MIM 2016 DEPLOYMENT AND CONGIGURATION GUIDE

1 ARCHITECTURE OVERVIEW

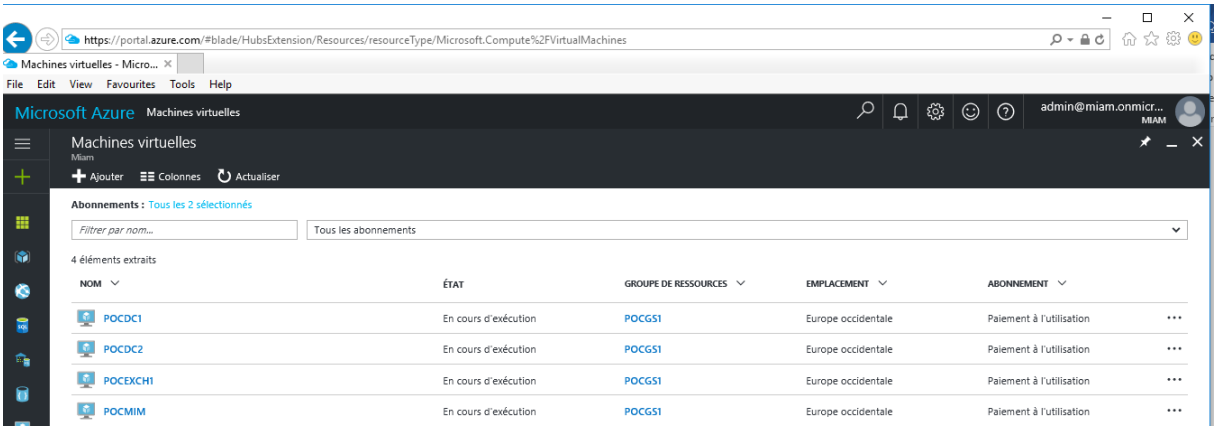
1.1 MIM 2016 / AZURE ACTIVE DIRECTORY COMPONENTS

MIM 2016 is a family of products.

Component	Description
MIM Synchronization Service (previously MIIS 2003, ILM 2007, FIM 2010)	This is the MIM 2016 synchronization engine.
MIM Service / MIM Portal	MIM Service is Windows service that provide MIM Portal with web APIs. MIM Portal is the SharePoint website. It allows: ➢ Configuration of MIM Service. ➢ User and groups management from Business teams via a customizable web interface. All the configuration is stored in a dedicated database.
BHOLD	This component provides access-based user roles, attestation, analytics and role reporting features. This component will not be deployed on this lab.
MIM Reporting	This component is based on SQL Server Reporting Services and Microsoft System Center Service Manager (SCSM). System Center 2012 Service Manager provides an integrated platform for automating and adapting your organization's IT service management best practices, such as those found in Microsoft Operations Framework (MOF) and Information Technology Infrastructure Library (ITIL). It provides built-in processes for incident and problem resolution, change control, and asset lifecycle management. MIM reporting will not be deployed in this lab.
MIM Certificate Management (previously named Certificate Lifecycle Manager - CLM)	This tool allows smart cards, user certificates and computer certificates management. Smart card is requested from MIM Certificate Management web interface. MIM Certificate Management includes workflows which allow to send email notifications. A modern app is available for MIM Certificate Management. This component will not be deployed in this lab.
Privilege Access Management (PAM)	This component allows to protect against vulnerabilities like *Pass the hash* attack. PAM allows to define group membership expiration for highly privileged group like Domain Admins. This component will not be deployed in this lab.
Azure Active Directory	The MIM 2016 Password Self-Service site will not be deployed because we will use *Azure Active Directory Premium* feature to perform this task.

1.2 MIM 2016 SERVERS

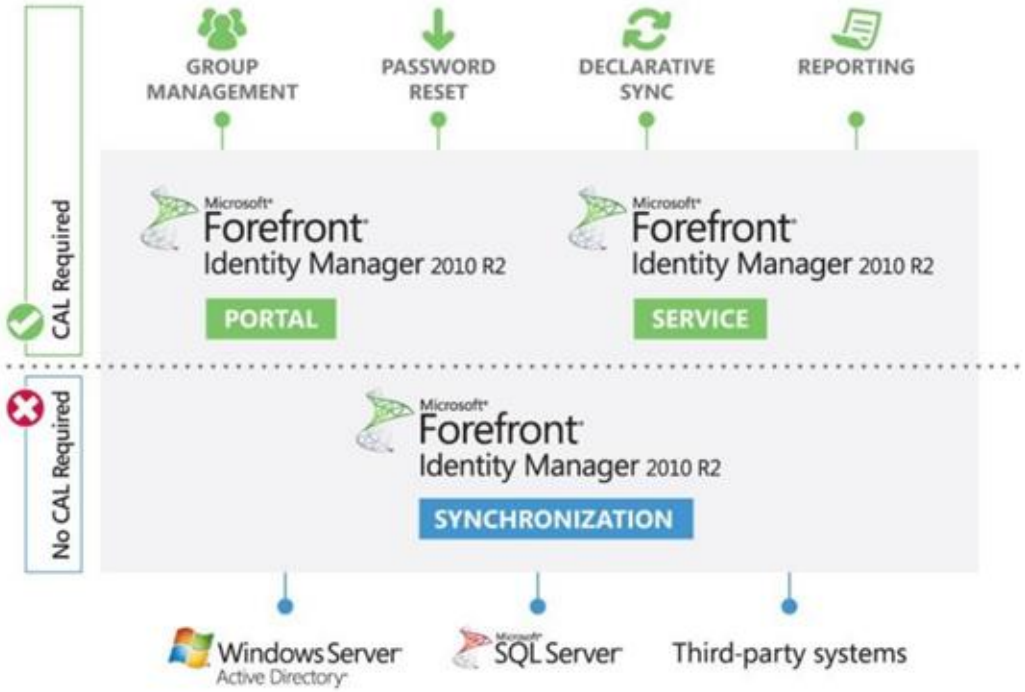
The lab environment will be created on Azure IaaS solution and will be based on 4 servers.



The following tables describes the lab environment.

Server	Configuration
POCDC1	Standard_A2_v2 (2 vCPU, 4 GB of memory, one 130 GB system disk) OS: Windows 2008 R2 Roles: domain controller (*POCMIAM.INTRA*) and Azure Active Directory Connect server. Remote access: RDP (pocdc1.westeurope.cloudapp.azure.com) Backup: every day at 3 AM.
POCDC2	Standard_A2_v2 (2 vCPU, 4 GB of memory, one 130 GB system disk) OS: Windows 2008 R2 Role: domain controller (*CHILD.POCMIAM.INTRA*) Remote access: RDP (*pocdc2.westeurope.cloudapp.azure.com*) Backup: every day at 3 AM.
POCEXCH1	Standard_A2_v2 (2 vCPU, 4 GB of memory, one 130 GB system disk) OS: Windows 2012 R2 Role: Exchange 2013 server SP1 Remote access: RDP (*pocexch1.westeurope.cloudapp.azure.com*) Backup: every day at 3 AM.
POCMIM	Standard DS11 v2 (2 vCPU, 14 GB of memory, one 130 GB SSD system disk) OS: Windows 2012 R2 Standard Roles: SQL Server 2012 SP2 SP3 (MIM), MIM 2016 Synchronization Services, MIM 2016 Services, SharePoint 2013 portal, Visual Studio 2015 U3. Remote access: RDP (*pocmim.westeurope.cloudapp.azure.com*) Backup: every day at 3 AM.

1.3 MIM 2016 LICENSING



Microsoft has completely change MIM 2016 license model since April 2015.

Windows Server license includes Microsoft Identity Manager 2006 server license.

After 1st of April 2015:

- Windows Server license (Standard & Datacenter) will include FIM server entitlement
- FIM Server 2010 R2 licenses will not be available anymore on the price lists

The FIM server will no longer be sold as a separate license, but instead Windows Server licenses will allow customers to install the FIM Server software.

An *Azure Active Directory Premium P1* or *P2* license is required for each user which is managed via MIM portal / service or MIM Certificate Management.
If you only use MIM Synchronization Service, no *Azure Active Directory Premium* license is required.
Enterprise Mobility Suite (EMS) or Enterprise Cloud Suite (ECS) plans include *Azure Active Directory Premium* license component.

If the FIM Portal, Service, or Certificate Management component is going to be deployed, a FIM CAL is required for each user which is managed by FIM. If you will *only* be using the FIM Sync Service, CALs are not required.

If you use MIM 2016 to manage external users, an external connector license is required (price divided by 1000).

Summary

- a server license is needed for each server on which FIM components are installed
- you need a CAL for each user for whom the software issues or manages identity information. (inlc. smart card & digital certs)
- a CAL is required for a administrator using FIM portal & services.

BUT

- no CAL is needed if you only use the sync service
- no device CALs needed

AND

- Under SA you are allowed to install one cold-standby server with the same license
- you can use ILM 2007 with your FIM license

MIM Portal requires to deploy a SharePoint Server farm. MIM 2016 license doesn't include SharePoint Server license. SharePoint 2016 foundation no longer exists. To avoid use of SharePoint Server 2013 licenses, it's required to deploy SharePoint Server 2013 Foundation.

You could use Office 365 E3 / E1 licenses which includes a SharePoint client access license to deploy SharePoint 2016.

MIM includes license for System Center Service Manager (*MIM 2016* reporting feature).

More information:
https://technet.microsoft.com/en-us/library/mt346112(v=office.16).aspx
http://social.technet.microsoft.com/wiki/contents/articles/2487.how-to-license-fim-2010-and-mim-2016.aspx
http://www.interlink.com/blog/entry/what-is-microsoft-s-enterprise-cloud-suite-ecs-1

1.4 SQL SERVER CONFIGURATION

Performance on MIM 2016 solution is relying to SQL Server performance.

System Center Service Manager Management Server doesn't support SQL Server 2014. That's why SQL Server 2012 will be used for all SQL servers (one SQL Server version) for the POC environment.

System Center Service Manager (Management Server and Data Wharehouse) require a supported collation type (*Latin1_General_100_CI_AS)* to allow multi languages support.
https://blogs.technet.microsoft.com/servicemanager/2012/05/24/clarification-on-sql-server-collation-requirements-for-system-center-2012/

That's why all SQL servers will use this collation (*Latin1_General_100_CI_AS).*

SQL server 2012 SP2 will be installed on POCMIM (instance MIM) with *database engine*, *full-text search components.*

MIM Synchronization Service (Forefront Identity Manager 2010 R2) has better performance when collocating service and database.

You must perform these actions on SQL server to obtain best performance:

- On the left, click Memory and change the Maximum server memory (in MB) value to 4096. This will limit the amount of memory allocated to this SQL Server Instance and reduce the risk to have the operating system competing with SQL Server for memory resources.
- On the left, click Database Settings and check the Compress Backup box.
- On the left, click Advanced, look at the value of Max Degree of Parallelism. It should be set to 1.

When SQL Server runs on a computer with more than one microprocessor or CPU, it detects the best degree of parallelism, that is, the number of processors employed to run a single statement, for each parallel plan execution. You can use the max degree of parallelism option to limit the number of processors to use in parallel plan execution. To enable the server to determine the maximum degree of parallelism, set this option to 0, the default value. Setting maximum degree of parallelism to 0 allows SQL Server to use all the available processors up to 64 processors. To suppress parallel plan generation, set max degree of parallelism to 1. Set the value to a number greater than 1 to restrict the maximum number of processors used by a single query execution. The maximum value for the degree of parallelism setting is controlled by the edition of SQL Server, CPU type, and operating system.

1.5 SHAREPOINT ARCHITECTURE

SharePoint 2013 Foundation will be used for the POC because:

- MIM license doesn't include SharePoint Server license.

- SharePoint 2016 foundation is not available: https://technet.microsoft.com/en-us/library/mt346112(v=office.16).aspx

SharePoint Foundation will be configured to use a *POCMIM\MIM*.
Indexing in the SharePoint Server will be disabled to gain performance.

1.6 MIM SYNCHRONIZATION SERVICE AND MIM SERVICE SCHEMA

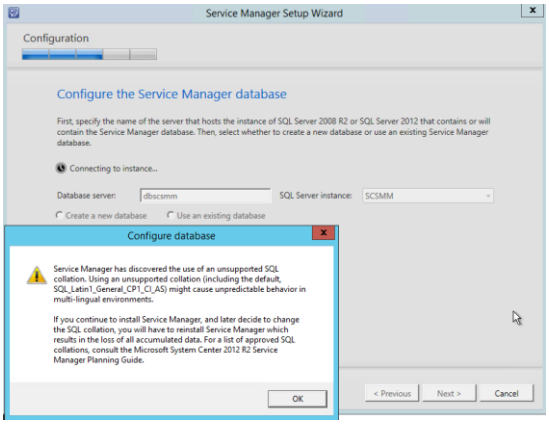
The schema of MIM Services and MIM Synchronization Services will be updated to add attributes like *Global_ID, Domain, HomeMdb, MsExchHomeServer* to the class *Person*.

The *EmployeeType* attribute will be updated to allow only the values: *Internal, External*.
http://bit.ly/MIMServiceSchema
http://aka.ms/FIMServiceSchema

The company attribute will be a drop-down list.

1.7 MIM REPORT

MIM 2016 report is based on System Center Service Manager Management Server, System Center Service Manager Data Warehouse and SQL Server reporting Services. System Center Service Manager Management Server and System Center Service Manager Data Warehouse could not be deployed on the same server. The collation of System Center Service Manager databases must be *Latin1_General_100_CI_AS* as explained here:
https://technet.microsoft.com/en-us/library/gg429478.aspx
https://blogs.technet.microsoft.com/servicemanager/2012/05/24/clarification-on-sql-server-collation-requirements-for-system-center-2012/



MIM report will not be deployed on this lab.

1.8 SERVICE ACCOUNT

The following user account will be created in Active Directory

User	Description
svc-sql	This account starts SQL Server service (database and agent services).
svc-mimsync	This account starts MIM Synchronization Service
svc-mimservice	This account starts MIM Service
svc-mimsps	MIM SharePoint configuration account
svc-mimspspool	MIM SharePoint Server pool account.
svc-mimma	This user account is used for MIM Synchronization Services connectors
svc-miminstall	User account for all administrative tasks.
svc-scsmwf	System Center Service Manager mail-enabled user to use for workflow.
svc-scsmrep	System Center Service Manager reporting and analysis service account.
svc-scsm	Service account to start System Center Service Manager services.
svc-adma	Service account used by MIM Synchronization Service Active Directory Connector to connect to Active Directory. This account has right to create, update and delete users, groups, contacts on POCMIAM OU.
svc-sqlma	Service account used by MIM Synchronization Service SQL Server Connector to connect to Active Directory. This account is DBOWNER on HR database.

The following groups will be created:

- FIMSyncAdmins (members: *svc-miminstall*, *svc-mimservice* and *svc-miminstall*)
- FimSyncOperators
- FIMSyncJoiners
- FIMSyncBrowse
- FIMSyncPasswordSet
- SCSM-Admins (members: *svc-miminstall*, *svc-scsmwf*, *svc-scsmrep*, *svc-scsm*)

1.9 PASSWORD SELF-SERVICE FEATURES

The MIM 2016 Password Self-Service site will not be deployed because we use *Azure Active Directory Premium* to perform this task.

1.10 MIM CERTIFICATE MANAGEMENT

MIM certificate Management will not be deployed on this lab.

1.11 BHOLD

BHOLD will not be deployed on this lab.

1.12 LANGUAGE PACK

MIM language pack will not be deployed on this lab.
Pay attention of the type of the collation for report features (SCSM)
https://technet.microsoft.com/en-us/library/gg429478.aspx

The architecture has been defined based of the following guide:
MIM capacity Planning Guide (http://bit.ly/MIMCapacityPlanning)
MIM compatibility matrix (https://docs.microsoft.com/en-us/microsoft-identity-manager/plan-design/microsoft-identity-manager-2016-supported-platforms).
https://docs.microsoft.com/en-us/microsoft-identity-manager/plan-design/microsoft-identity-manager-2016-supported-platforms
http://blog.ilmbestpractices.com/

1.13 NETWORK FLOWS

MIM Service listens on port *TCP 5725* by default.
The following item describes all System Center Service Manager network flows:
http://aka.ms/SCSM2010Ports
Windows firewall has been disabled to make the lab easier to deploy.

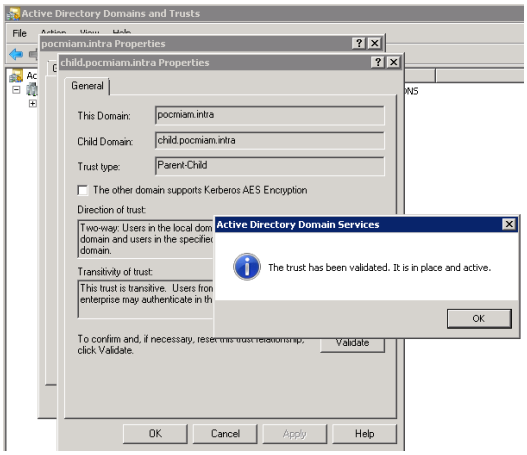
2 INSTALLATION STEP BY STEP

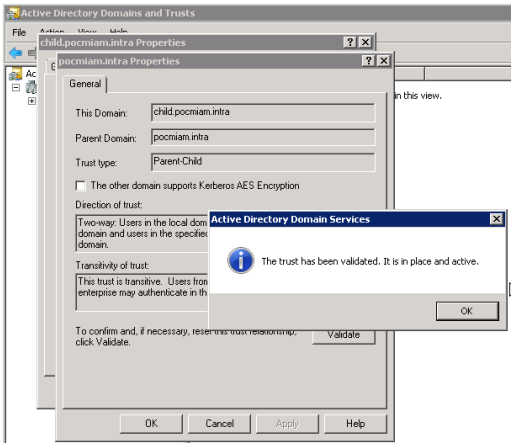
2.1 DEPLOY THE ACTIVE DIRECTORY FOREST

Apply this guide to create domain controller in Azure IaaS.
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-new-forest-virtual-machine

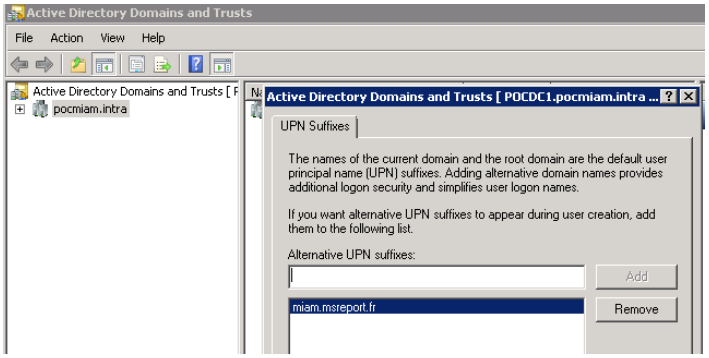
We will create a forest with 2 domains.

After promotion of the child domain, you need to reset the password of the trust between the 2 domains.
NETDOM TRUST child.pocmiam.intra /Domain:pocmiam.intra /UserD:child\gmathieu /PasswordD:XXXXX /UserO:pocmiam\gmathieu /PasswordO:XXXX /Reset /TwoWay





You also need to create the UPN Suffix *miam.msreport.fr*.

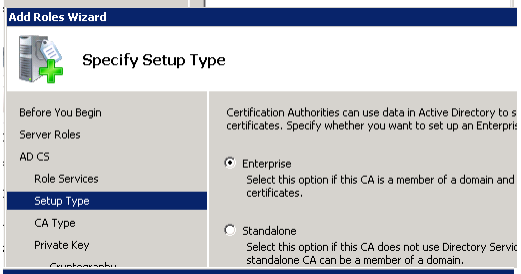


Create 3 OU at the root of the domain. In this lab we have three entities.
In each OU, create a sub OU named *Users, Disabled_Users, Groups*.
Perform this tasks in the 2 domains.

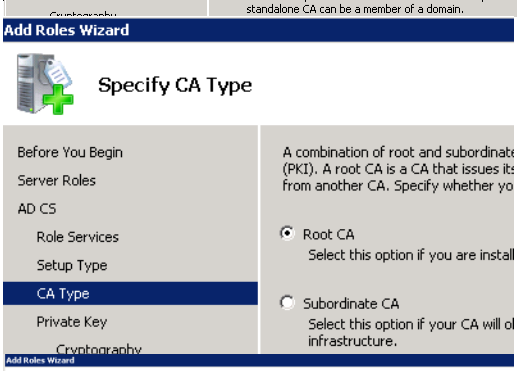
2.2 CREATE A ROOT PUBLIC KEY AUTHORITY

A PKI has been created on POCDC1 to generate a proper Exchange (SAN) certificate for POCEXCH1.

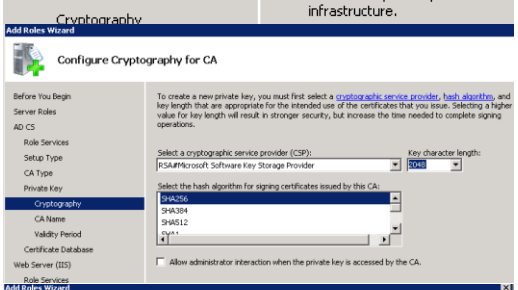
Select *Certification Authority* and *Certification Authority Web Enrollment*.



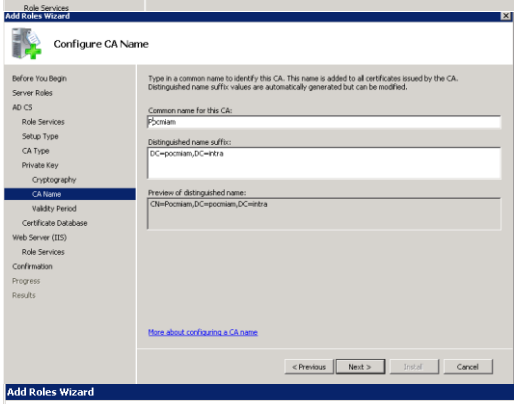
Select *Enterprise*.



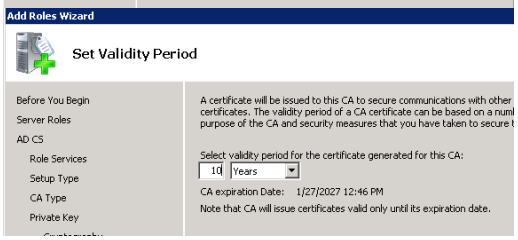
Select *Root CA*.



Select *SHA256* (instead of *SHA1*).

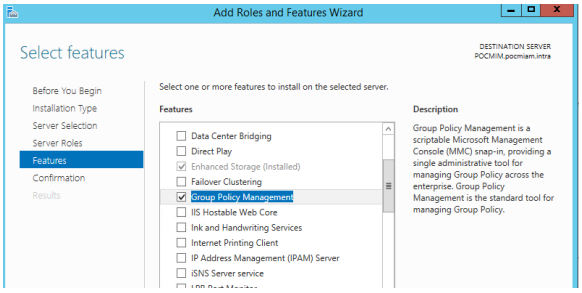


Enter *Pocmiam*.

