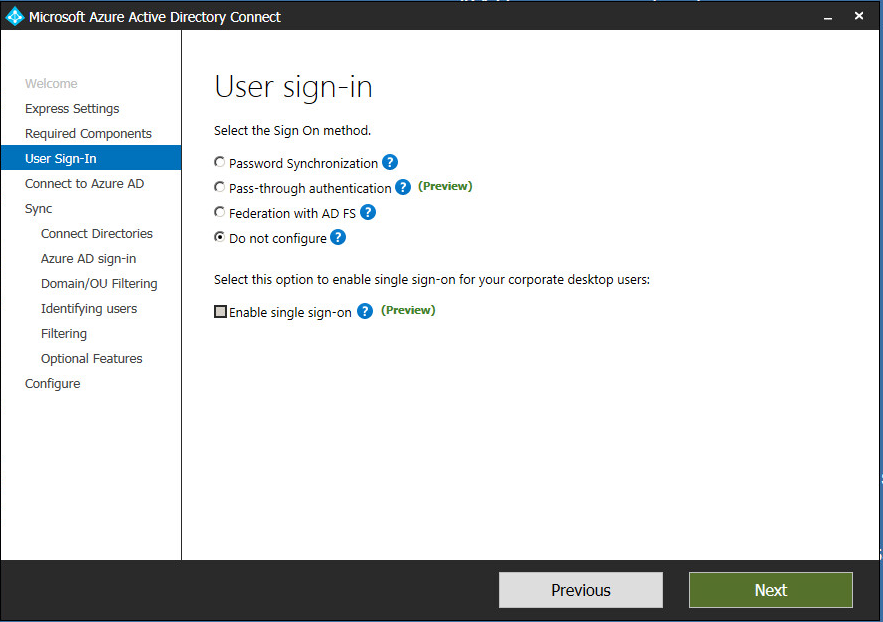
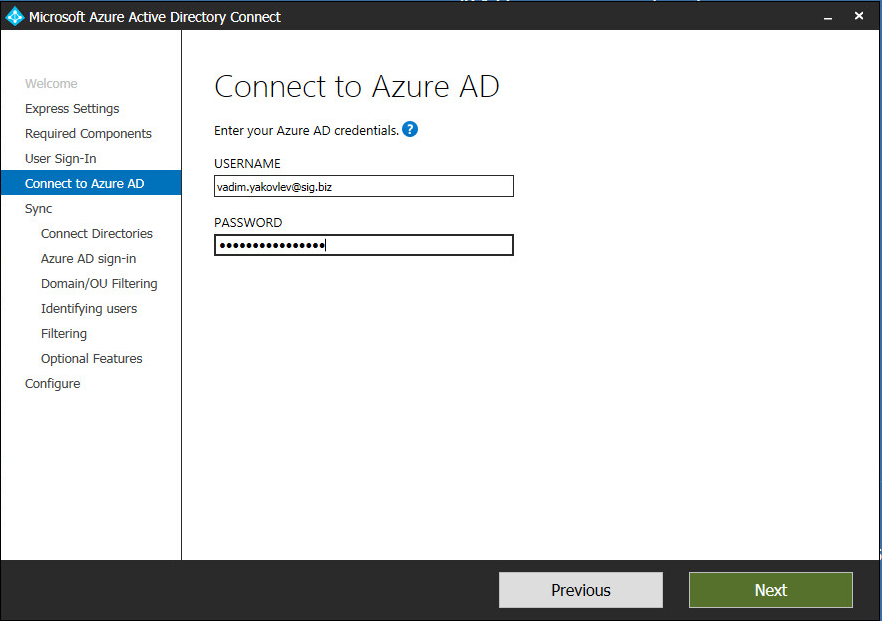
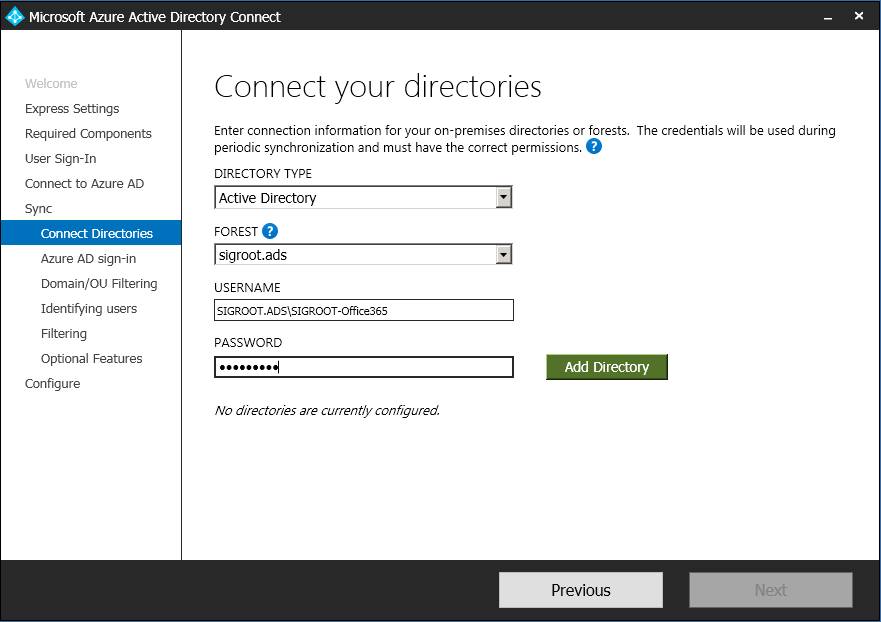
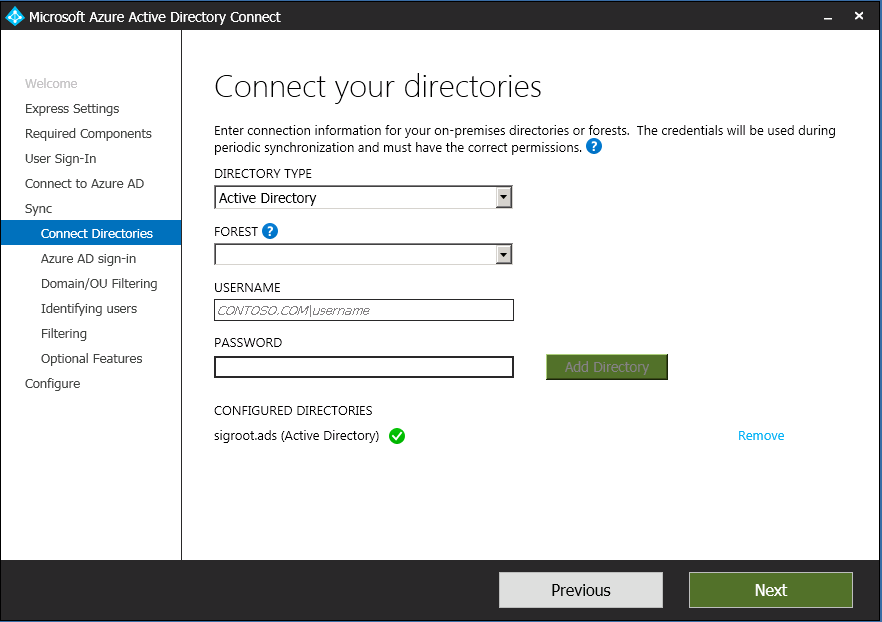
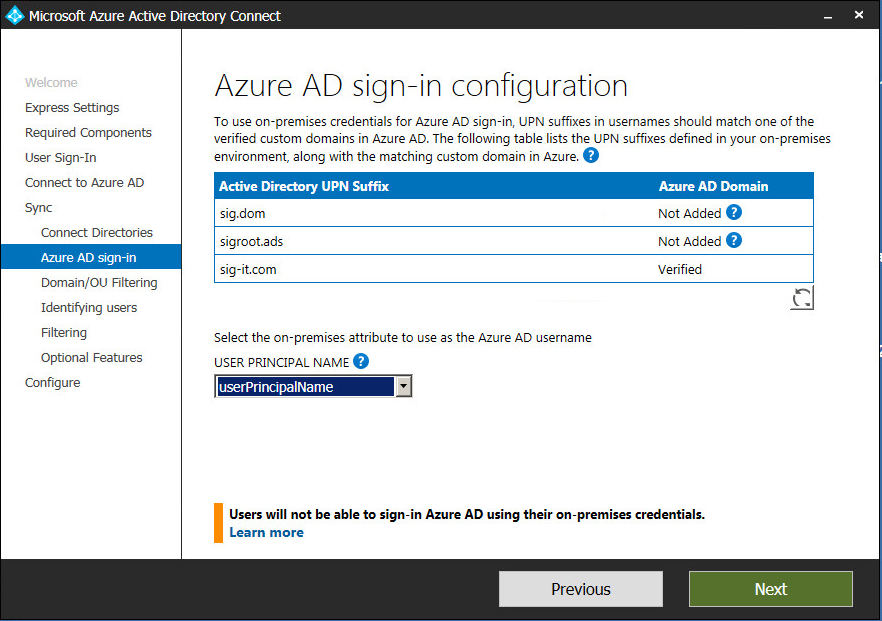
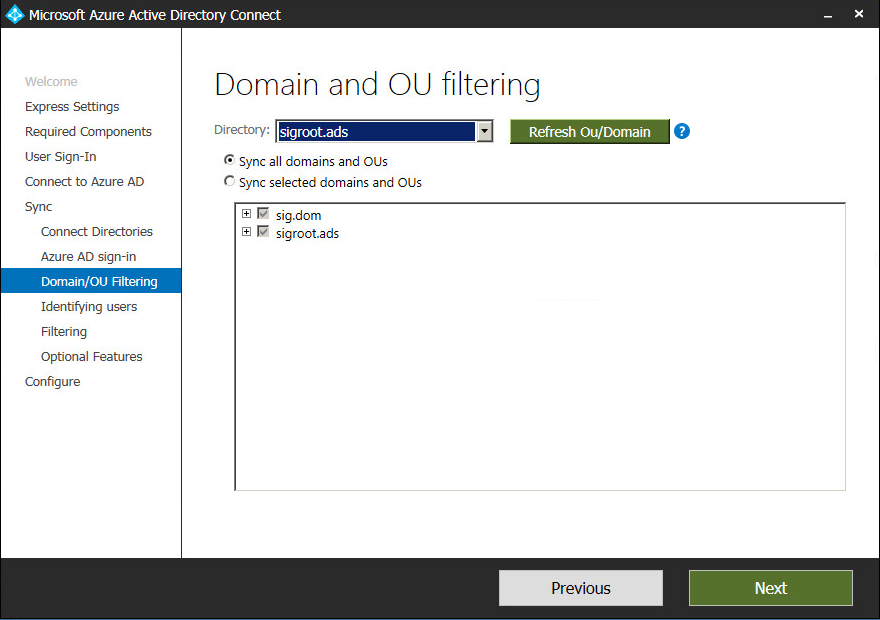