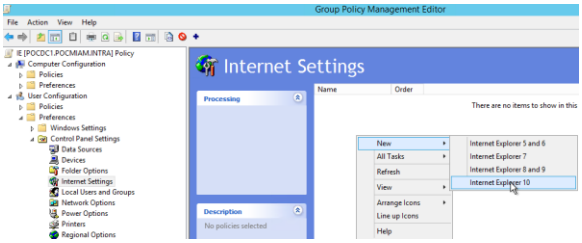


Perform a default installation and click on *Finish*.

2.3 CONFIGURE INTERNET EXPLORER BY GPO

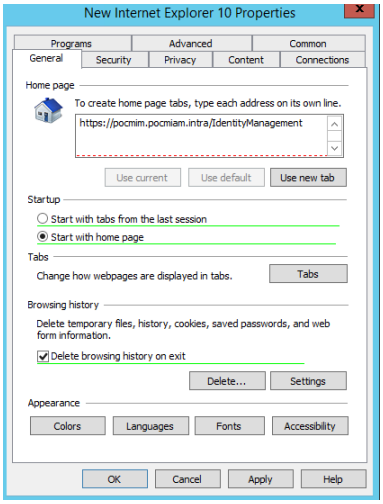


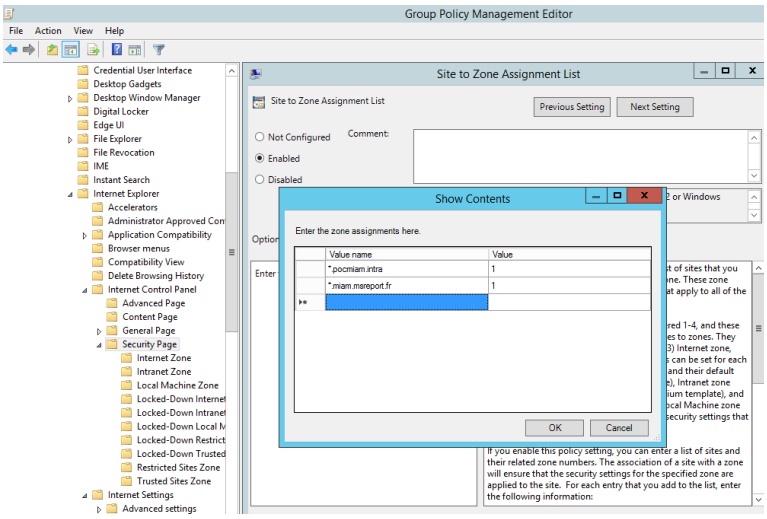
Install GPMC on POCMIM.

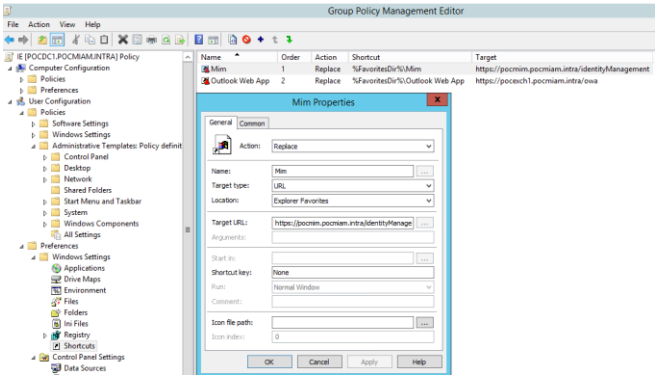


Start GPMC with an account member of the group *Enterprise Admins*.

Configure Internet Explorer default URL, favorites and local Intranet zone.
https://blogs.msdn.microsoft.com/askie/2012/06/05/how-to-configure-internet-explorer-security-zone-sites-using-group-polices/
https://blogs.msdn.microsoft.com/asiatech/2014/12/16/how-to-apply-favorites-links-to-ie10ie11-in-gpo-without-iem/

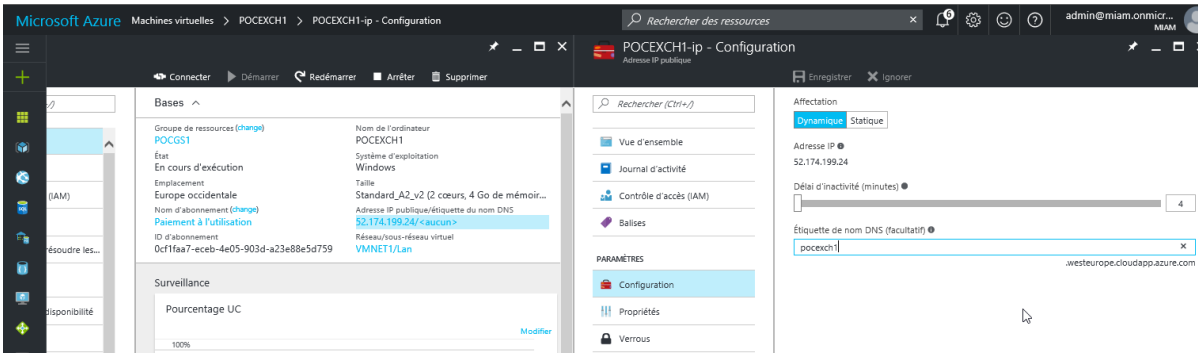


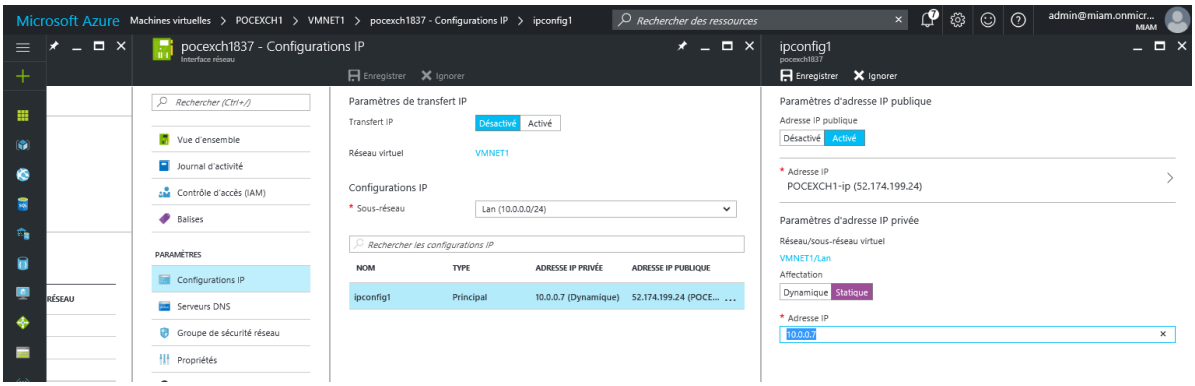




2.4 INSTALL POCEXCH1

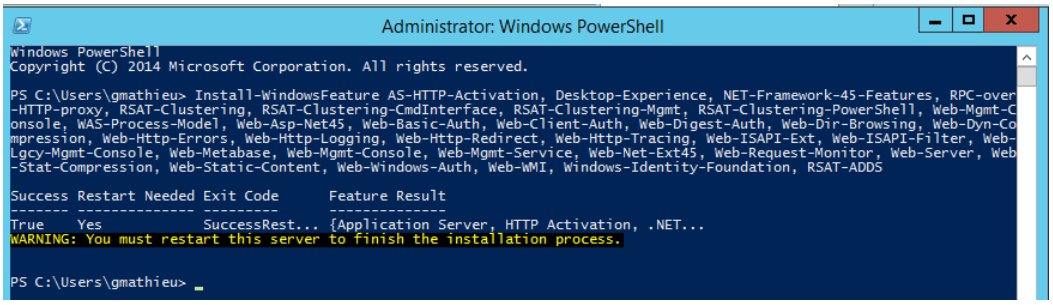
Configure a static private IP in Azure IaaS for the Exchange server.
Configure a DNS alias for dynamic public IP. This allows to connect via *MSTSC* (RDP): *pocexch1.westeurope.cloudapp.azure.com*





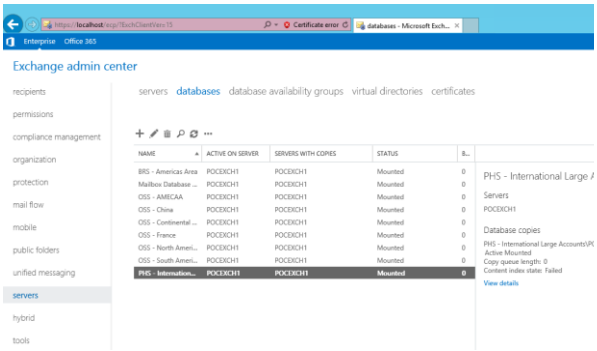
Prepare the server to deploy Exchange 2013
https://technet.microsoft.com/en-us/library/bb691354(v=exchg.150).aspx

Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS



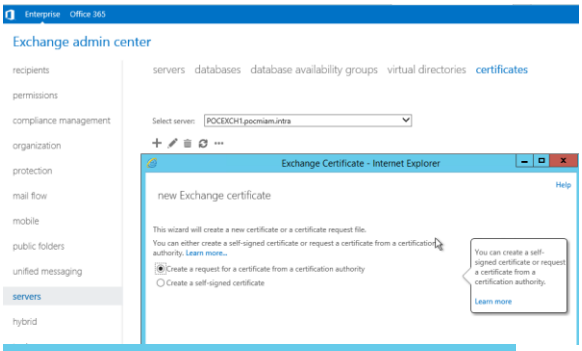
Install the required hotfixes: https://support.microsoft.com/en-gb/help/3146715/hotfix-rollup-3146715-for-the-.net-framework-4.6-and-4.6.1-in-windows

Install Unified Communications Managed API 4.0 Runtime
https://technet.microsoft.com/en-us/library/bb691354(v=exchg.150).aspx

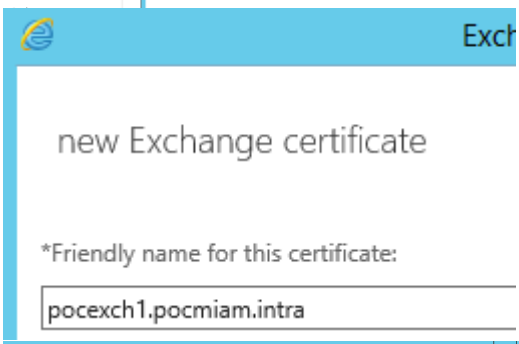


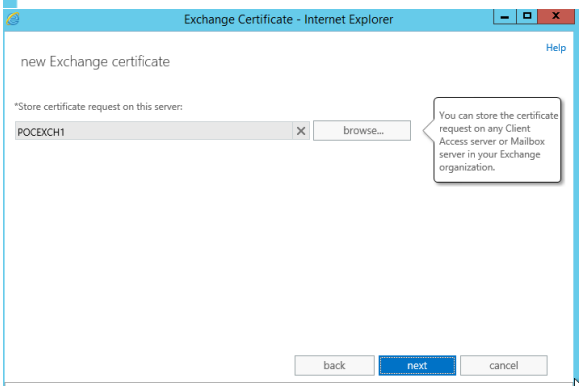
Create one database for each entity. Use the same name than the company name.

Install the Exchange 2013 Enterprise license.

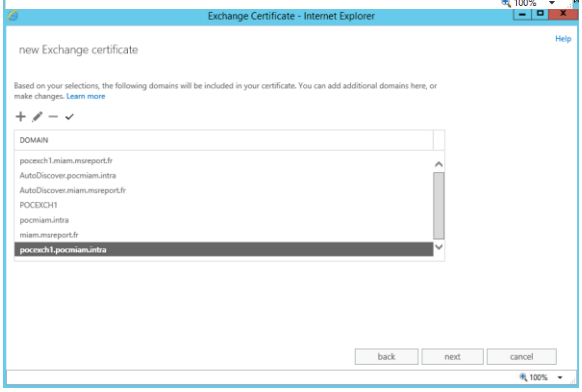


Generate Exchange 2013 certificate.

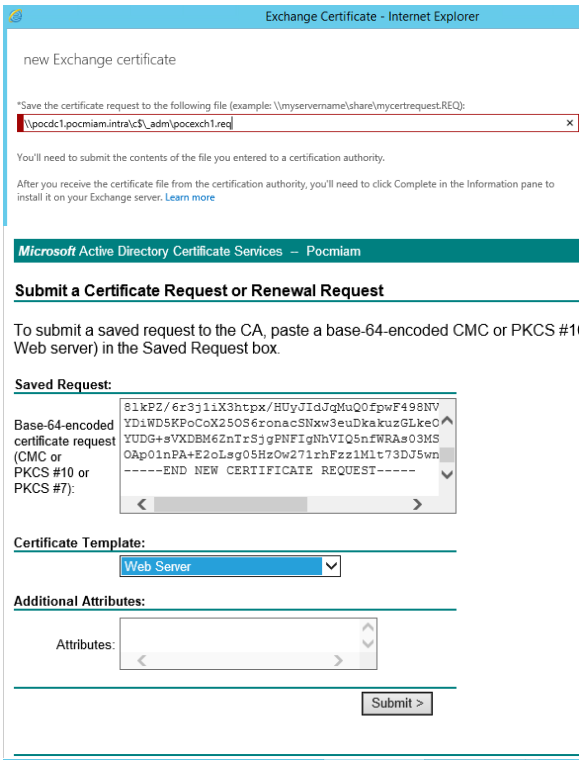




Click on *Next*.

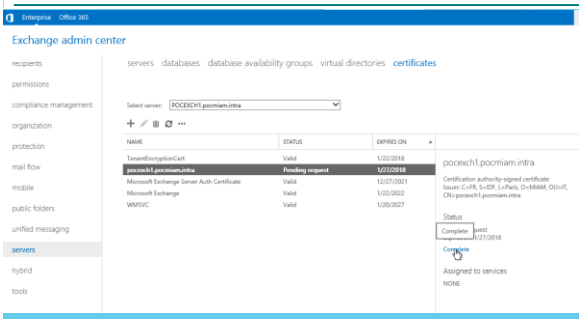


Click on *Next*.

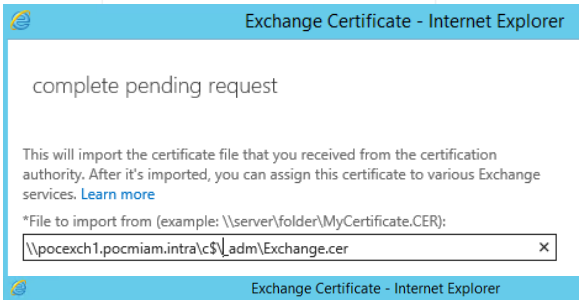


Use a local shared folder to store the request.

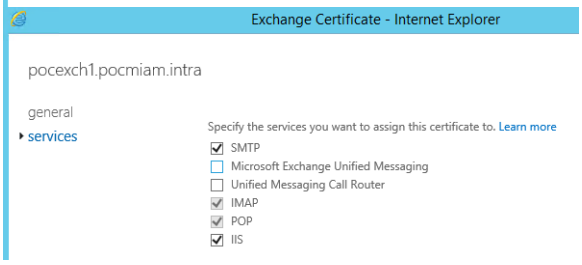
Click on *Submit* button.



Click on *Complete* link to install the new certificate.



Use a local shared folder.



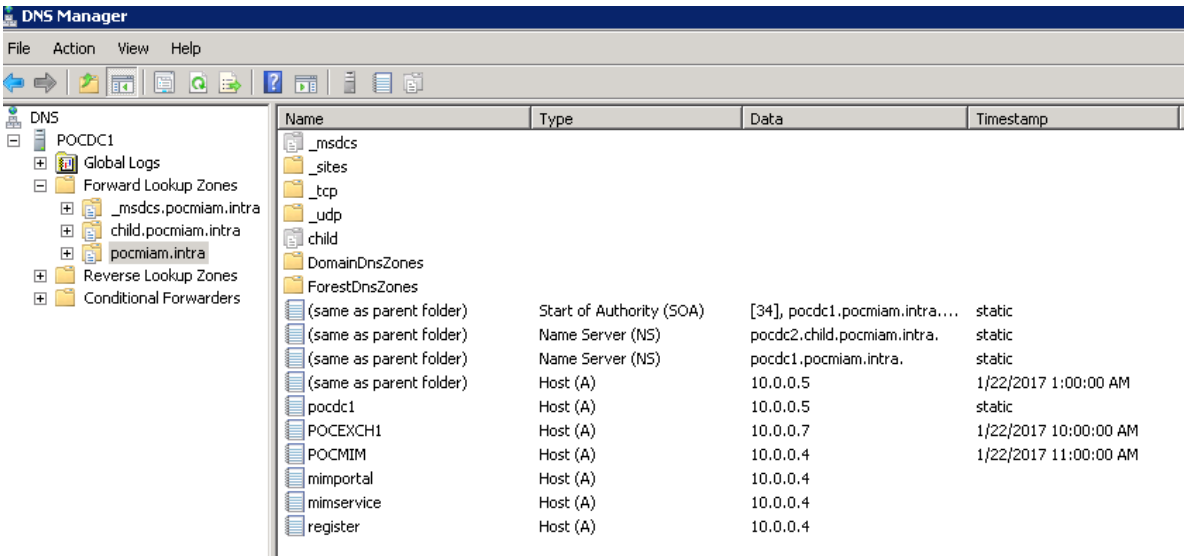
Assign all Exchange 2013 services to the new Exchange certificate.

Create an Exchange mailbox for *svc-adma* and add this user in the group *Organization Management*.
Also create an Exchange mailbox for *svc-mimservice*.

2.5 PREPARE THE ENVIRONMENT (DNS, SERVICE ACCOUNT AND PREPARE POCMIM)

The following procedure is based on the items:
https://docs.microsoft.com/fr-fr/microsoft-identity-manager/deploy-use/preparing-domain
https://docs.microsoft.com/fr-fr/microsoft-identity-manager/deploy-use/prepare-server-ws2012r2

Create DNS entries (10.0.0.4).
mimportal.pocmiam.intra
mimservice.pocmiam.intra
register.pocmiam.intra



Create all services accounts.
Start PowerShell and enter the following commands:

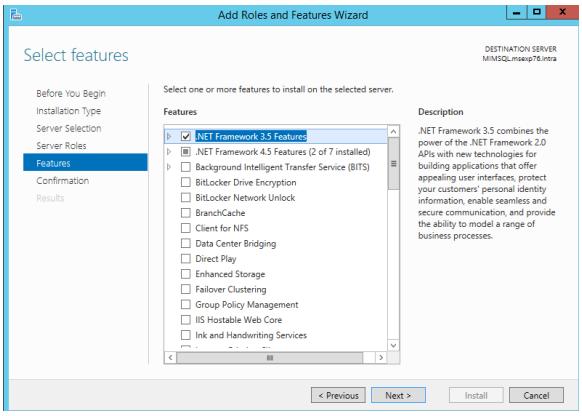
```
import-module activedirectory
$sp = ConvertTo-SecureString "!!!!YOURPASSWORD!!!!" -asplaintext -force
New-ADUser -SamAccountName svc-mimma -name svc-mimma
Set-ADAccountPassword -identity svc-mimma -NewPassword $sp
Set-ADUser -identity svc-mimma -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-mimservice -name svc-mimservice
Set-ADAccountPassword -identity svc-mimservice  -NewPassword $sp
Set-ADUser -identity svc-mimservice  -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-mimsync -name svc-mimsync
Set-ADAccountPassword -identity svc-mimsync -NewPassword $sp
Set-ADUser -identity svc-mimsync -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-mimsps -name svc-mimsps
Set-ADAccountPassword -identity svc-mimsps -NewPassword $sp
Set-ADUser -identity svc-mimsps -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-sql -name svc-sql
Set-ADAccountPassword -identity svc-sql -NewPassword $sp
Set-ADUser -identity svc-sql -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-mimspspool -name svc-mimspspool
Set-ADAccountPassword -identity svc-mimspspool -NewPassword $sp
Set-ADUser -identity svc-mimspspool -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-miminstall -name svc-miminstall
Set-ADAccountPassword -identity svc-miminstall -NewPassword $sp
Set-ADUser -identity svc-miminstall -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-scsm -name svc-scsm
Set-ADAccountPassword -identity svc-scsm -NewPassword $sp
```

Set-ADUser -identity svc-scsm -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-scsmrep -name svc-scsmrep
Set-ADAccountPassword -identity svc-scsmrep -NewPassword $sp
Set-ADUser -identity svc-scsmrep -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-scsmwf -name svc-scsmwf
Set-ADAccountPassword -identity svc-scsmwf -NewPassword $sp
Set-ADUser -identity svc-scsmwf -Enabled 1 -PasswordNeverExpires 1
New-ADUser -SamAccountName svc-adma -name svc-adma
Set-ADAccountPassword -identity svc-adma -NewPassword $sp
Set-ADUser -identity svc-adma -Enabled 1 -PasswordNeverExpires 1

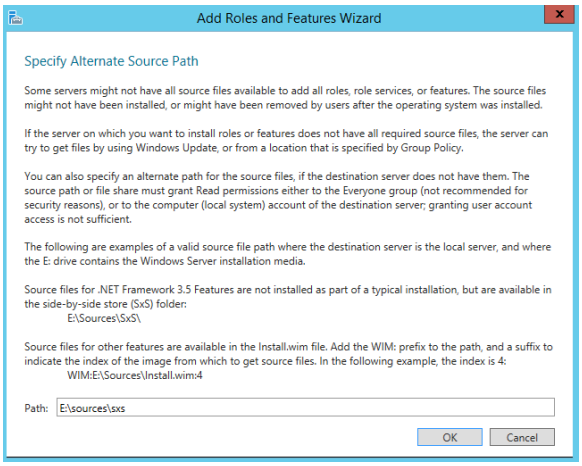
ServicePrincipalName must be created to enable Kerberos authentication.
setspn -S http/mimservice svc-mimservice
setspn -S http/mimservice.pocmiam.intra svc-mimservice
setspn -S fimservice/mimservice.pocmiam.intra pocmiam\svc-mimservice
setspn -S fimservice/mimservice pocmiam\svc-mimservice
setspn -S http/mimportal pocmiam\svc-mimspspool
setspn -S http/mimportal.pocmiam.intra pocmiam\svc-mimspspool

Create the groups below (global groups).
FIMSyncAdmins
FIMSyncBrowse
FIMSyncJoiners
FimSyncOperators
FIMSyncPasswordSet
SCSM-Admins

Add *svc-mimservice* as member of the group *FIMSyncPassword* (to enable *Password reset portal*).
Add *gmathieu*, *sa-mathieu*, *svc-mimservice* and *svc-miminstall* as members of the group *FIMSyncAdmins*.
Add *gmathieu*, *sa-mathieu*, *svc-miminstall*, *svc-scsmwf*, *svc-scsmrep*, *svc-scsm* as members of the group *SCSM-Admins*.

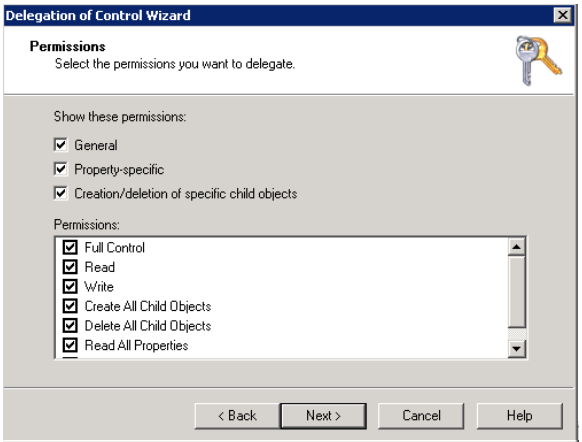


Install .Net Framework 3.5 on *POCMIM*.

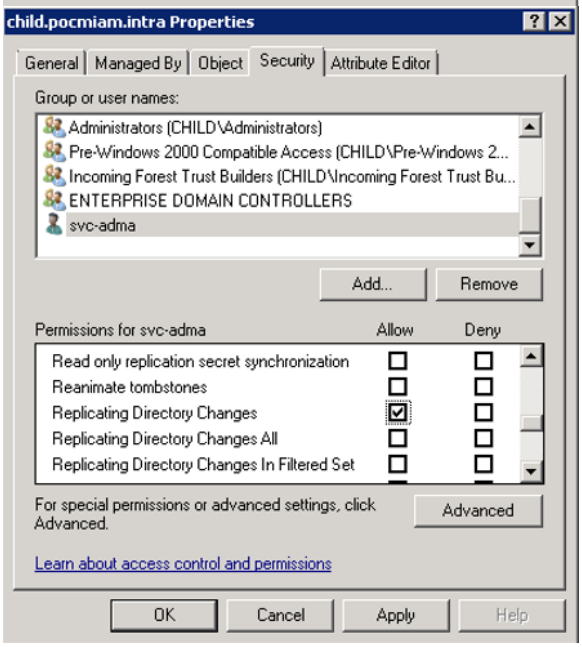


You need to specify the path to the *SXS* folder on Windows 2012 R2 installation drive (*E:\sources\sxs*).

You need also to delegate access on the domain *pocmiam.intra* and *child.pocmiam.intra* to the service account *pocmiam\svc-adma* on each OU (which contains non system objects).



Delegate the right to create, delete and users and groups in each OU.

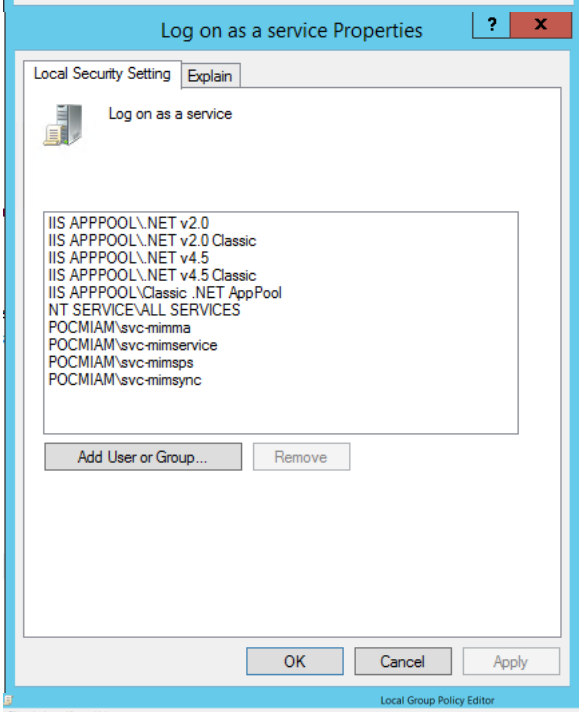


Delegate also to *pocmiam\svc-adma* the right *Replicate Directory Changes* at the domain level for *POCMIAM.INTRA* and *CHILD.POCMIAM.INTRA*. This is required to allow the MIM 2016 AD connector to perform delta sync: https://support.microsoft.com/en-us/kb/303972

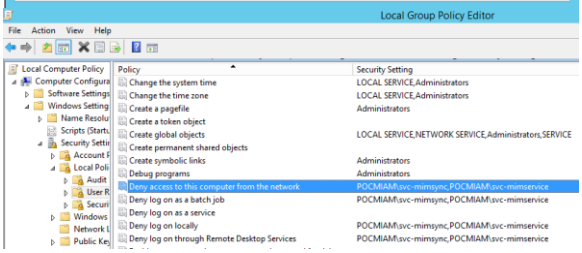
Add IIS roles and Active Directory PowerShell module on POCMIM.
import-module ServerManager
Install-WindowsFeature Web-WebServer,rsat-ad-powershell,Web-Mgmt-Tools,Application-Server,Windows-Identity-Foundation,Server-Media-Foundation,Xps-Viewer -includeallsubfeature -restart

Add *pocmiam\svc-sql*, *pocmiam\svc-mimsync*, *pocmiam\svc-mimservice, pocmiam\svc-mimsps* and *pocmiam\svc-miminstall* as members of the local administrators group on POCMIM.

Disable *Internet Explorer Enhanced Security Configuration* on all servers of the lab.
https://social.technet.microsoft.com/wiki/contents/articles/16682.fim-troubleshooting-synchronization-service-setup-is-having-trouble-contacting-sql-server.aspx

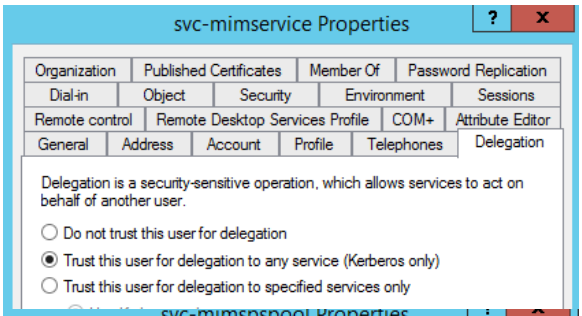


Reduce privilege of *svc-mimsync* and *svc-mimservice* on POCMIM.
Start *gpedit.msc*
Configure the setting *Log on as a service* for the users :
pocmiam\svc-mimsync
pocmiam\svc-mimservice
pocmiam\svc-mimma
pocmiam\svc-mimsps

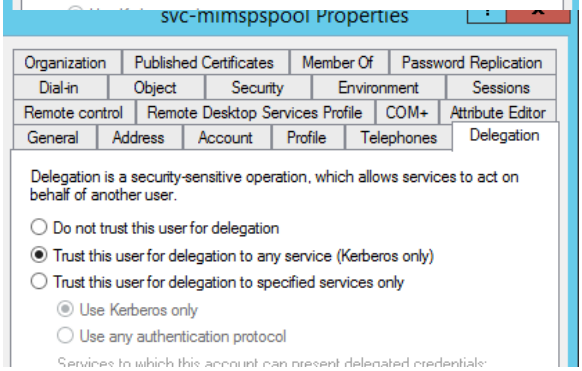


Configure the settings *Deny log on as a batch job*, *Deny log on locally, Deny logon through Remote Desktop Services* and *Deny access to this computer from the network* for the users:
pocmiam\svc-mimsync
pocmiam\svc-mimservice

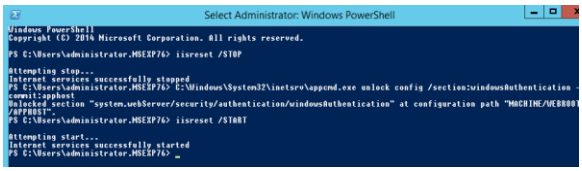
Enter *gpupdate /force* command.
https://docs.microsoft.com/fr-fr/microsoft-identity-manager/deploy-use/prepare-server-ws2012r2



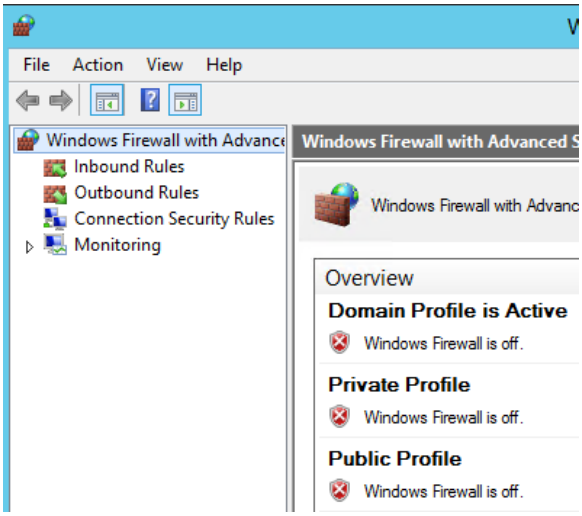
Configure *svc-mimservice* for Kerberos delegation.



Configure *svc-mimspspool* for Kerberos delegation.



Configure IIS on the server POCMIM.
iisreset /STOP
C:\Windows\System32\inetsrv\appcmd.exe unlock config /section:windowsAuthentication -commit:apphost
iisreset /START



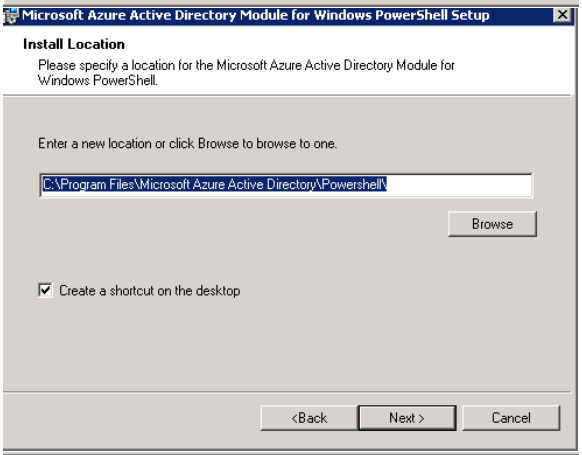
Disable Windows Firewall for the private, public and domain profils on all severs of the lab.

2.6 INSTALL AND CONFIGURE AZURE ACTIVE DIRECTORY CONNECT ON POCDC1

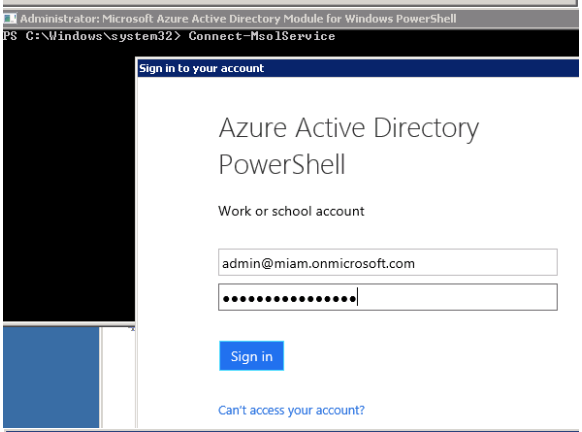
We will configure *Azure Active Directory Connect* tool to allow synchronization between Azure Active Directory and the Active Directory forest *POCMIAM.INTRA*.
This tool will also be used to replicate password from Azure Active Directory to Active Directory (Azure Active Directory Premium feature).

Install PowerShell V3 (Windows6.1-KB2506143-x64.msu).

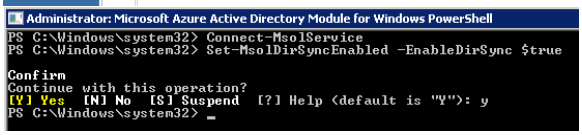
Install Azure Active PowerShell module.



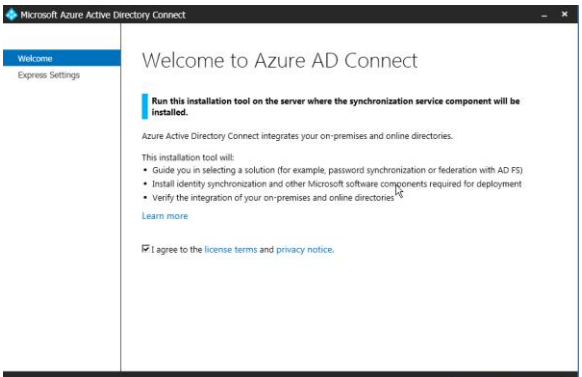
Click on *Next* then click on *Install*.



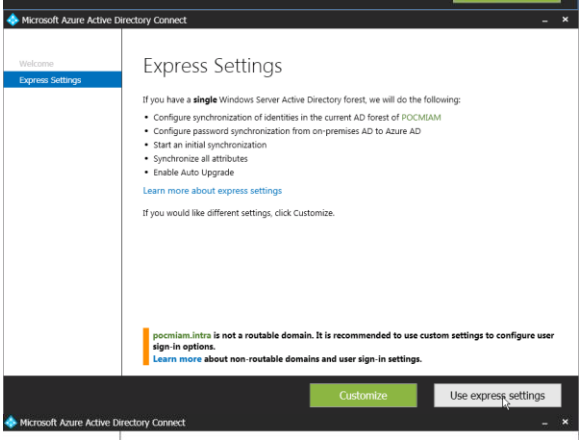
Start Azure Active Directory PowerShell module.
Enter the command:
Connect-MsolService
Connect to Azure Active Directory with the user *admin@miam.onmicrosoft.com*.



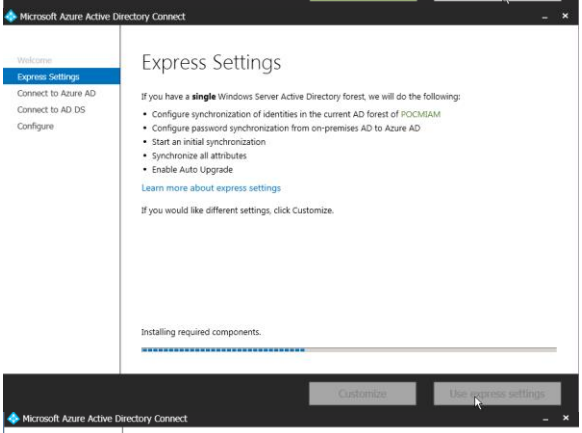
Enter this command to enable synchronization on Azure Active Directory.
Set-MsolDirSyncEnabled -EnableDirSync $true

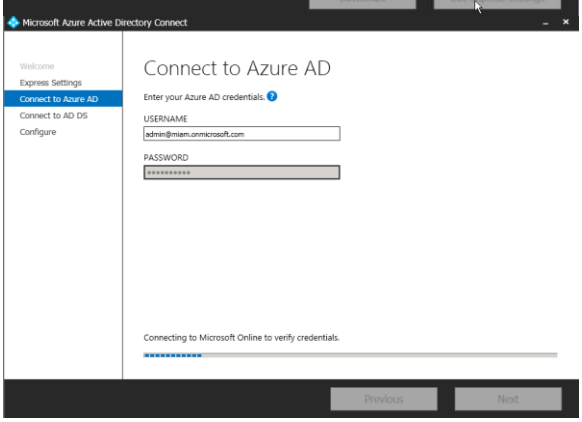


Download and start the installation of Azure Active Directory Connect: https://www.microsoft.com/en-us/download/details.aspx?id=47594

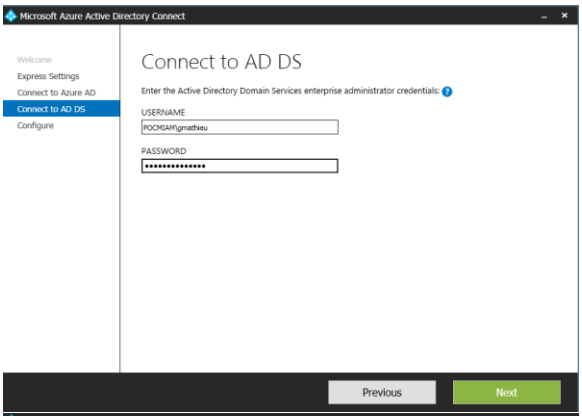


Use *Express Settings*.
This will deploy *SQL Server Express Local DB* automatically.

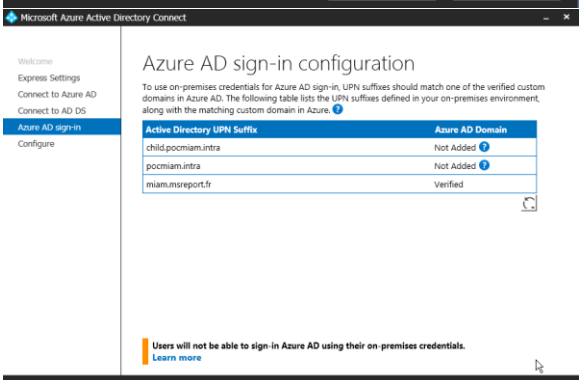




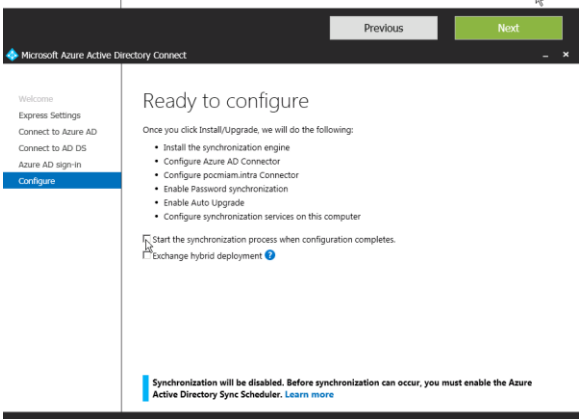
Username: *admin@miam.onmicrosoft.com*
Click on *Next*.



Username: *pocmiam\gmathieu*
Click on *Next*.

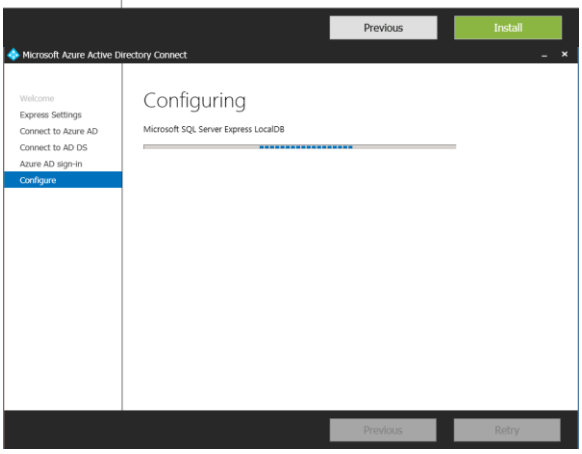


Click on *Next*.

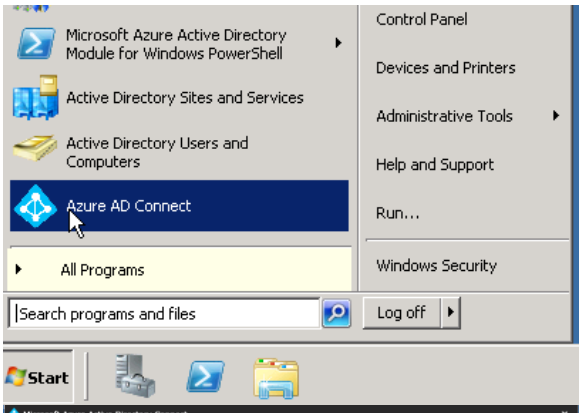


Uncheck the box *Start the synchronization process when configuration completes*.

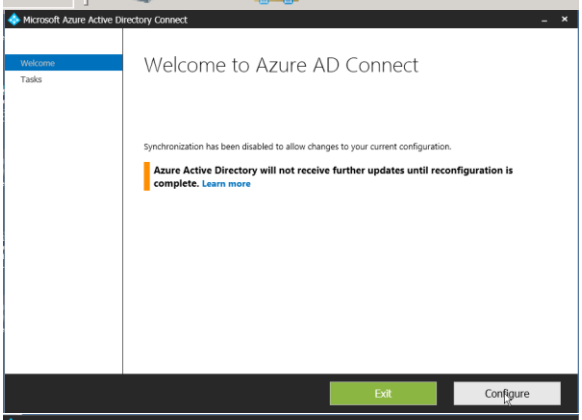
Click on *Install*.



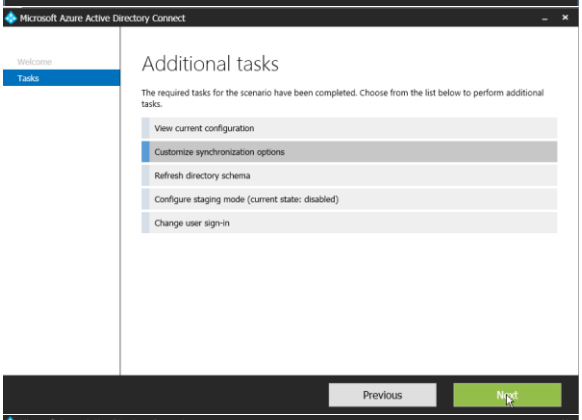
Click on *Close*.



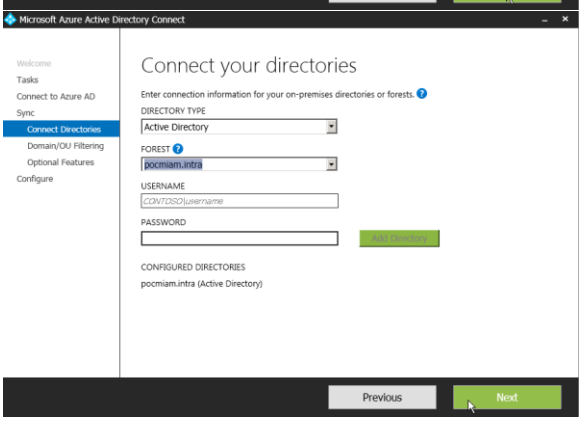
Start *Azure AD Connect* console.



Click on *Configure*.

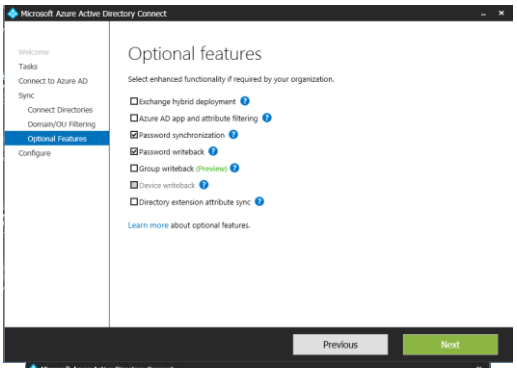


Click on *Customize synchronization options*.

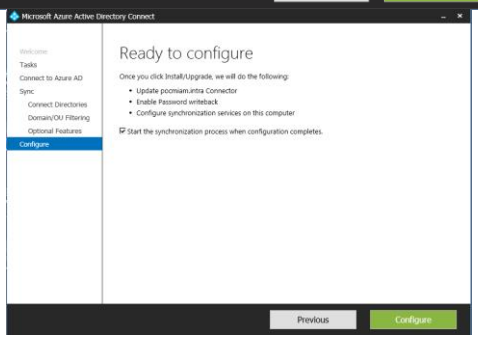


Click on *Next*.