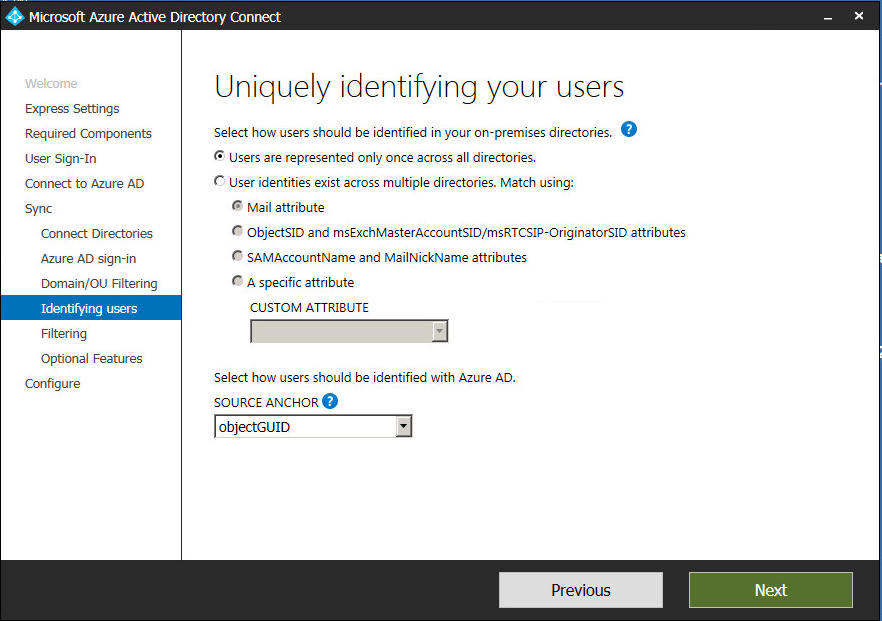
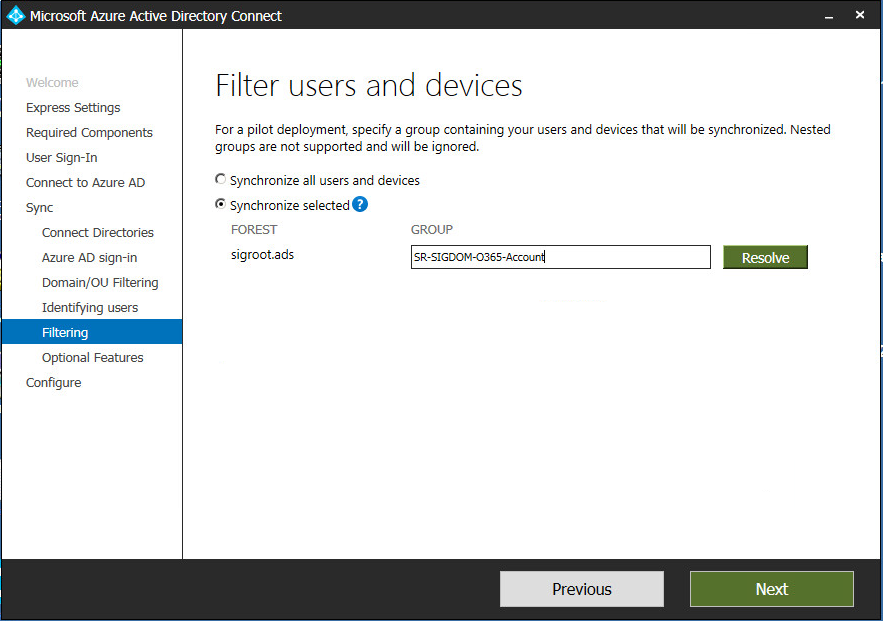
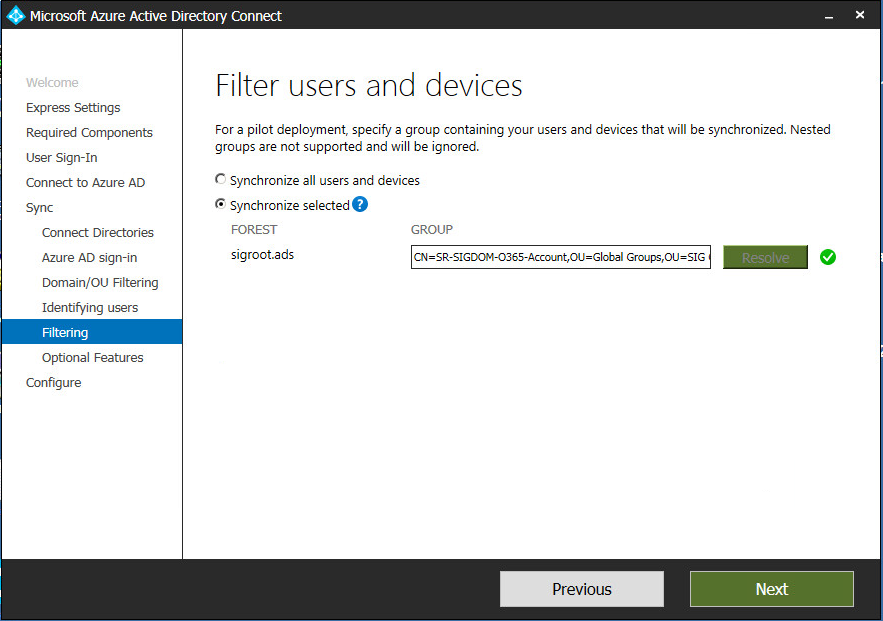
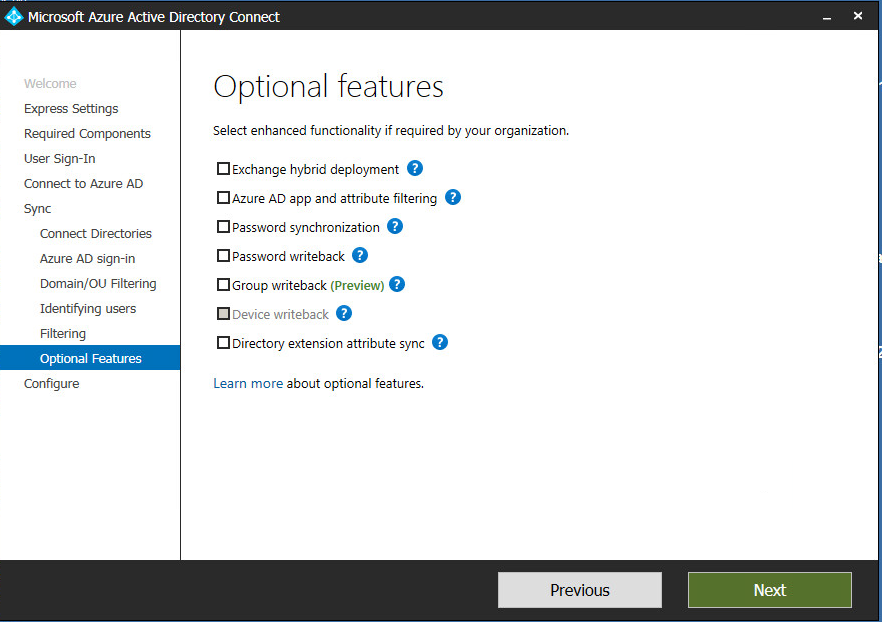
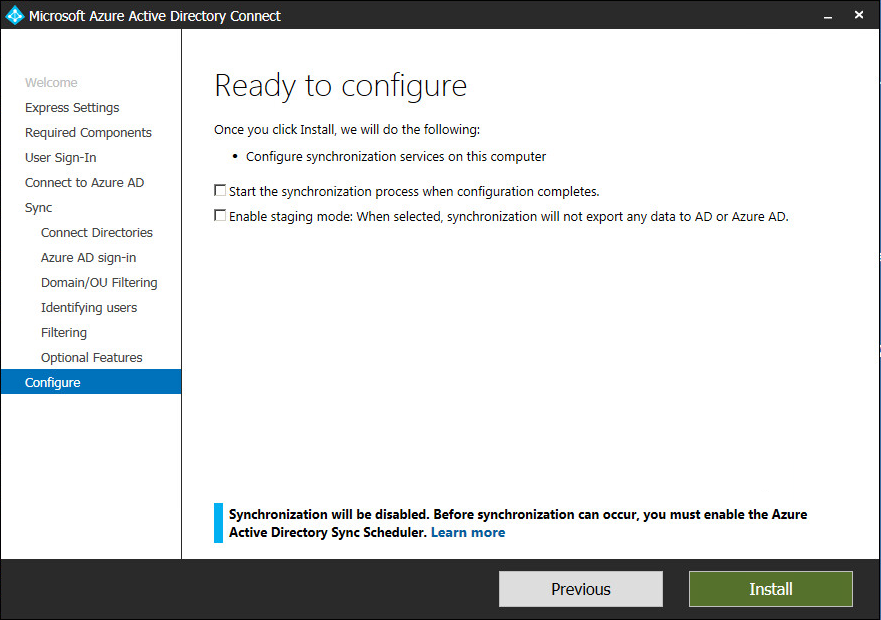
The purpose of this IT operations manual is to provide all necessary information for proper operation of the service / application.