Select only the OU *MIM\Groups* and the OU *Users* and *Disabled_Users* under each OU corresponding to the entity

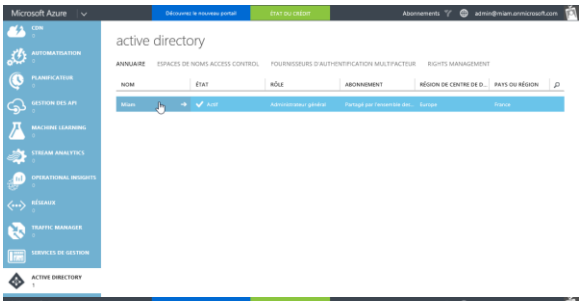


Check the boxes *Password writeback* and *Password synchronization*.

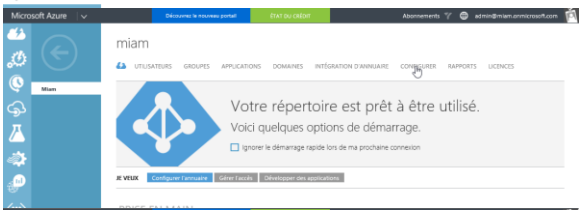


Check the box *Start the synchronization process when configuration completes*.

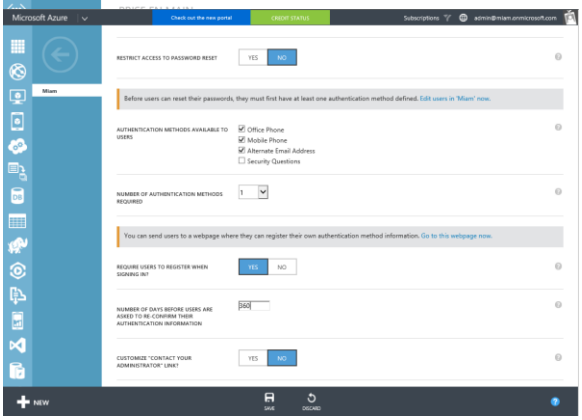
2.7 CONFIGURE AZURE ACTIVE DIRECTORY PASSWORD SELF SERVICE FEATURES



Go to https://manage.windowsazure.com and click on Active Directory.



Click on *Configure*.

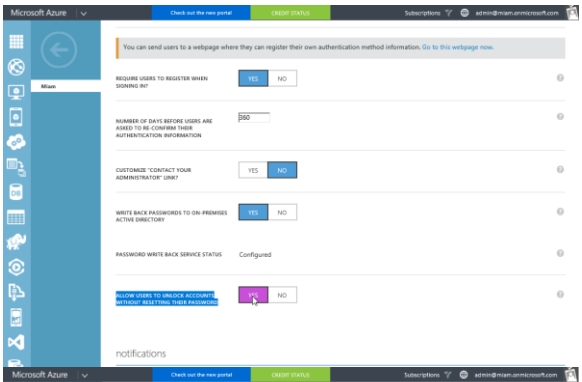


Users enabled for password reset: select *Yes*.

Restrict access to password reset: select *No*.

On *Authentication Methods Available to Users*, select only *Office Phone*, *Mobile Phone* and *Alternate Email Address*.

Number of authentication: 1

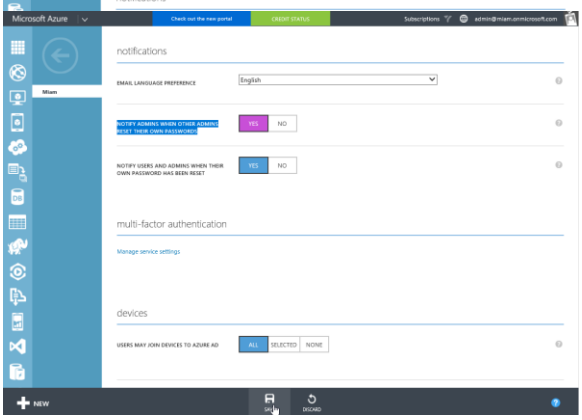


Require users to register when signing in: select *Yes*

Number of days before users are asked to re-confirm their authentication information: 360

Write back passwords to on-premises active directory: select *Yes*

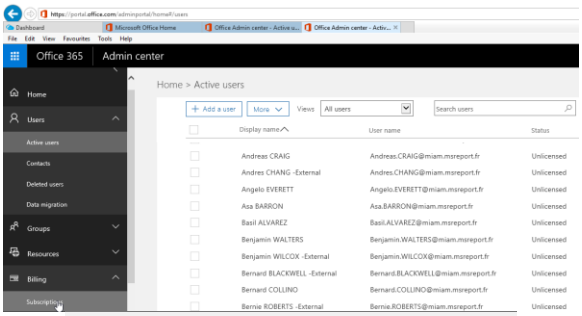
Allow users to unlock accounts without resetting their password: select *Yes*



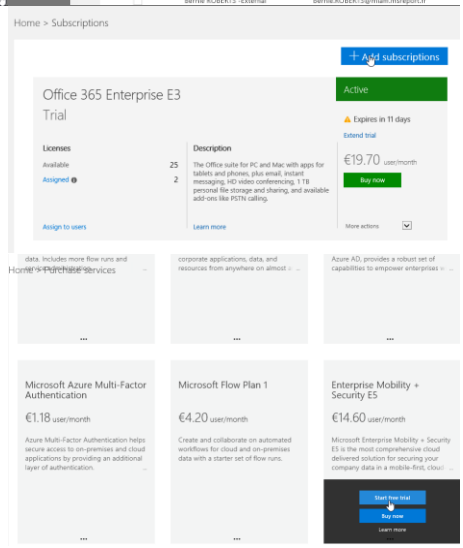
Email Language Preference: select *English*

Notify admins when other admins reset their own passwords: select *Yes*

Click on *Save*.

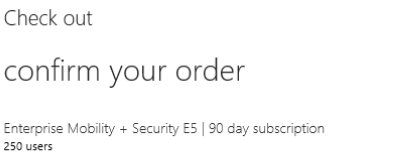


Connect to the Office 365 administrative portal.
Go to *Billing | Subscriptions*.

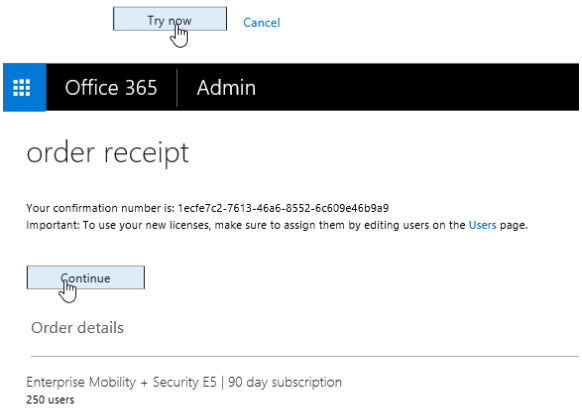


Click on *Add subscriptions*.

Start a trial of *Enterprise Mobility Security E5*.



Click on *Try now*.

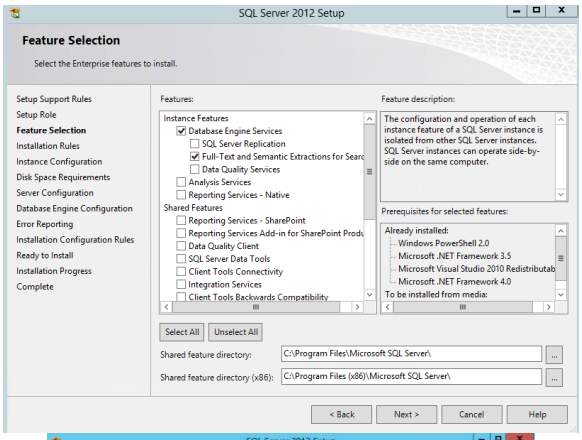


Click on *Continue*.

2.8 INSTALL POCMIM

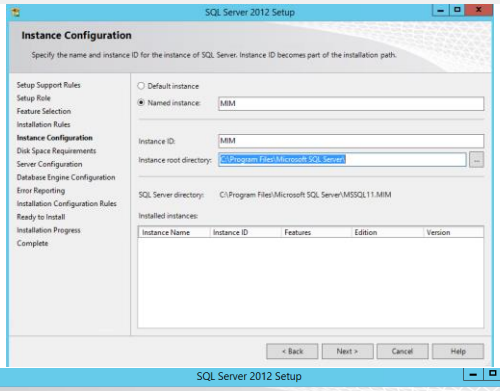
2.8.1 Install SQL server on POCMIM

Download Windows 2012 R2 installation file to install .Net Framework 3.5.
This is a prerequisite for SQL server 2012 SP3. Check that *pocmiam\svc-sql* is member of the local administrators group on POCMIM.

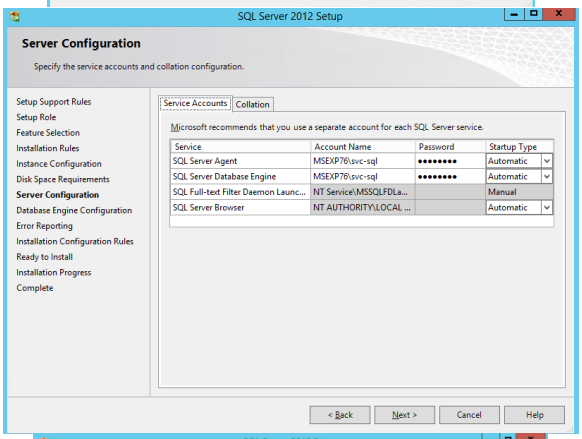


Select the following components:

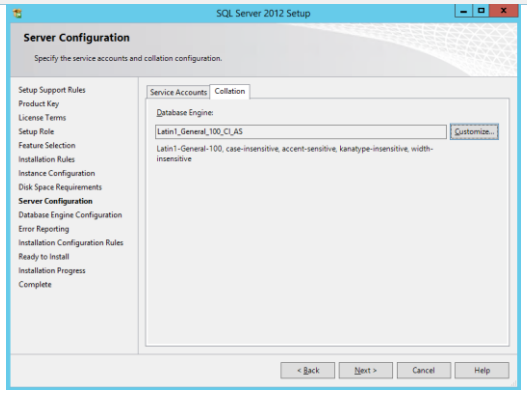
- *Database engine*
- *Full-text search*
- *Management Tools - Basic*
- *Management Tools - Complete*



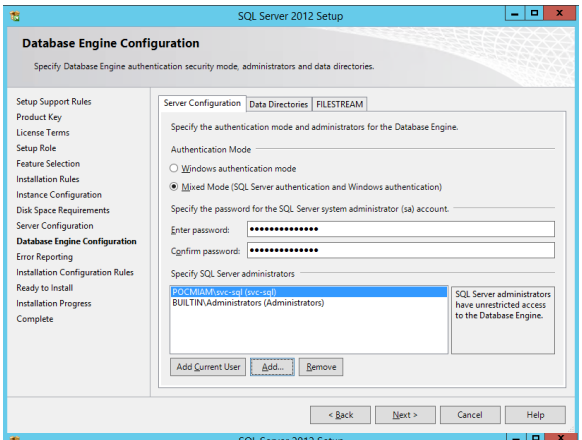
Enter *MIM* as Instance name.



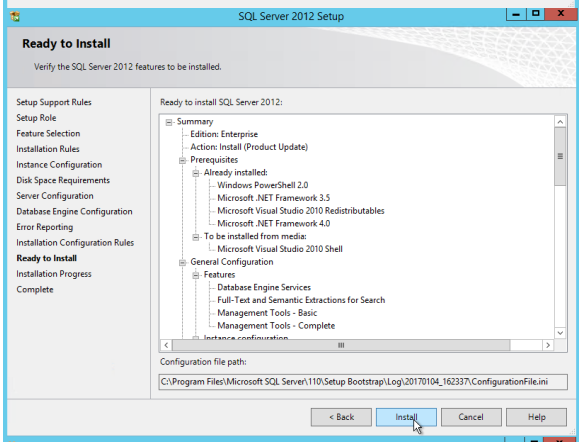
Click on *Next*.



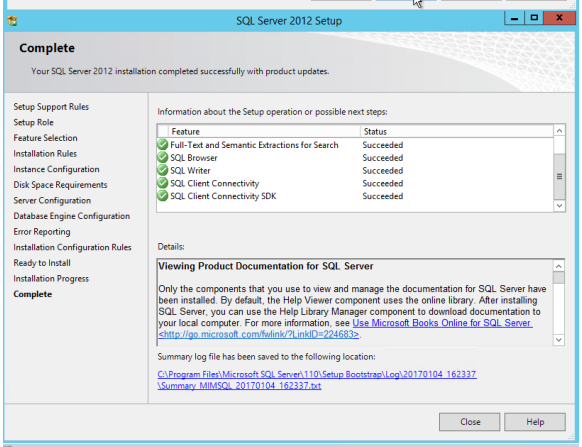
Collation: *Latin1_General_100_CI_AS*



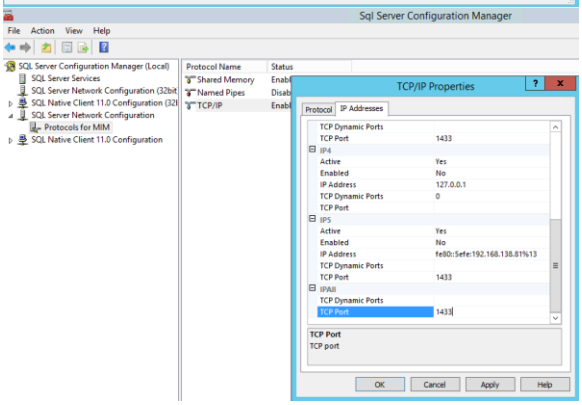
Add *pocmiam\svc-sql* and local administrators group as SYSADMIN.



Click on *Install* button.



Click on *Close* button.



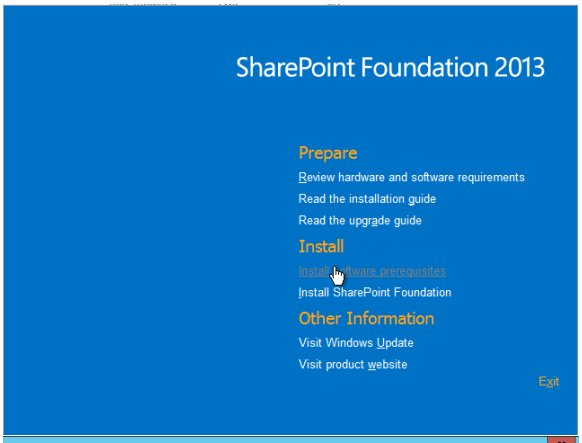
Start SQL Server Configuration Manager.
Go to *Protocols for MIM* properties in the tab *IP Adresses*.
Configure SQL Server database to listen on port *TCP 1433*.

2.8.2 Install SharePoint 2013 Foundation on POCMIM

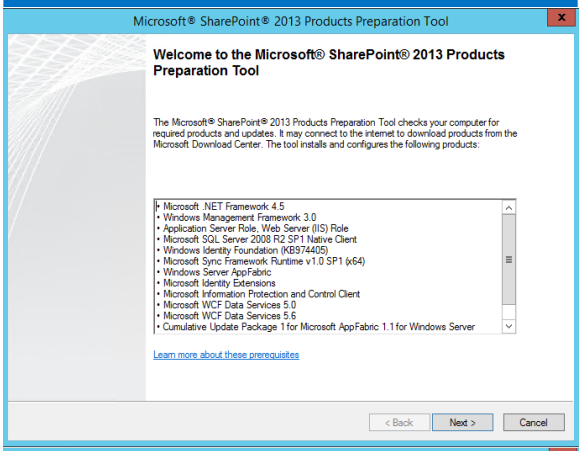
This documentation is based on https://docs.microsoft.com/fr-fr/microsoft-identity-manager/deploy-use/prepare-server-sharepoint

Download SharePoint Foundation Server 2013 SP1: http://www.microsoft.com/fr-fr/download/details.aspx?id=42039

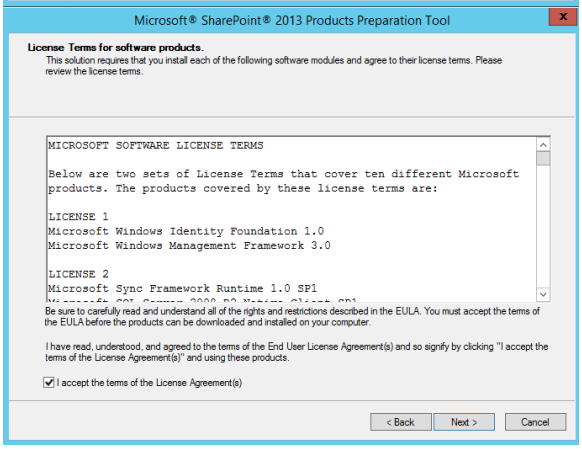
Check that the user account *pocmiam\svc-mimsps* is a local administrator of the server POCOIM.



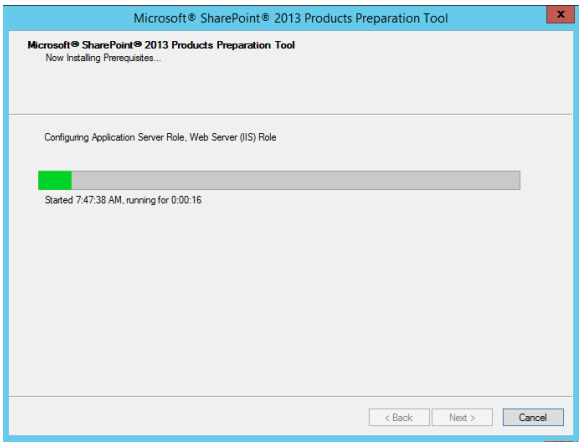
Click on *Install Software prerequisites*.

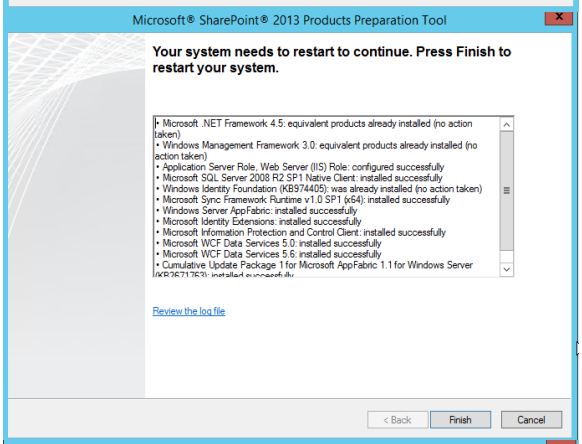


Click *Next*.

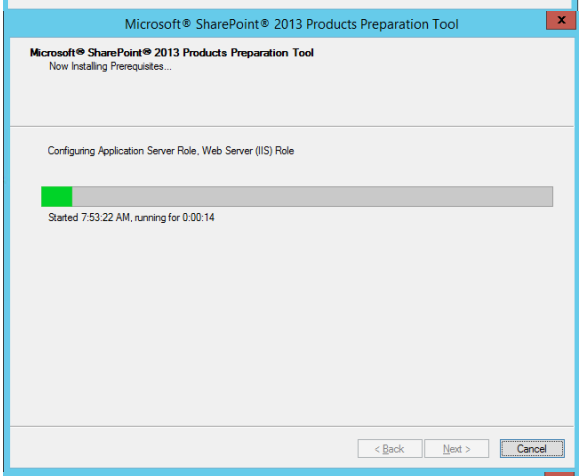


Click *Next*.

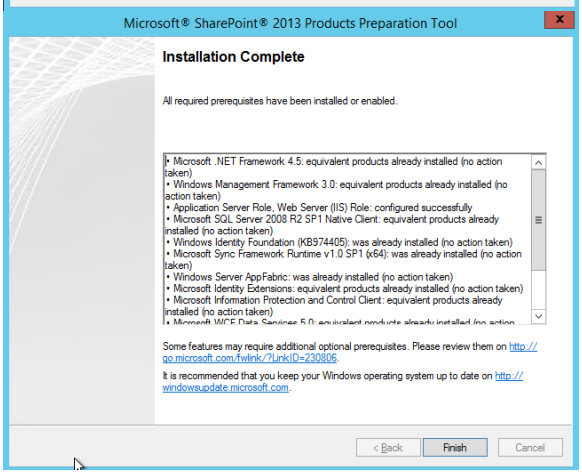




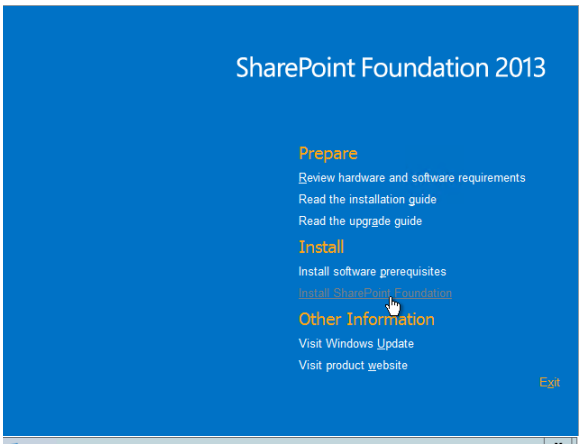
Click on *Finish* and then restart the server.



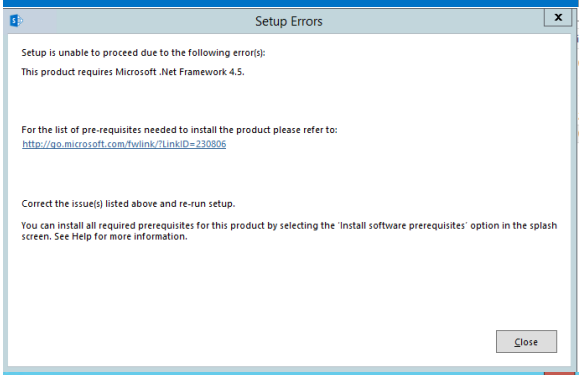
After Restart, the installation continues.



Click on *Finish* button.

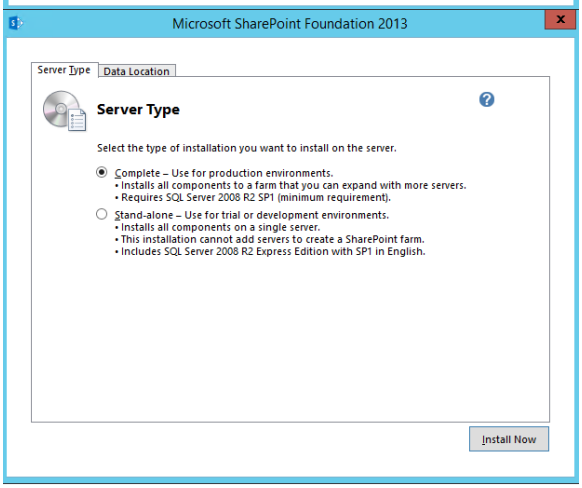


Start the installation of SharePoint 2013 Foundation.