The intended audience of the operating manual is the IT support organization (GUS / GITO).

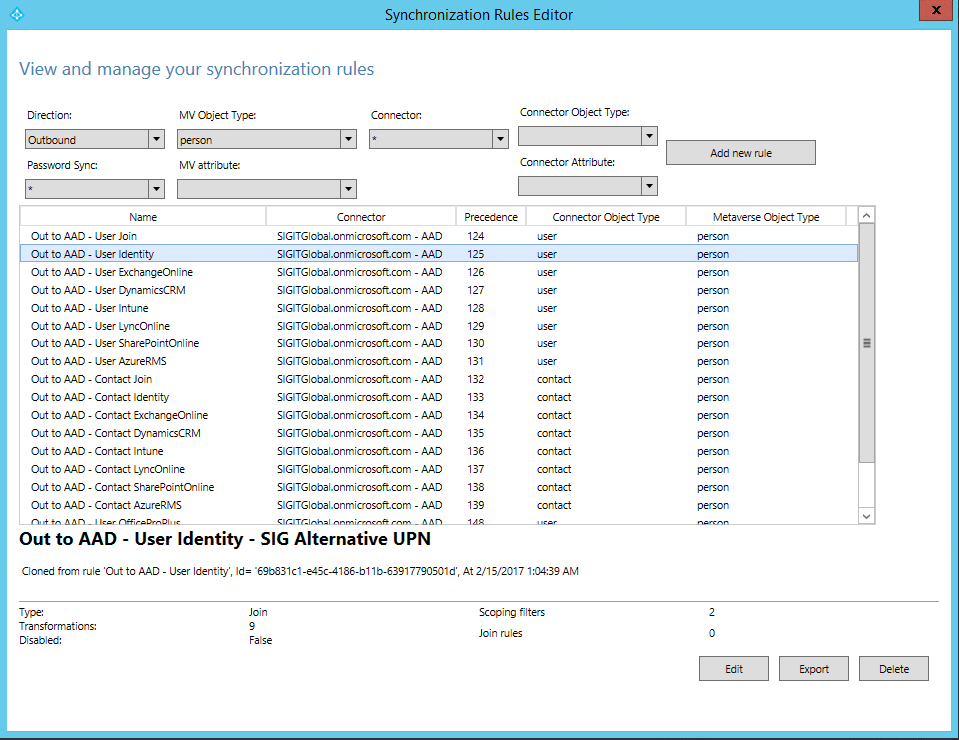
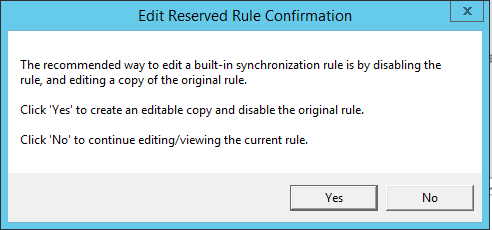
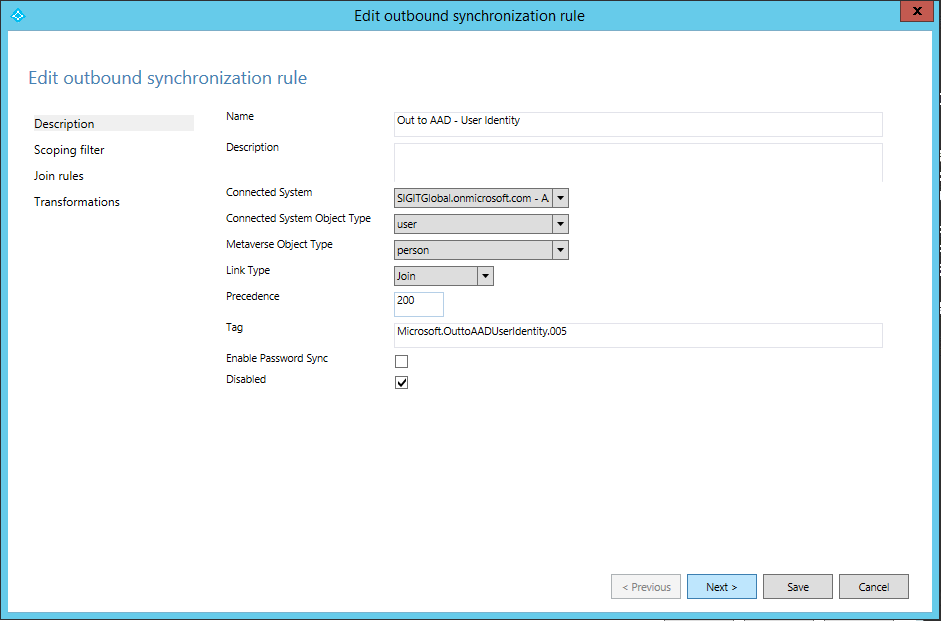
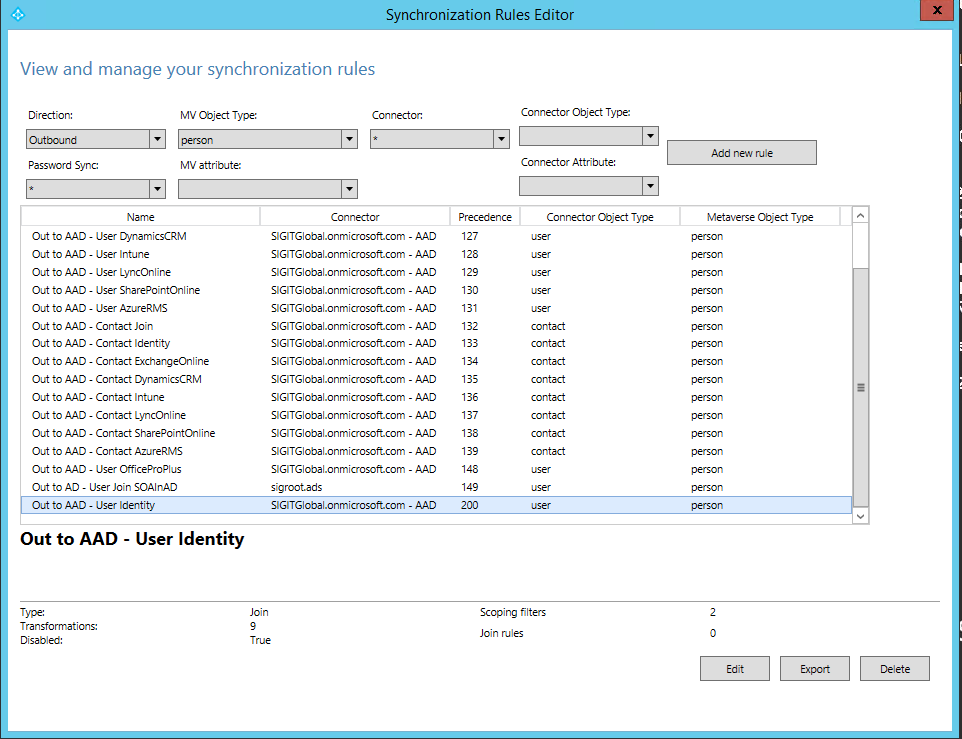