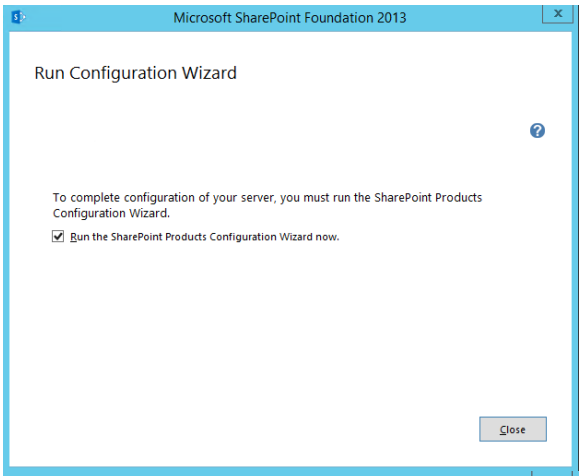


If the following message appears, apply this procedure: https://support.microsoft.com/fr-fr/help/3087184/sharepoint-2013-or-project-server-2013-setup-error-if-the-.net-framework-4.6-is-installed

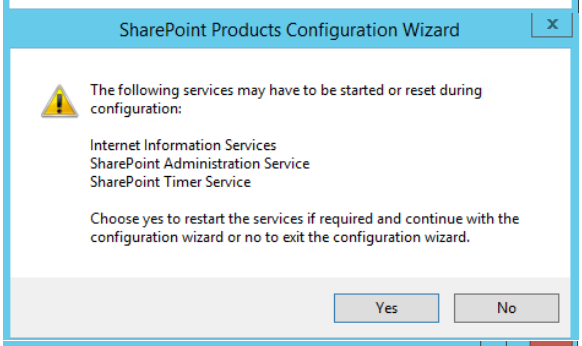
Click on *Continue*.



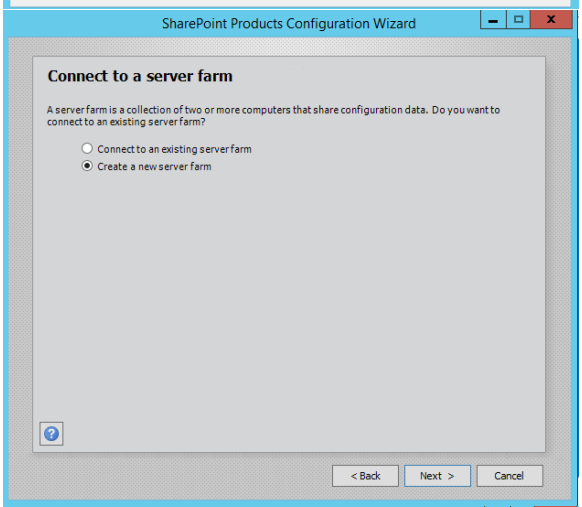
Click on *Install Now*.



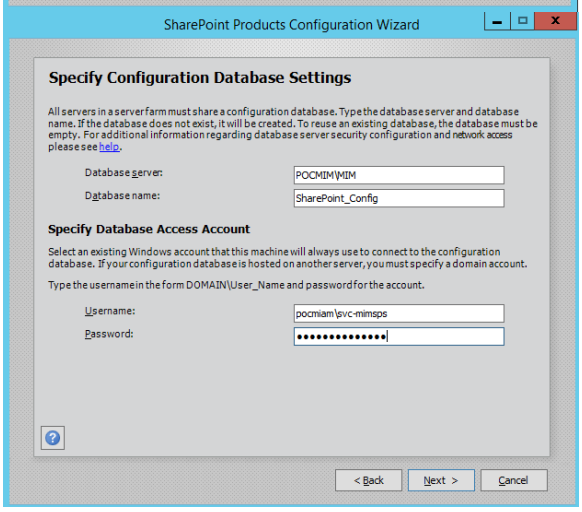
Click on *Close*.



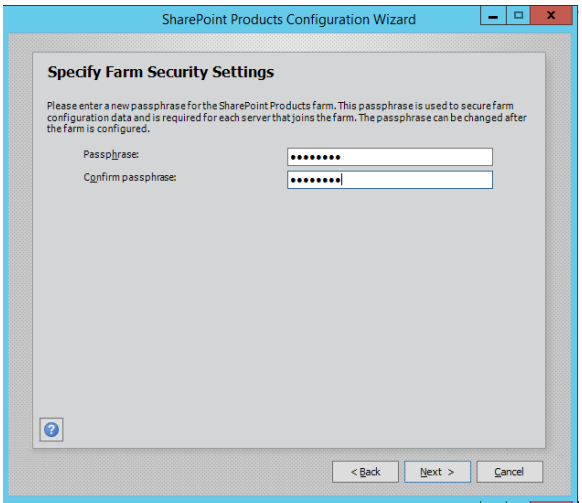
Click *Yes*.



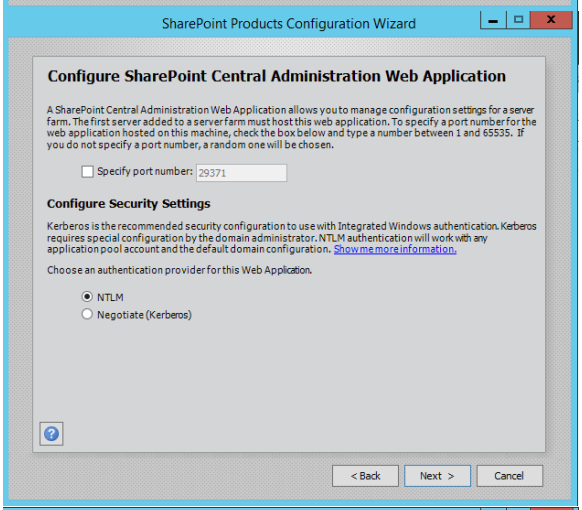
Select *Create a new server farm*.
Click on *Next*.



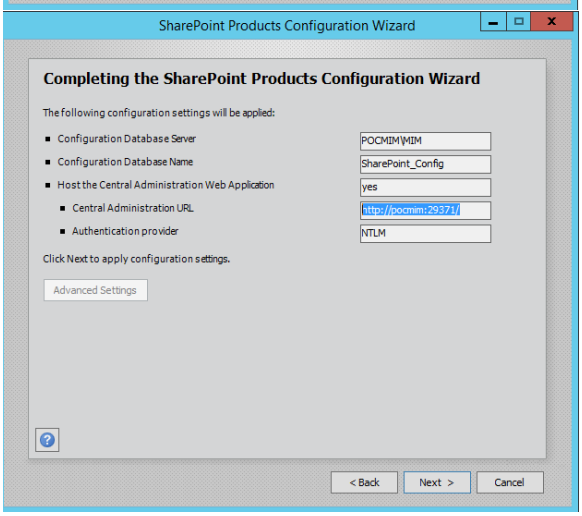
Enter the following information:
Database Server: *POCMIM\MIM*
Database name: *SharePoint_Config*
User: *pocmiam\svc-mimsps*



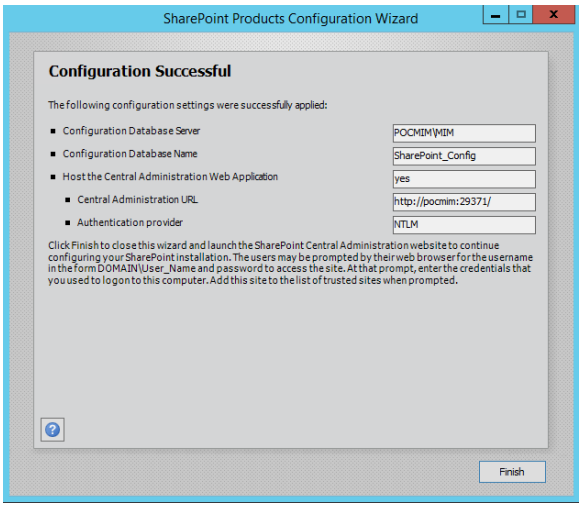
Enter the passcode.



Click on *Next*.



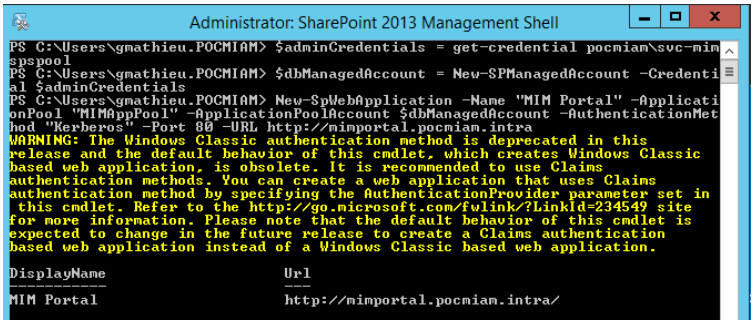
The URL of the central admin is http://pocmim:29371/



Click on *Finish*.

Create web application.
Start SharePoint 2013 Management Shell.

$adminCredentials = get-credential pocmiam\svc-mimspspool
$dbManagedAccount = New-SPManagedAccount -Credential $adminCredentials
New-SpWebApplication -Name "MIM Portal" -ApplicationPool "MIMAppPool" -ApplicationPoolAccount $dbManagedAccount -AuthenticationMethod "Kerberos" -Port 80 -URL http://mimportal.pocmiam.intra

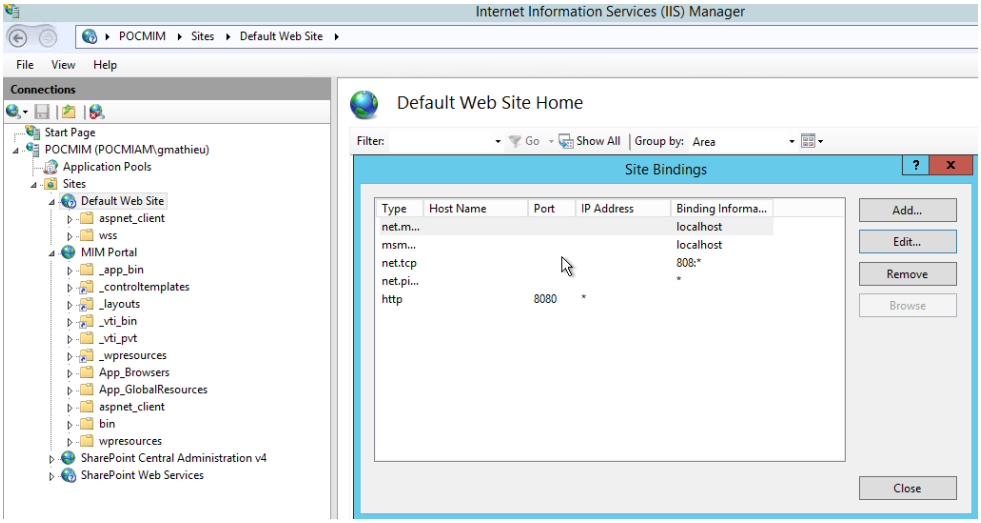


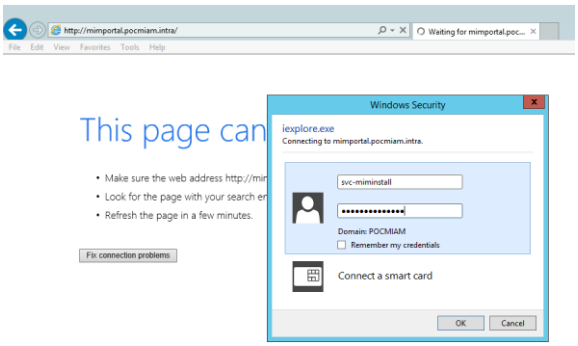
Create the SharePoint site collection.

$t = Get-SPWebTemplate -compatibilityLevel 14 -Identity "STS#1"
$w = Get-SPWebApplication "MIM Portal"
New-SPSite -Url $w.Url -Template $t -OwnerAlias pocmiam\svc-mimspspool -CompatibilityLevel 14 -Name "MIM Portal" -SecondaryOwnerAlias pocmiam\svc-miminstall
$s = SpSite($w.Url)
$s.AllowSelfServiceUpgrade = $false
$s.CompatibilityLevel
$contentService = [Microsoft.SharePoint.Administration.SPWebService]::ContentService;
$contentService.ViewStateOnServer = $false;
$contentService.Update();
$fimPortalUrl = "http://mimportal.pocmiam.intra"
Set-SPWebApplication -Identity $fimPortalUrl -AuthenticationMethod Kerberos -Zone Default
cd c:\windows\system32\inetsrv
.\config\applicationHost.config .\config\applicationHost.config.bak
.\appcmd.exe set config "MIM Portal" /section:windowsauthentication

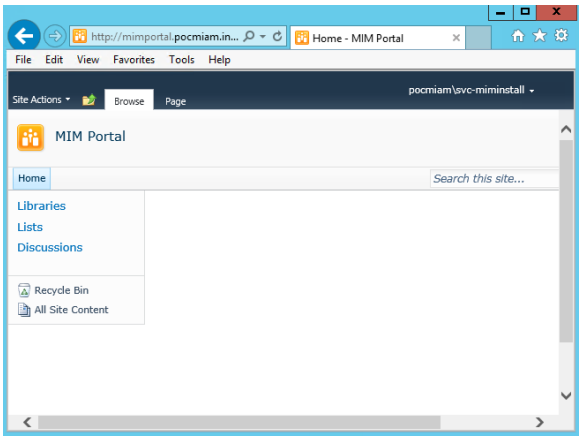
```
PS C:\Users\gmathieu.POCMIAM>
PS C:\Users\gmathieu.POCMIAM>
PS C:\Users\gmathieu.POCMIAM> $t = Get-SPWebTemplate -compatibilityLevel 14 -Ide
ntity "STS#1"
PS C:\Users\gmathieu.POCMIAM> $w = Get-SPWebApplication "MIM Portal"
PS C:\Users\gmathieu.POCMIAM> New-SPSite -Url $w.Url -Template $t -OwnerAlias po
cmiam\svc-mimspspool -CompatibilityLevel 14 -Name "MIM Portal" -SecondaryOwnerAl
ias pocmiam\svc-miminstall

Url                                                    CompatibilityLevel
---                                                    ------------------
http://mimportal.pocmiam.intra                         14


PS C:\Users\gmathieu.POCMIAM> $s = SpSite($w.Url)
PS C:\Users\gmathieu.POCMIAM> $s.AllowSelfServiceUpgrade = $false
PS C:\Users\gmathieu.POCMIAM> $s.CompatibilityLevel
14
PS C:\Users\gmathieu.POCMIAM> $contentService = [Microsoft.SharePoint.Administra
tion.SPWebService]::ContentService;
PS C:\Users\gmathieu.POCMIAM> $contentService.ViewStateOnServer = $false;
PS C:\Users\gmathieu.POCMIAM> $contentService.Update();
PS C:\Users\gmathieu.POCMIAM> $fimPortalUrl = "http://mimportal.pocmiam.intra"
PS C:\Users\gmathieu.POCMIAM> Set-SPWebApplication -Identity $fimPortalUrl -Auth
enticationMethod Kerberos -Zone Default
PS C:\Users\gmathieu.POCMIAM> cd c:\windows\system32\inetsrv
PS C:\windows\system32\inetsrv> .\config\applicationHost.config .\config\applica
tionHost.config.bak
PS C:\windows\system32\inetsrv> .\appcmd.exe set config "MIM Portal" /section:wi
ndowsauthentication
Applied configuration changes to section "system.webServer/security/authenticati
on/windowsAuthentication" for "MACHINE/WEBROOT/APPHOST/MIM Portal" at configurat
ion commit path "MACHINE/WEBROOT/APPHOST/MIM Portal"
PS C:\windows\system32\inetsrv> _
```

Change the configuration of the default website to listen on port TCP 8080 instead of TCP 80.





Connect to the SharePoint website by using the user account *pocmiam\svc-miminstall*.



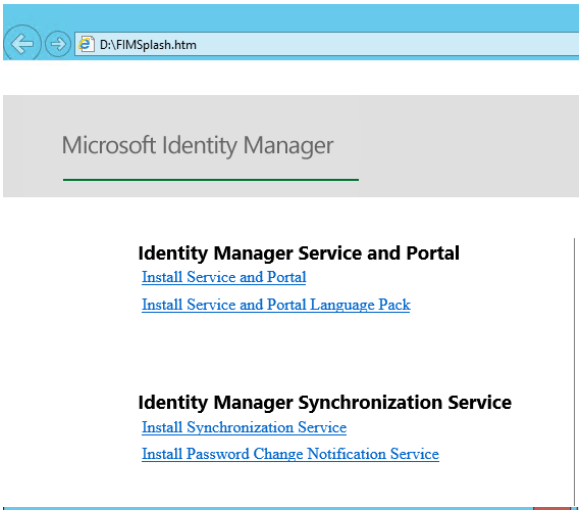
Disable indexing. Start SharePoint 2013 Management Shell:
Get-SPTimerJob hourly-all-sptimerservice-health-analysis-job | disable-SPTimerJob

```
PS C:\> Get-SPTimerJob hourly-all-sptimerservice-health-analysis-job | disable-S
PTimerJob
PS C:\> _
```

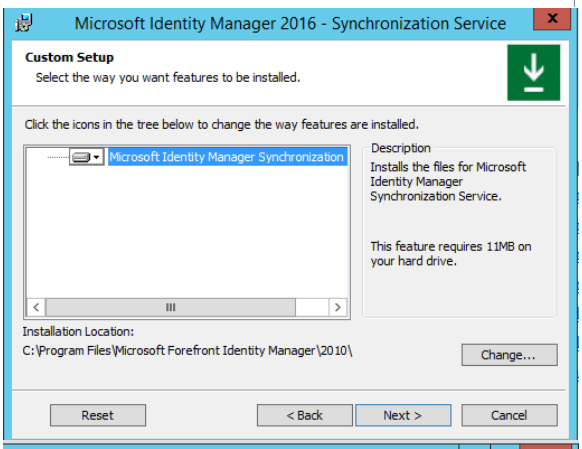
Restart the server.

2.8.3 Deploy MIM Synchronization Service on POCMIM

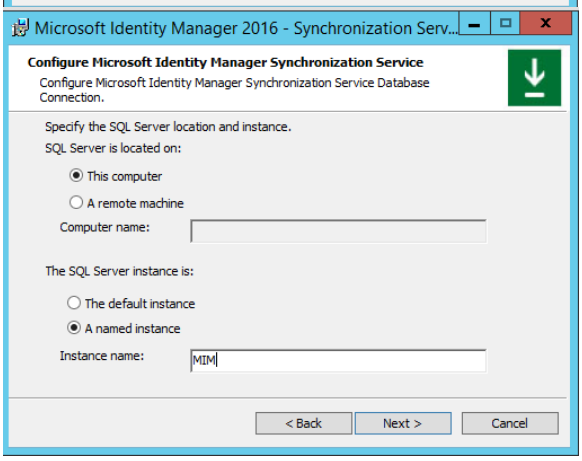
Check if *pocmiam\svc-mimsync* is member of the group Administrators on POCMIM. The account will obtain SYSADMIN right on the SQL server instance MIM.
Check if .Net Framework 3.5 and 4.5 are installed on POCMIM.
Check if SQL Server 2012 native client is installed on POCMIM.



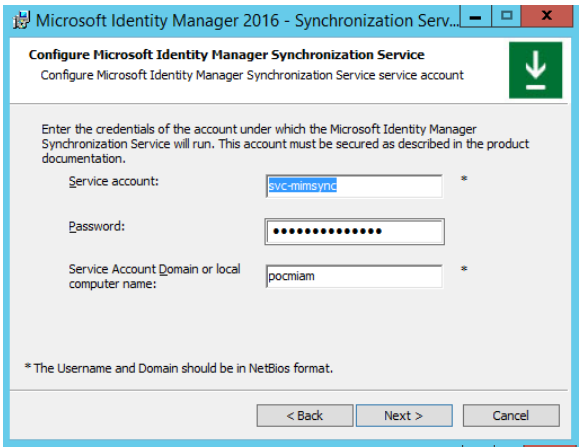
Open a session with a domain user which have local administrator right.
Check if you have created the 5 MIM Synchronization Service groups created previously.
Click on *Install Synchronization Service* link.



Click on *Next*.

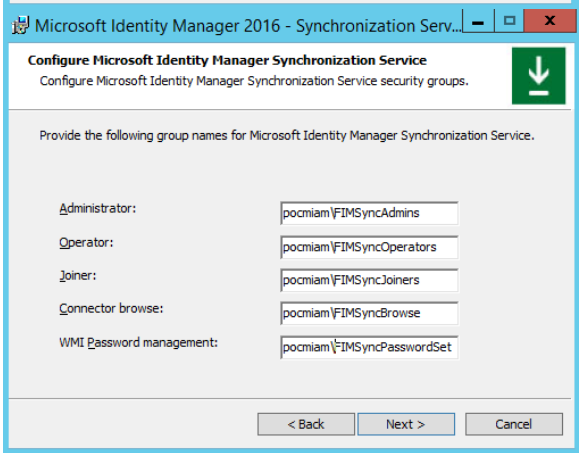


Select a named instance and enter *MIM*.

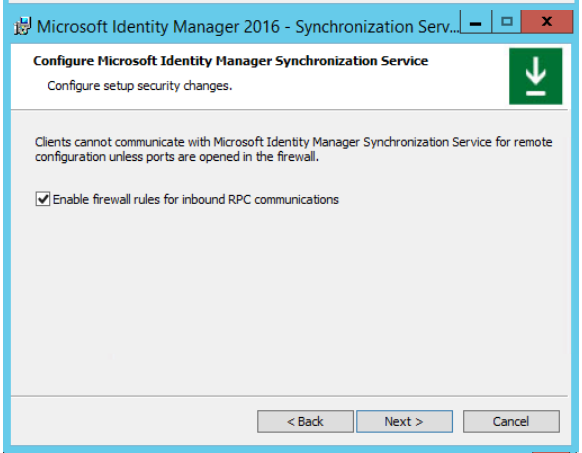


Enter the following information:
Service account: *svc-mimsync*
Password: *enter the password*
Service Account Domain or local computer name: *pocmiam*

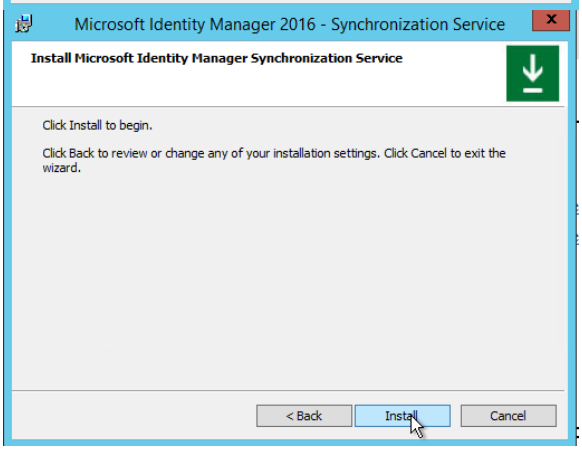
<u>The domain name must be entered in NETBIOS format.</u>



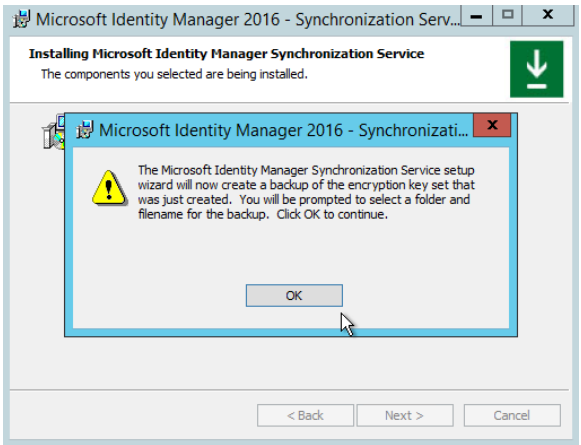
Administrator: *pocmiam\FIMSyncAdmins*
Operator: *pocmiam\FimSyncOperators*
Joiner: *pocmiam\FIMSyncJoiners*
Connector browse: *pocmiam\FIMSyncBrowse*
WMI Password Management: *pocmiam\FIMSyncPasswordSet*



Check the box *Enable firewall rules for inbound RPC communications*.