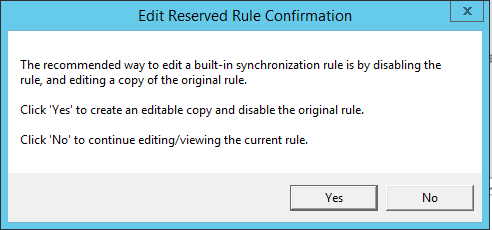
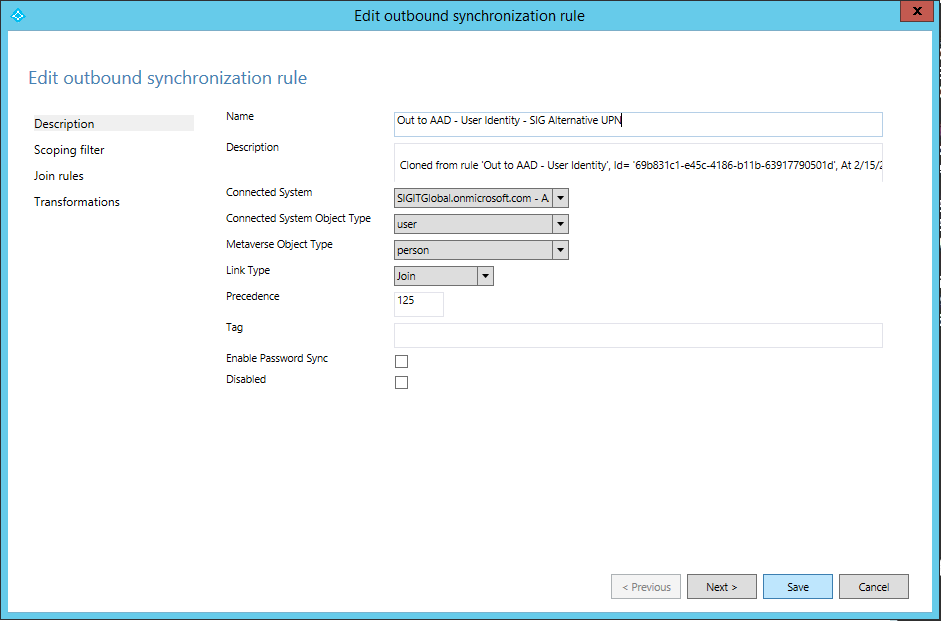
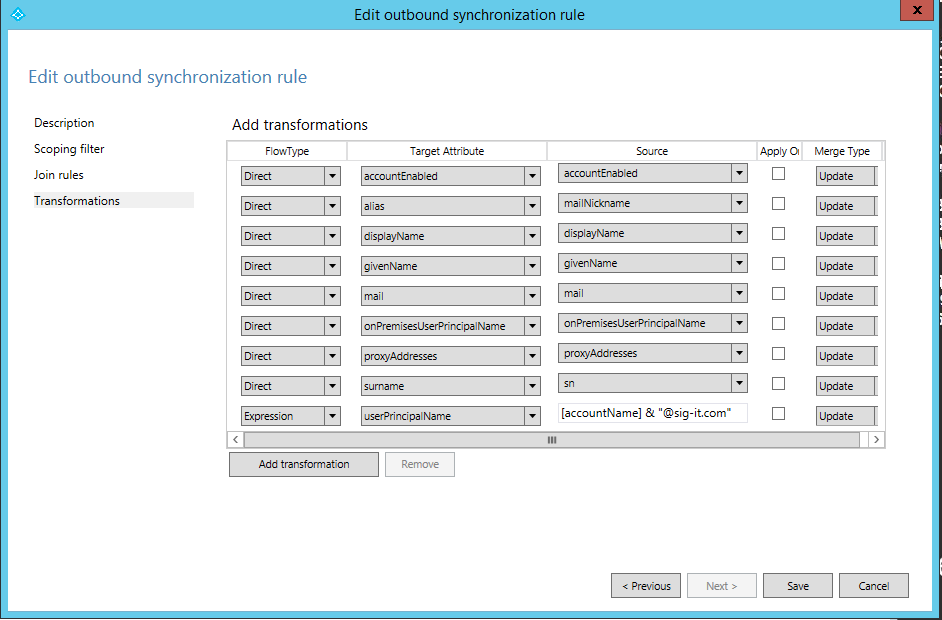
This document will contain information regarding the AZURE AD connection for the Office 365 SSO project.