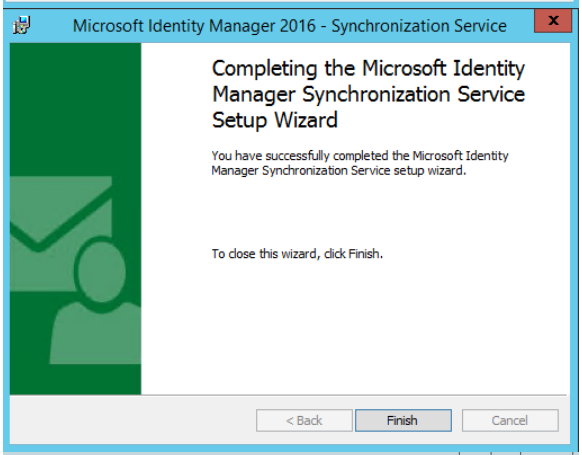


Click on *Install*.

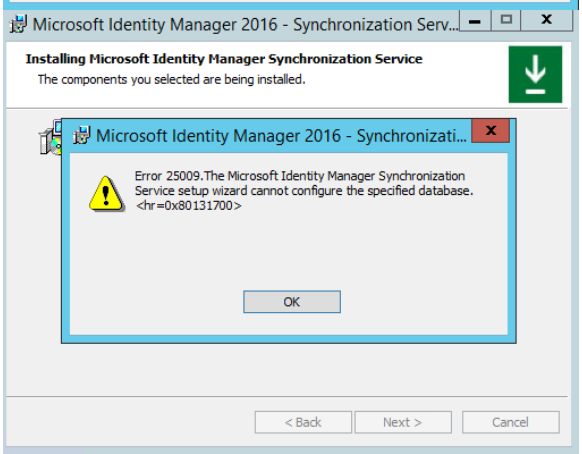


Click on *OK*.

Backup the key in the folder *C:_adm*.



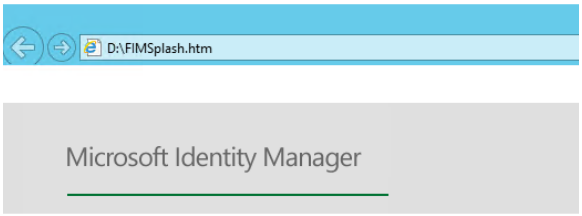
Click on *Finish* and then restart the server.



In case of installation error, you can start the installation with a log file by using this command:
*msiexec /i "D:\Synchronization Service\Synchronization Service.msi" /L*v c:\Log\LOG.txt*
If you obtain this error 25009, apply the following procedure and check if you have install .Net Framework 3.5.
https://social.technet.microsoft.com/wiki/contents/articles/1734.fim-troubleshooting-installation-error-25009-sa-admin-rights-missing.aspx

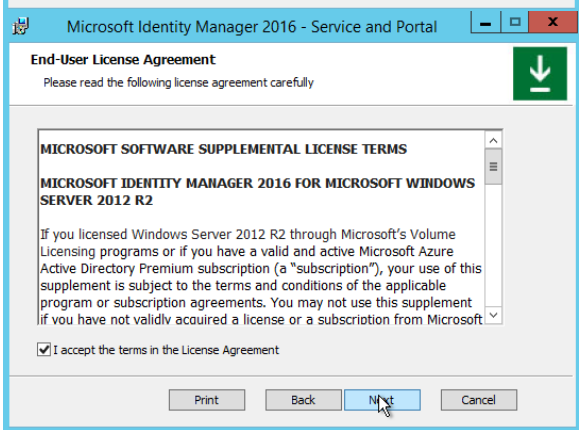
2.8.4 Install MIM Service on POCMIM

Open a session with the user *pocmiam\svc-miminstall.*
This user has local administrative right on POCMIM server, on the SharePoint Server and on SQL server instance. Provide SYSADMIN right to this account: *Pocmiam\svc-mimma.*

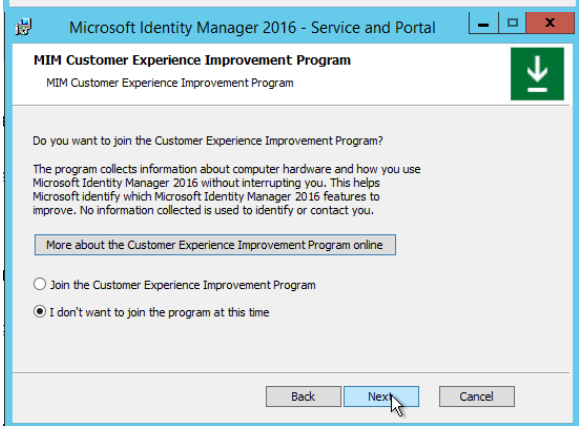


Click on *Install Service and Portal*.

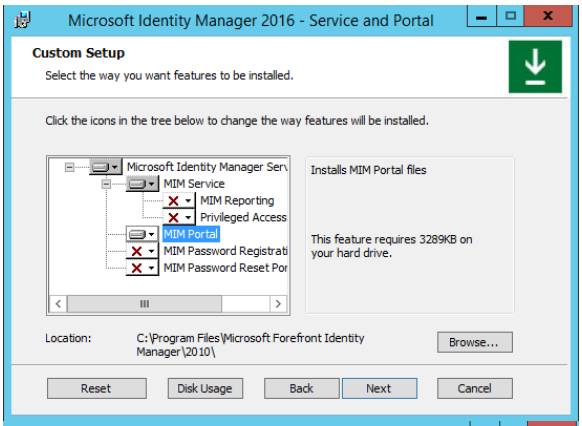
Click on *Next*.



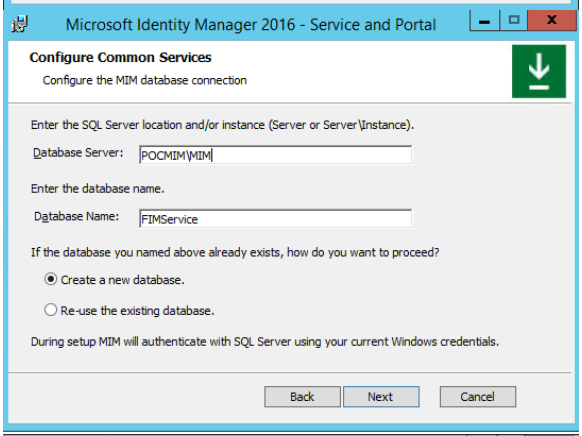
Click on *Next*.



Click on *Next*.

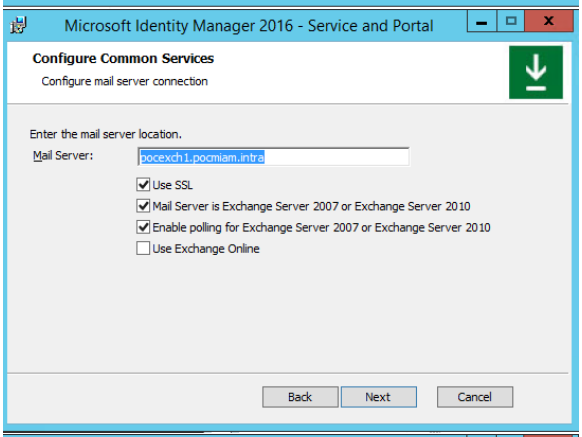


Do not install the following components:
MIM password Registration Service
MIM Password Reset Portal
MIM Reporting
Privileged Access Management.

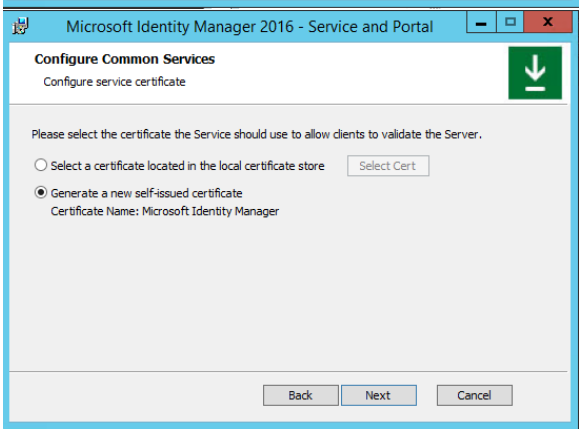


Database Server: *POCMIM\MIM*
Click on *Next*.

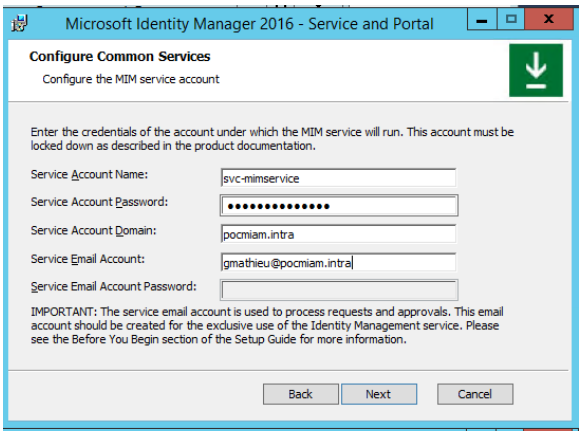
Note:
Install will continue even if you enter a bad SQL instance name but the FIM Service will not start.



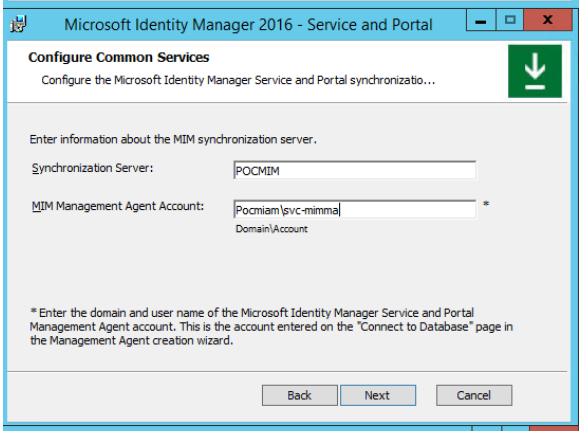
Enter the name of the Exchange Server:
pocexch1.pocmiam.intra



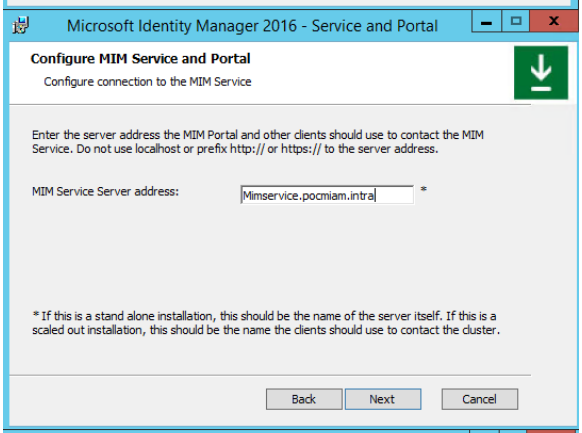
Click on *Next*.



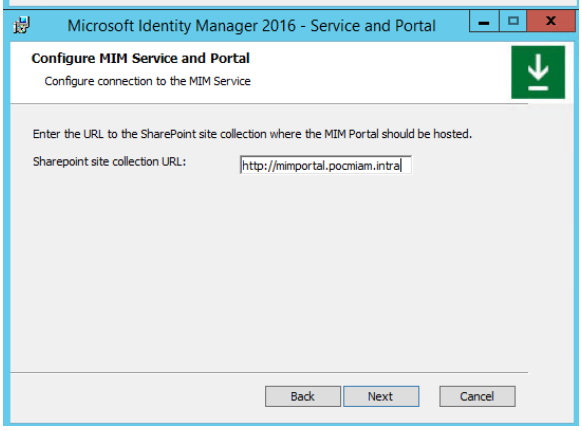
Enter the following information:
Service Account Name: *svc-mimservice*
Service Account Domain: *pocmiam.intra*
Service Email Account: *gmathieu@pocmiam.intra*



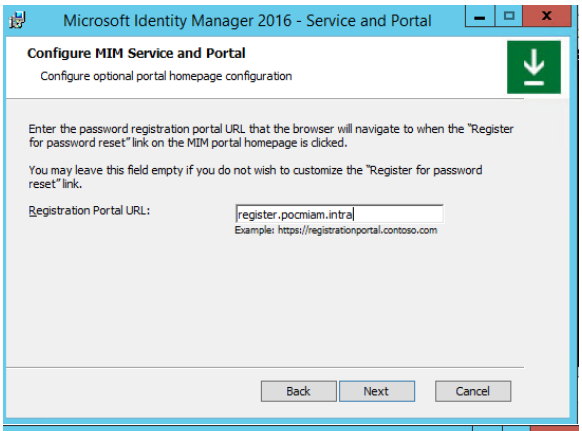
MIM Management Agent Account: *Pocmiam\svc-mimma*



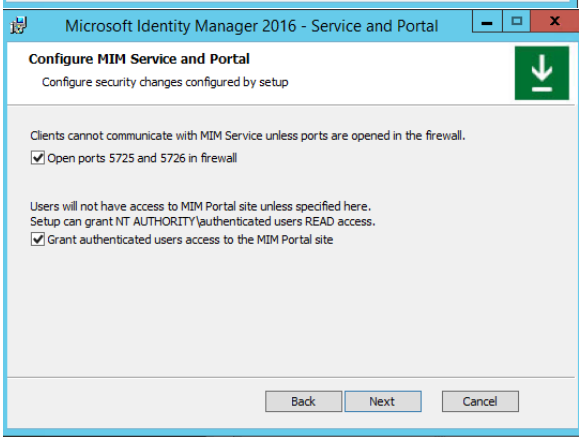
MIM Service Server address:
Mimservice.pocmiam.intra



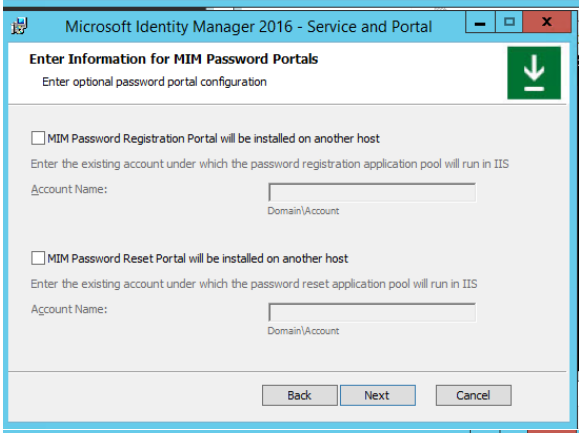
SharePoint site collection URL:
http://mimportal.pocmiam.intra



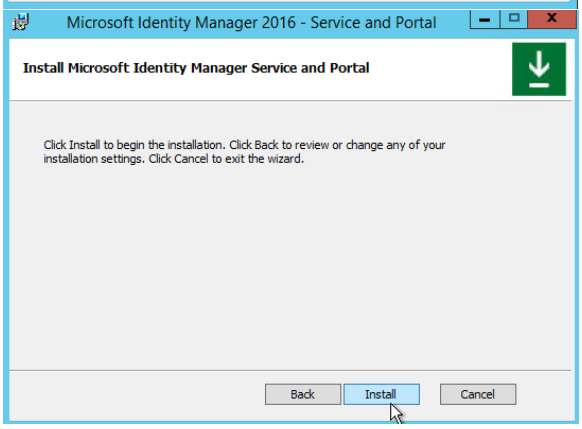
Registration Portal URL:
https://register.pocmiam.intra



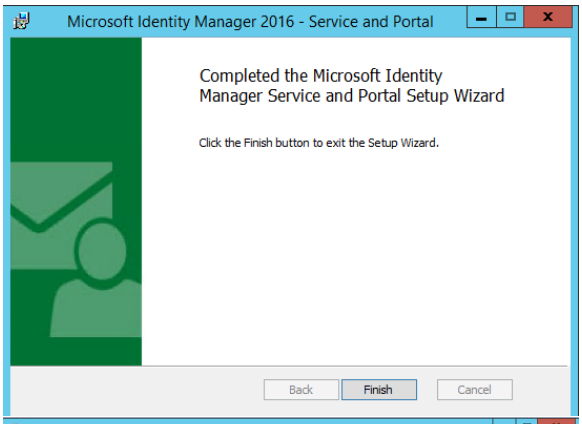
Check the boxes *Open ports 5725 and 5726 in firewall* and *Grant authenticated users access to MIM Portal site*.



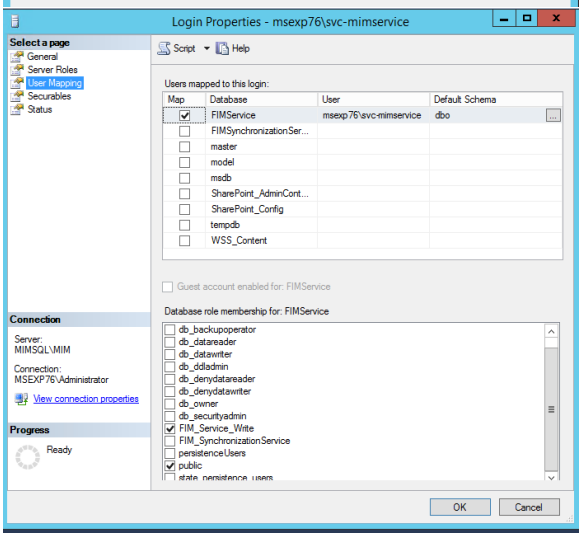
Click on *Next*.



Click on *Install*.



Click on *Finish*.



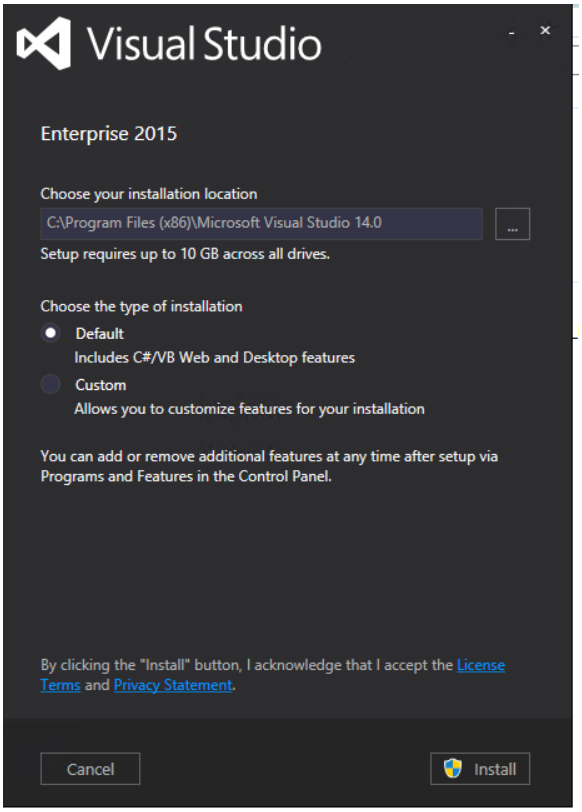
The user *Pocmiam\svc-mimservice* has been granted access to SQL Server database automatically by the setup.

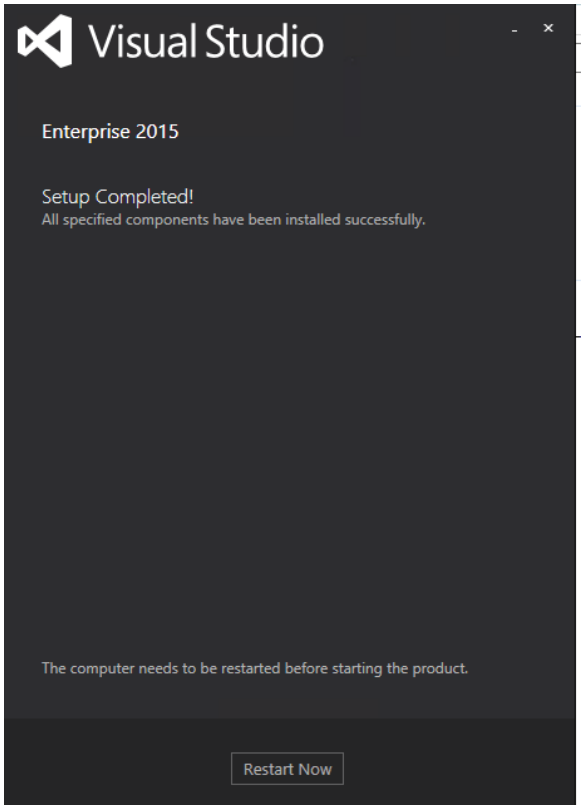
Add **.pocmiam.intra* in *Local Intranet website* zone to enable Kerberos authentication.
Start IIS and configure the MIM portal website to listen on TCP 443 and map a web server certificate.

Connect to: http://mimservice.pocmiam.intra/IdentityManagement

2.8.5 Install Visual Studio 2015 on POCMIM

Install Visual Studio 2015.
This tool is required to create MIM 2016 rules extension or Metaverse rules.
Perform a default installation.