# Installation

Put a mark on checkbox “I agree to the license terms and privacy notice” and click “Continue”:  


1. Click “Customize”:  
   
2. Keep all checkboxes clean and click “Install”:  
   
3. Set option “Do not configure” and click “Next”:  
   
4. Enter credentials of global Azure AD administrator account and click “Next”:  
   
5. Ensure that AD forest is correctly identified, enter credentials of pre-created AD user account which will be used by Azure AD Connect to connect to Active Directory and click “Add Directory”.  
   
6. After the forest is successfully queried and added, click “Next”:  
   
7. Review the list of domains, keep field “USER PRINCIPAL NAME” set to “userPrincipalName” and click “Next”:  
   
8. Keep option “Sync all domains and OUs” set and click “Next”:  
   
9. Keep option “Users are represented only once across all directories” set and field “SOURCE ANCHOR” set to “objectGUID” and click “Next”:  
   
10. Enable group filtering. Set option “Synchronize selected”, enter AD group name for Office 365 users and click “Resolve”:  
    
11. After group name is successfully resolved to group DN, click “Next”:  
    
12. Keep checkboxes of all optional features clean and click “Next”:  
    
13. Clear the checkbox “Start the synchronization process when configuration completes.” and click “Install”:  
    

# Post-installation configuration

1. Start “Synchronization Rules Editor”. Set display filter to “Direction” = “Outbound” and “MV Object Type” = “person”. Locate rule called “Out to AAD – User Identity” and note its precedence number (here - 125). Select the rule and click “Edit”:  
   
2. When prompted to create editable rule copy or edit or view the current rule, click “No” to edit the current rule:  
   
3. Set rule precedence to 200 (or any other high enough value to move it to the bottom of the list), mark “Disabled” checkbox and click “Save”:  
   
4. Now select the same rule in the list again and press “Edit”:  
   
5. When prompted, click “Yes” to create an editable rule copy:  
   
6. On “Description” page enter rule name “Out to AAD – User Identity – SIG Alternative UPN”, enter “Precedence” value of the original rule (here – 125), clear checkbox “Disabled”:  
   
7. On “Transformations” page locate transformation rule with target attribute “userPrincipalName”. Change its flow type to “Expression” and in field “Source” enter expression “[accountName] & "@sig-it.com"”. Then click “Save”:  
   

# Miscelaneous

## Generating or importing certificates

This configuration requires two different certificates (one to sign the SAML assertion, and the other to be used by external users to connect to ldp)

System🡪File Management🡪SSL Certificate List

Here we can use either **Import** or **Create** for the SAML certificate.

For the SSL certificate we will have to take the same steps.

System🡪File Management🡪SSL Certificate List🡪Import🡪Import type

## Download and import Office 365 iApp template

1. Download iApp file
2. In the BIG-IP web-based config Main🡪iApp🡪Templates🡪Import
3. Check Overwrite Existing Templates
4. Browse for the file and Upload.

## Configure iApp according to requirements

Configure iApp according to wizard propts.