2.8.6 Install MIMWAL

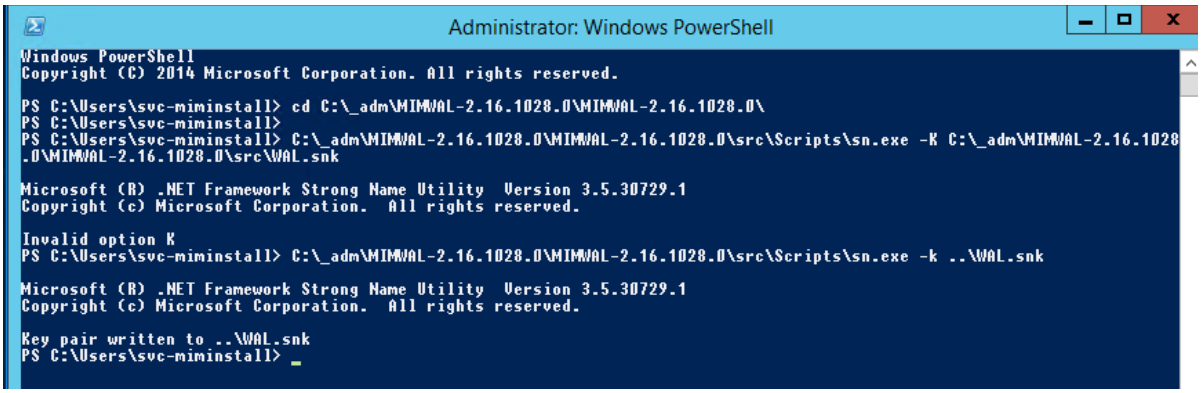
MIMWALL allows to extend MIM workflow activities:

- Add Delay - Add delay in workflow processing
- Create Resource - Create new MIM resources
- Delete Resources - Delete existing MIM resources
- Generate Unique Value - Generate unique value for use in attributes
- Request Approval - Request Approval during authorization phase
- Run PowerShell Script - Run PowerShell script code
- Send Email Notification - Send Email Notifications
- Update Resources - Update existing MIM resources or read existing MIM resources to populate WorkflowData dictionary
- Verify Request - Verify request during authorization phase

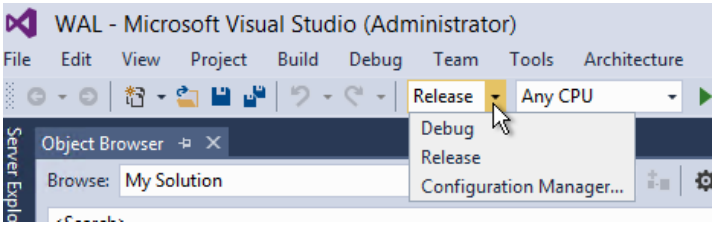
http://microsoft.github.io/MIMWAL/
https://github.com/Microsoft/MIMWAL/wiki/Add-Delay-Activity

The step to install MIMWALL is described here:
https://github.com/Microsoft/MIMWAL/wiki/build-and-deployment
https://tlktechidentitythoughts.wordpress.com/2016/02/02/mimfim-workflow-activity-library-installation/

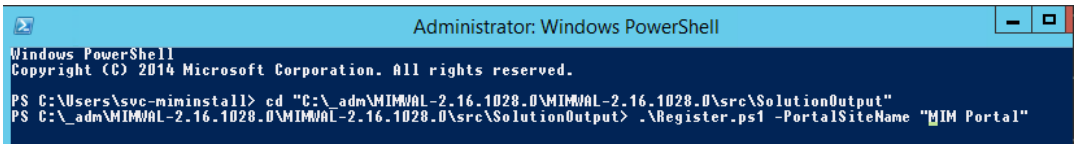
Create the Key pair.



Copy the pair key to the proper emplacement.
Edit the file *WAL.sln* with Visual Studio.
Compile the project in *Release* mode.



Go to the folder *C:_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput*.
Start the register.ps1 script.



```
PS C:\Users\svc-miminstall> cd "C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput"
PS C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput> .\Register.ps1 -PortalSiteName "MIM Portal"
DEBUG: Registering assembly in GAC:
'C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivi
Library.dll'
DEBUG: Microsoft (R) .NET Global Assembly Cache Utility.  Version 3.5.21022.8
Copyright (c) Microsoft Corporation.  All rights reserved.

Assembly successfully added to the cache
DEBUG: Registering assembly in GAC:
'C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivi
Library.UI.dll'
DEBUG: Microsoft (R) .NET Global Assembly Cache Utility.  Version 3.5.21022.8
Copyright (c) Microsoft Corporation.  All rights reserved.

Assembly successfully added to the cache
DEBUG: Loading Assembly:
C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivit
ibrary.dll
DEBUG: Loading Assembly:
C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivit
ibrary.UI.dll
DEBUG: Updating Assembly Bindings in the config file: C:\Program Files\Microsoft Forefront Identity
Manager\2010\Service\Microsoft.ResourceManagement.Service.exe.config
DEBUG: Updated Assembly Bindings in the config file: C:\Program Files\Microsoft Forefront Identity
Manager\2010\Service\Microsoft.ResourceManagement.Service.exe.config
DEBUG: Configuring WAL event source in the config file: C:\Program Files\Microsoft Forefront Identity
Manager\2010\Service\Microsoft.ResourceManagement.Service.exe.config
DEBUG: Configured WAL event logging in the config file: C:\Program Files\Microsoft Forefront Identity
Manager\2010\Service\Microsoft.ResourceManagement.Service.exe.config
VERBOSE: Loading module from path
'C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WebAdministration\WebAdministration.psd1'.
VERBOSE: Loading 'Assembly' from path
'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.IIS.PowerShell.Framework\v4.0_8.5.0.0__31bf3856ad364e35\Microso
.IIS.PowerShell.Framework.dll'.
VERBOSE: Loading 'TypesToProcess' from path
'C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WebAdministration\iisprovider.types.ps1xml'.
VERBOSE: Loading 'FormatsToProcess' from path
'C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WebAdministration\iisprovider.format.ps1xml'.
VERBOSE: Exporting function 'IIS:'.
VERBOSE: Exporting cmdlet 'Start-WebCommitDelay'.
Creating event source MicrosoftServices.IdentityManagement.WorkflowActivityLibrary in event log WAL
Event source MicrosoftServices.IdentityManagement.WorkflowActivityLibrary created in event log WAL
Writing a test event in the event log 'WAL'
The Forefront Identity Manager Service service is stopping...
The Forefront Identity Manager Service service was stopped successfully.

The Forefront Identity Manager Service service is starting..
The Forefront Identity Manager Service service was started successfully.


Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
Review script console output for any errors. Once the deployment is successful on *ALL* the servers, update the assembly
 version in MIMWAL XOMLs by executing UpdateWorkflowXoml.ps1 script.
PS C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput> .
```

Start also the command: *UpdateWorkflowXoml.ps1*

```
PS C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput> .\UpdateWorkflowXoml.ps1
DEBUG: Loading Assembly:
C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivityL
ibrary.dll

Skipping Workflow : '_AD User Deletion Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : '_AD User Deprovision Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : '_Add-To-Group'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : '_AD-Out-Test1'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : '_Security Group Provisioning to AD'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'Expiration Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'Filter Validation Workflow for Administrators'. No updates necessary. It does not use any MIMWAL ac
tivities.

Skipping Workflow : 'Filter Validation Workflow for Non-Administrators'. No updates necessary. It does not use any MIMWA
L activities.

Skipping Workflow : 'Group Expiration Notification Workflow'. No updates necessary. It does not use any MIMWAL activitie
s.

Skipping Workflow : 'Group Validation Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'Owner Approval Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'PAM: Handle PAM Request'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'PAM: Request Authorization'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'Password Reset Action Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'Password Reset AuthN Workflow'. No updates necessary. It does not use any MIMWAL activities.

Skipping Workflow : 'Requestor Validation With Owner Authorization'. No updates necessary. It does not use any MIMWAL ac
tivities.

Skipping Workflow : 'Requestor Validation Without Owner Authorization'. No updates necessary. It does not use any MIMWAL
 activities.

Skipping Workflow : 'System Workflow Required for Registration'. No updates necessary. It does not use any MIMWAL activi
ties.
PS C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\SolutionOutput>
```

Check that all news workflow activities are available.


Create Workflow
Add Activity
Activity Picker
Active Directory - Add User to Group
An Activity for adding users to Active Directory Groups
Active Directory Password Reset Activity
This is an activity to reset a user's password.
Function Evaluator
This activity allows functions to be used in workflow definition.
Notification
This activity sends notification to specific recipients.
Synchronization Rule Activity
This activity manages the application of Synchronization Rules to FIM objects.
WAL: Add Delay
Add a delay / wait to the workflow execution.
WAL: Create Resource
Create a new resource and assign attribute values.
WAL: Delete Resources
Delete one or more resources.
WAL: Generate Unique Value
Generate a unique string value based on defined criteria.
WAL: Run PowerShell Script
Run a PowerShell script from workflow.
WAL: Send Email Notification
Send Email Notification
WAL: Update Resources
Update multiple attributes on one or more

3 CONFIGURE MIM 2016 SOLUTION

3.1 MAIN USE CASES

3.1.1 schema and synchronization rules

HR database (person class)	AD attribute (User class)	MIM Synchronization Service (person class)	MIM Service (person class)	Provision (source of authority)	Update (source of authority)	Rules
Global_ID	ExtensionAttribute 15	Global_ID	Global_ID	HR Database	No update allowed	Change is not allowed. Global_ID is a counter (digits only).
FIRST_NAME	Sn	LastName	LastName	HR Database	HR Database	
LAST_NAME	givenName	Firstname	Firstname	HR Database	HR Database	
	MailNickName	MailNickName	MailNickName	HR Database	AD (Manual change)	Allow to build email address. Generate automaticaly: GivenName + . + Sn
	displayName	displayName	displayName	Mim portal	Mim portal	Sn + space + GivenName
EMPLOYEE_ID	ExtensionAttribute 1	EmployeeId	EmployeeId	HR Database	HR Database	HR code entity and employee ID Example: S000000002E000000001 EmployeeID doesn't support this format. We will use ExtensionAttribute1 instead.
EMPLOYEE_TYPE	EmployeeType	EmployeeType	EmployeeType	HR Database	HR Database	2 possibles values : *Internal* and *External* Could be changes by manager (Mim portal) or by HR team.
EMPLOYEE_TYPE	EmployeeType	EmployeeTypeMim	EmployeeType	N.A	Mim portal	

	samAccountName	AccountName	AccountName	MIM portal	MIM portal	Active Directory login Generated automatically : *givenname + . + Sn.* *In case of conflict, add a digit* Size: 20 characters If first name or last name is changed, SamAccountName is not updated automatically.
	distinguishedName			AD	AD (Manual change)	Size: 255 caractères Generated automatically. If first name or last name is changed, DistinguishedName is not updated automatically.
	cn			AD	AD (Manual change)	Size: 255 caractères Generated automatically. If first name or last name is changed, Cn is not updated automatically (rename).
	mail	Email	Email	AD	AD	Generate by Exchange (email addresses policy) based on mailnickname
	userPrincipalName			MIM portal	MIM portal	Generate automatically based on SamAccountName and Company attribute: SamAccountName + @pocmiam.msreport.fr
DIVISION	company	company	company	HR Database	HR Database	Generate randomly based on HR6.XLS file. Example: ENTITY1
DEPARTMENT	department	department	department	HR Database	HR Database	Generate randomly based on HR6.XLS file. Example: Internal Communication
JOB_TITLE	title	JobTitle	JobTitle	HR Database	HR Database	Generate based on HR6.XLS file. Example: Executive Assistant Finance / Legal
MANAGER	Manager	Manager	Manager	HR Database	HR Database	Contains the Global_ID value of the Manager.
STATE	streetaddress	PostalAddress	Address	HR Database	HR Database	Generated randomly based on AddressesPhones.csv. Example: 255 quai de la Bataille de Stalingrad
ZIP_CD	postalCode	postalCode	PostalCode	HR Database	HR Database	Generated randomly based on AddressesPhones.csv. Example: 92866
CITY	l	City	City	HR Database	HR Database	Generated randomly based on AddressesPhones.csv. Example: London

C	co C CountryCode	Country	Country	HR Database	HR Database	Generated randomly based on AddressesPhones.csv. Example: France
Mobile	Mobile	MobilePhone	MobilePhone	HR Database	HR Database	Generated randomly based on AddressesPhones.csv. Example: +33 (0)6 57 75 84 28
Mobile	Mobile	Mobile	MobilePhone	N.A	Mim portal	Generated randomly based on AddressesPhones.csv. Example: +33 (0)6 57 75 84 28 Allow to update mobile from MIM portal (avoid bidirectional synchronization).
TelephoneNumber	TelephoneNumber	OfficePhone	OfficePhone	HR Database	HR Database	Generated randomly based on AddressesPhones.csv. Example: +33 (0)1 57 75 84 28
TelephoneNumber	TelephoneNumber	TelephoneNumber	OfficePhone	N.A	Mim portal	Generated randomly based on AddressesPhones.csv. Example: +33 (0)1 57 75 84 28
	thumbnailPhoto	Photo	Photo	Mim portal	Mim portal	Photo attribute
EmployeeEndDate	AccountExpires	EmployeeEndDate	EmployeeEndDate	HR Database	HR Database	Used to deprovision user.
EmployeeStartdate		EmployeeStartdate	EmployeeStartdate	HR Database	HR Database	Employee start date.
Type	ExtensionAttribute 10	Type	Type	HR Database	HR Database	Generated Randomly based on Type.csv. if "Cadre" or "Agent de maitrise": no manager approval if you change EmployeeTYpe, Mobile or TelephoneNumber. If cadre dirigeant, approval is required if you change HR field from MIM portal (EmployeeType, Mobile, TelephoneNumber)
Domain		Domain	Domain	HR Database	No change allowed	If 1, create user in domain, pocmiam.intra If 2, create user in domain child.pocmiam.intra

3.1.2 MIM 2016 Web interface customization

The edit form of the Mim 2016 web portal will be configured to display the fields in the table below:

General	Work info	Contact Info
Photo	Employee Start Date	**Office Phone**
Global_ID	Employee End Date	**Mobile Phone**
First name	**Employee Type**	Address
Last name	Employee Id	City
DisplayName	Manager	Postal code
AccountName	Company	Country
Domain	Department	
E-mail alias	Job title	
E-Mail	Type	

Only fields in Red and bold could be changed by a manager via MIM Portal.
Only fields which are underline could be changed by the user himself.
Other fields will be displayed in read only.

3.1.3 Other requirements

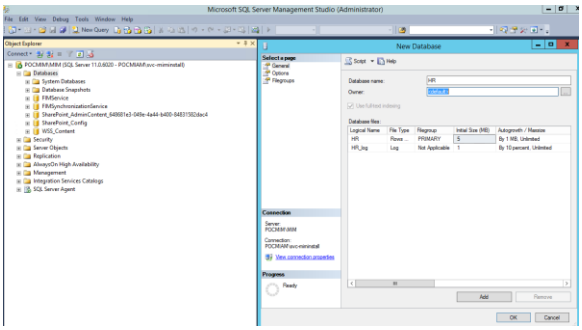
MIM 2016 will be configured to:

- Provision, update and deprovision accounts in AD and Exchange 2013 automatically based on HR CSV file (by synchronization).
- Implement different policies for internal and external users (value for *DisplayName*).
- Allow an end user to update himself his mobile phone.
- Allow manager to edit the AD accounts of this reports.

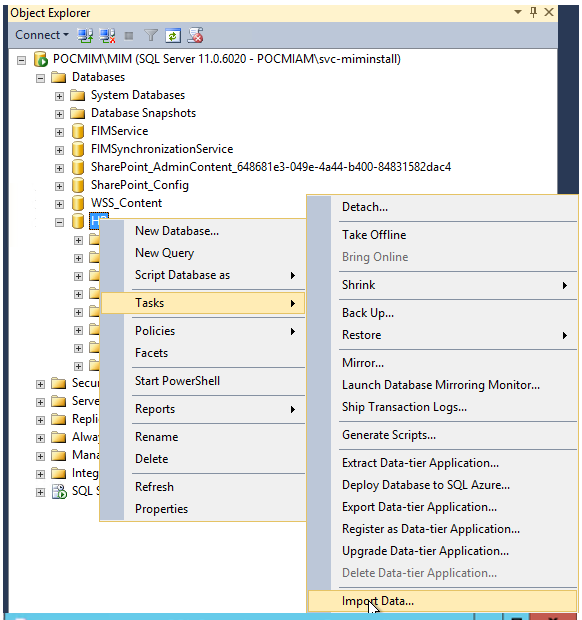
3.2 CREATE HR DATABASE AND IMPORT YOUR HR DATA

In this lab, I first create a HR CSV file with all information about my users.
You can use the solution provided here:
http://msreport.free.fr/articles/GenerateCSV.zip
The script *CreateCSV-V6.ps1* generates the HR CSV file with a specified number of random users.
You can also define the number of entity.
Each entity has a level 1 manager, a few level 2 managers and standards internal or external users.
The PowerShell script uses data of several files to generate information of the users.

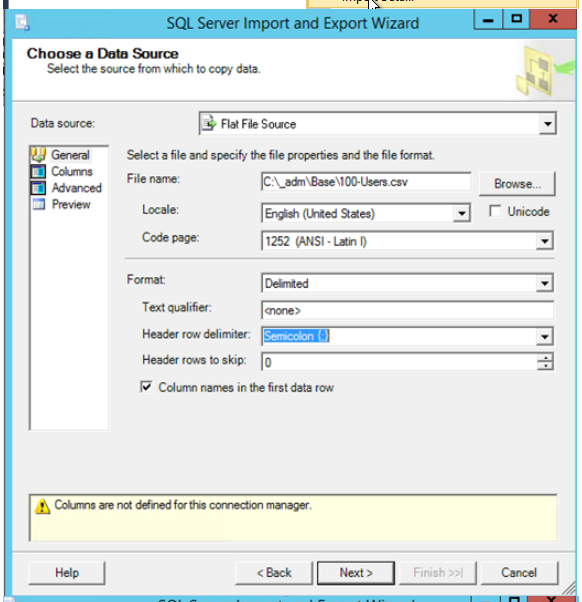
Pay attention to the name of each column (rename it if necessary). Then, you need to create a new table and import this file in a SQL table.



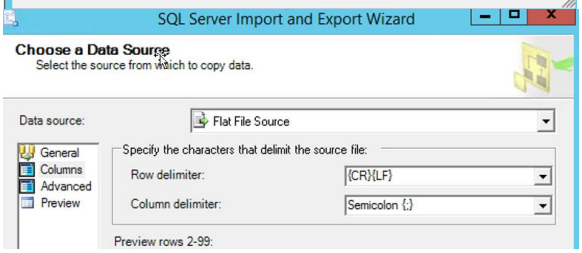
Create the HR SQL Server database.



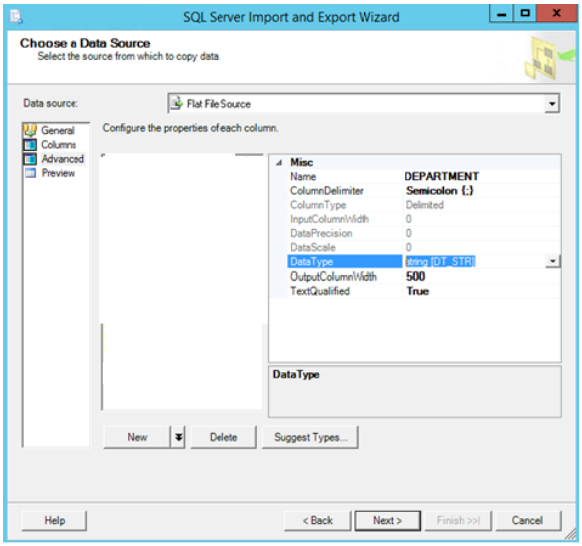
Import the CSV as a new table.



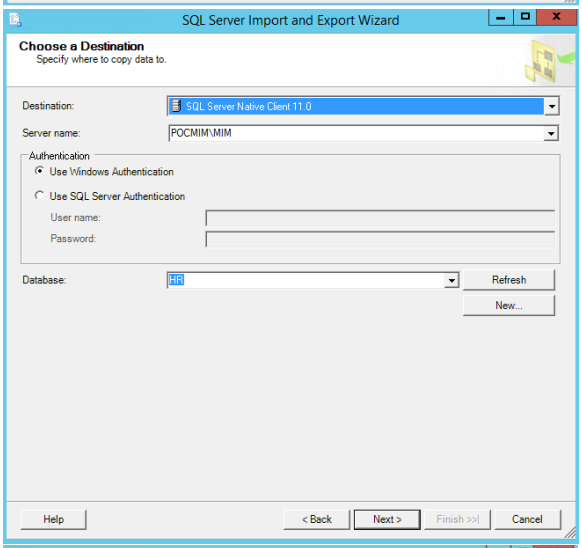
Text qualifier: *semicolon*



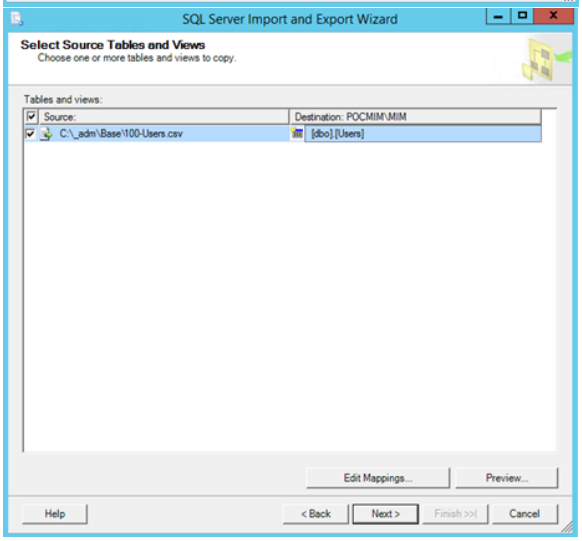
Click on *Advanced* Tab.



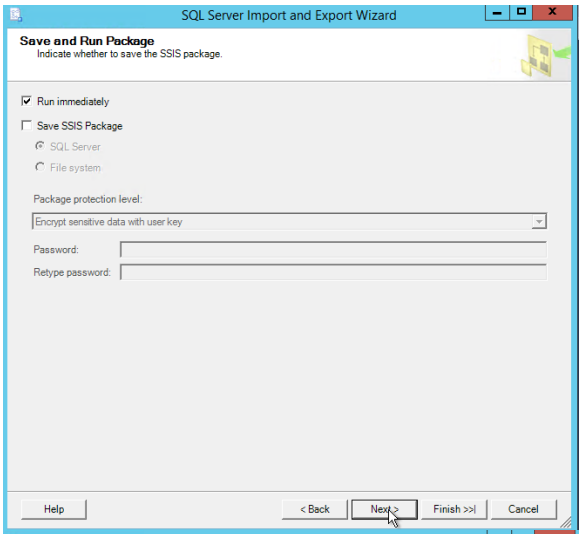
Configure each attribute with string *[DT_STR]* with a value of 500 for *OutputColumnWidth*.
Perform this action for each column / attribute.



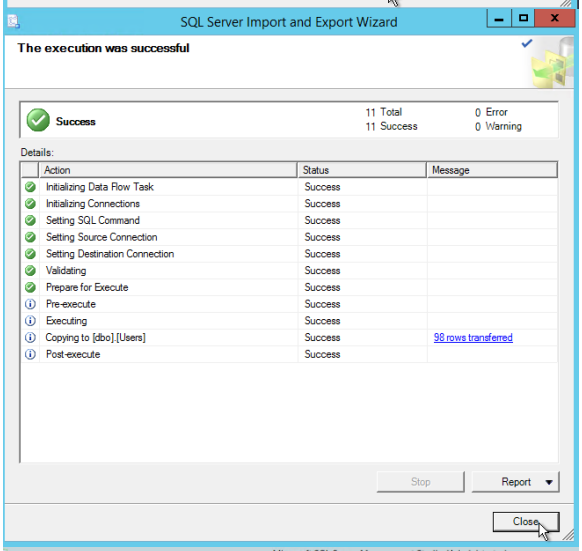
Click on *Next*.



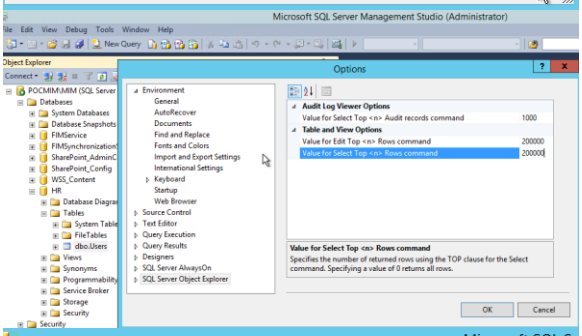
Click on *Edit Mappings* button.
Check result. All attributes must be *varchar 500*.
Click on *Next*.



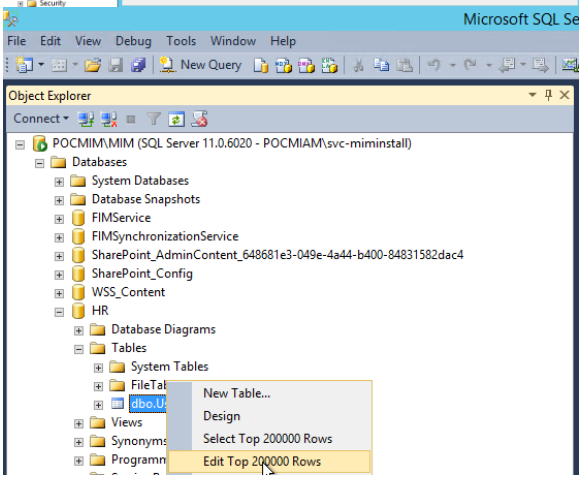
Click on *Next*.
Click on *Finish*.



Click on *Close*.



Go to *Tools | Options*.
Enter 200000 under *Table and View options*.



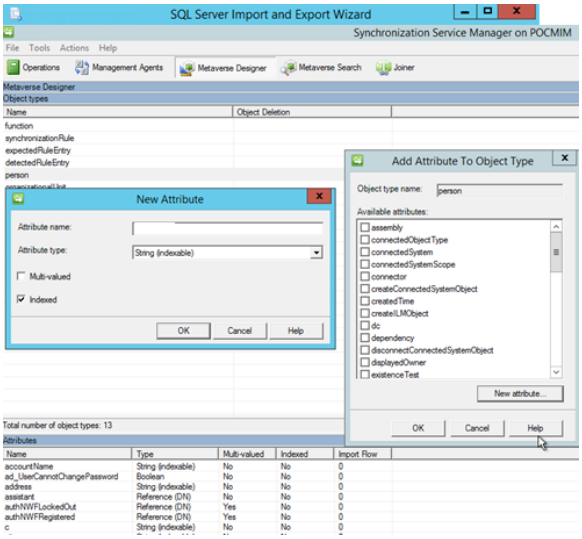
You can now edit via *SQL Server Management* tool a table with 200000 lines.

During this lab, we will directly modify this SQL table to validate behavior of the solution.

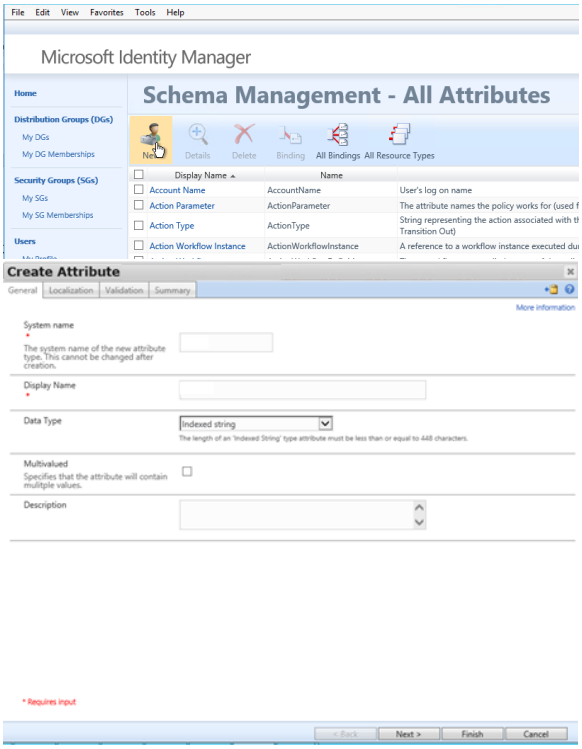
3.3 CONFIGURE LOGO

Go to the folder
C:\Program Files\Common Files\microsoft shared\Web Server Extensions\14\TEMPLATE\IMAGES\MSILM2
Rename the Logo.png as Logo-old.png.
Copy your logo.
Enter *iisreset* command.

3.4 CONFIGURE THE MIM SYNCHRONIZATION SERVICE SCHEMA AND THE MIM SERVICE SCHEMA



Add the *Global_ID* attribute (string) and index it to the class Person. Perform the same thing for attributes *EmployeeTypeMim*, *Type*, *HomeMdb*, *MsExchHomeServer* and *Domain*.

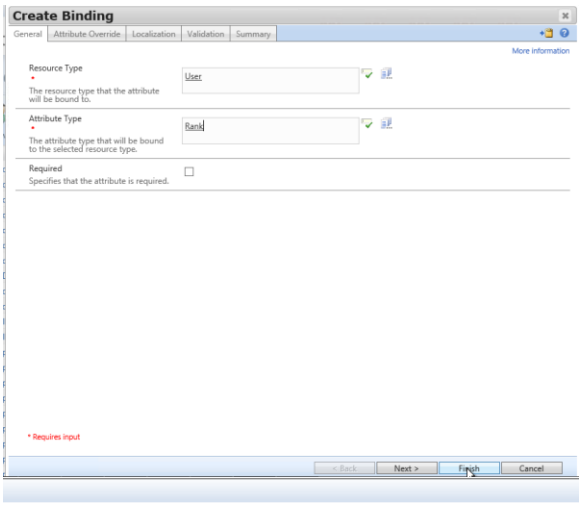


Go to MIM portal in *Administration | Schema*.
https://mimportal.pocmiam.intra/IdentityManagement/aspx/schema/AllAttributeDescriptions.aspx

Create the *Global_ID*, *Type*, *Domain*, *HomeMdb* and *MsExchHomeServer* attributes.

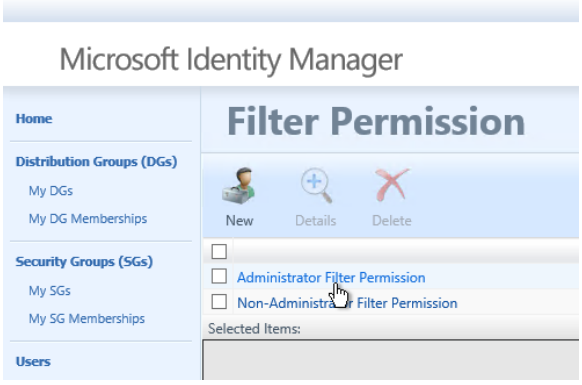
All these attributes must be string and be indexed.

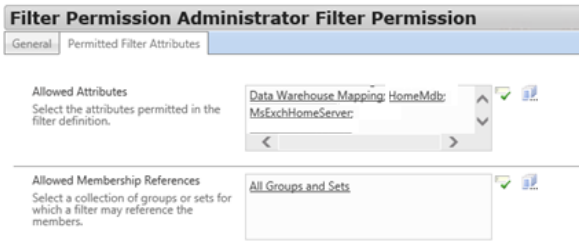
Click on *Finish* and then *Submit*.



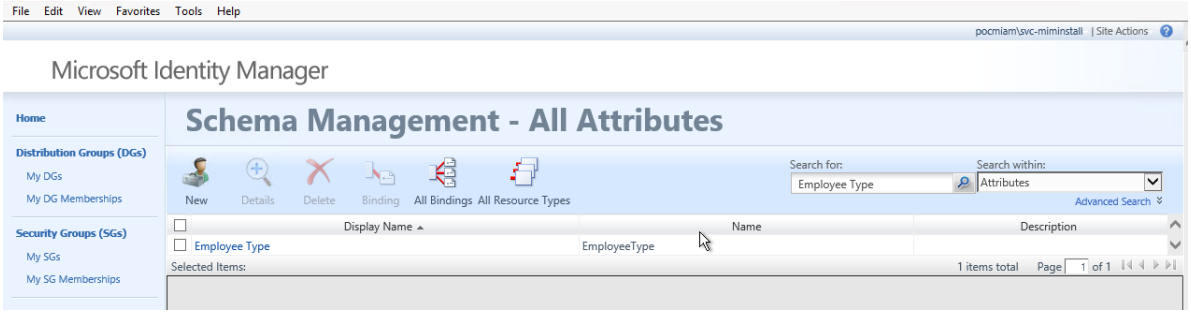
Create all bindings.
Assign each new attribute to the class *Person*.
https://mimportal.pocmiam.intra/IdentityManagement/aspx/schema/AllBindingDescriptions.aspx

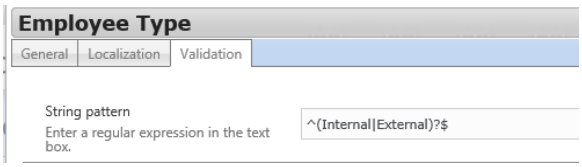
Configure the filter permission to allows administrators and non-administrators to use these new attributes (*Global_ID*, *Type*, *Domain*, *HomeMdb* and *MsExchHomeServer*) as filter.





Perform this action for administrator filters and for non-administrator filters.

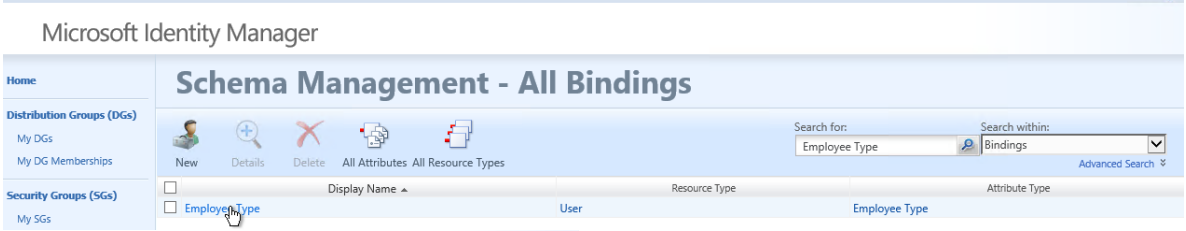


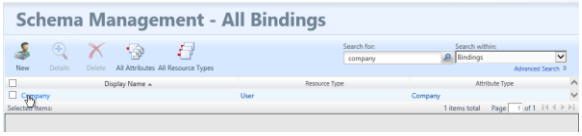


Configure EmployeeType attribute and EmployeeType binding to allow the following values : *Internal* and *External*.

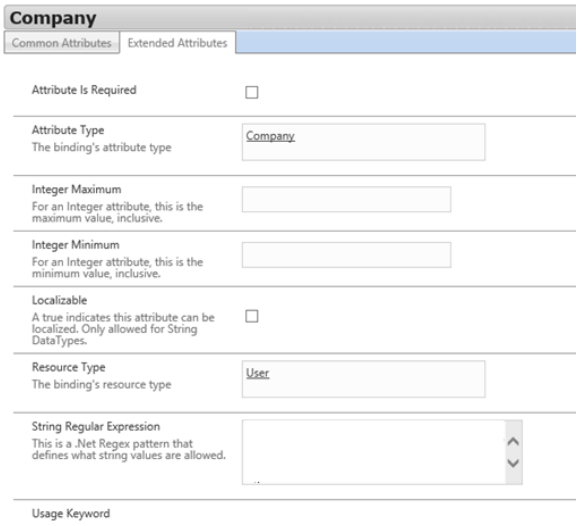
String pattern :
^(Internal|External)?$

Perform the same thing on the *Employee Type* binding.





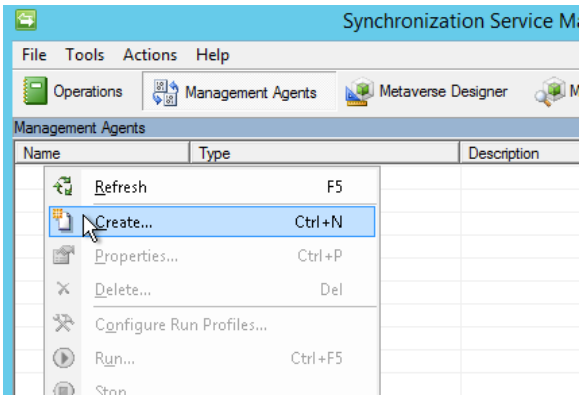
We need now to configure the list of companies. Go to *Administration | Schema Management* and click on *Bindings*.



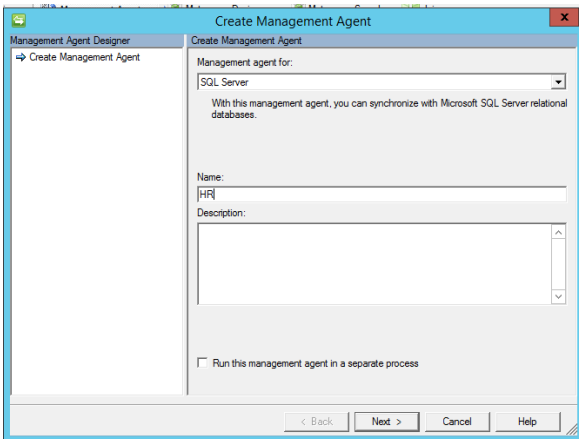
Go to advanced view and enter the following value in String regular Expression.
^(ENTITY1|ENTITY2|ENTITY3)?$

Start *IISRESET* in a command prompt to apply the change on MIM 2016 portal.

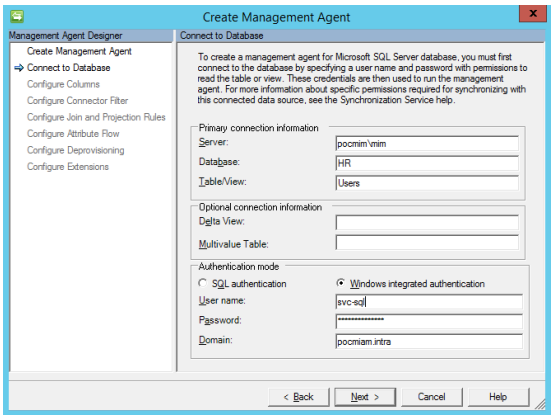
3.5 CREATE THE HR MANAGEMENT AGENT (SQL SERVER) IN MIM SYNCHRONIZATION SERVICE



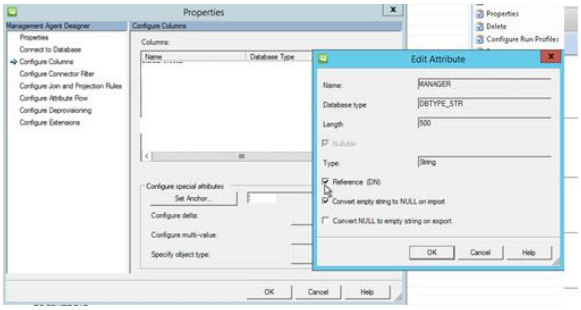
Start the console MIIS.EXE (*Synchronization Service*).



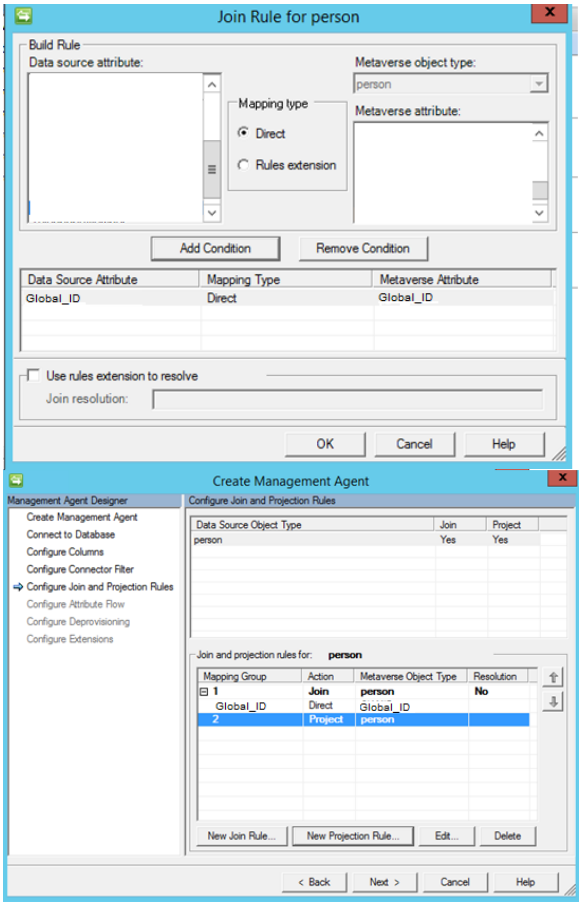
Create a SQL Server Management Agent named *HR*.



Enter the information to connect to the SQL Server database / table.
Click Next.
Define *Global_ID* as source anchor (set anchor button).



Select the attribute *MANAGER* and click on button *Edit*.
Configure as *MANAGER* as *Reference (Dn)* attribute.

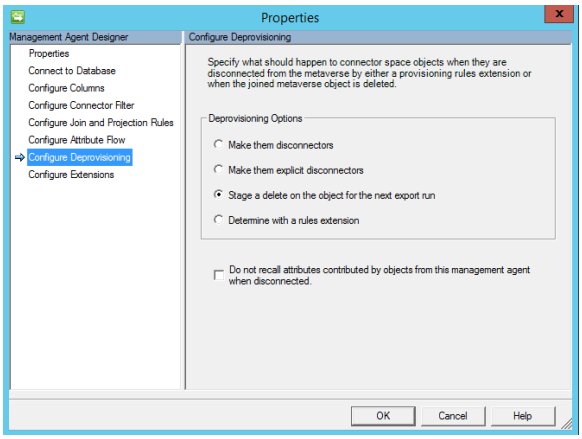


All user without a valid *Global_ID* will become disconnector.

Use the *Global_ID* as join rule.

Click on *New projection rule* and select *Person* as Metaverse Object type.

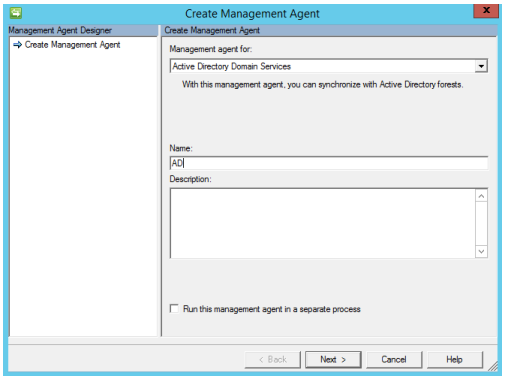
In the tab "Configure Attribute flow", configure no attribute flow. We will use a MIM service synchronization rule to replicates HR data to the Metaverse.



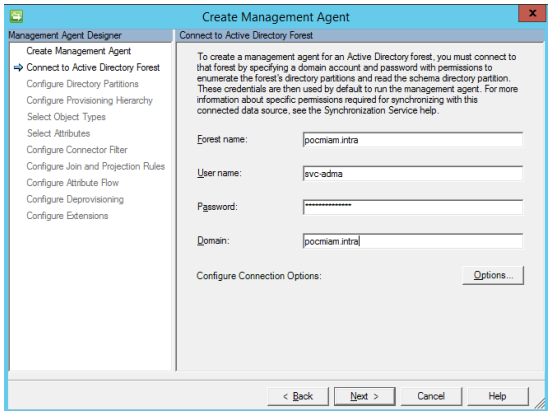
Select *Stage a delete on the object* for the next export run.

On the tab "Configure extensions", click on *Finish* button.

3.6 CREATE THE ACTIVE DIRECTORY MANAGEMENT AGENT

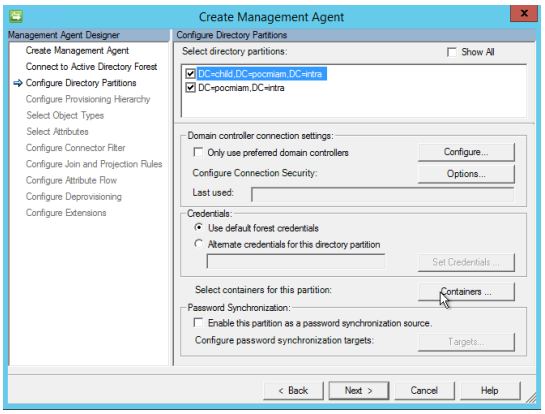


Create a new Active Directory Management Agent named *AD*.



Use the account *pocmiam\svc-adma* to connect to Active Directory forest.

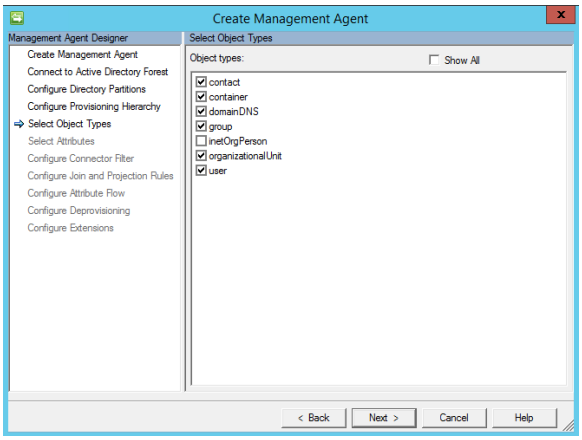
We have defined previously Active Directory permissions in the 2 domains for this service account.



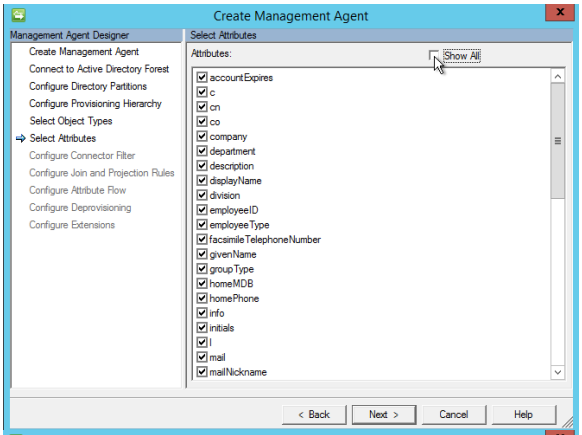
Click on *Containers* button.
Select only OU corresponding to each HR entities.

In the *Select Containers* windows, select for each entity root OU, the OU *Groups*, *Disabled_Users* and *Users*. Perform this operation for the 2 domains. Click on Next button.

In configure Provisionning hierarchy, click on Next.



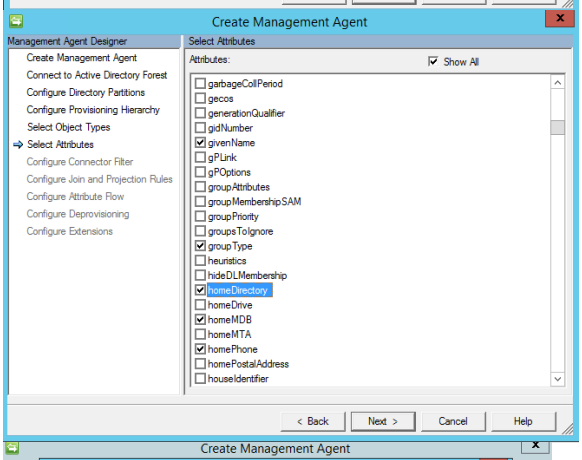
Keep existing object classes.
Select *contact*, *user* and *group* object.



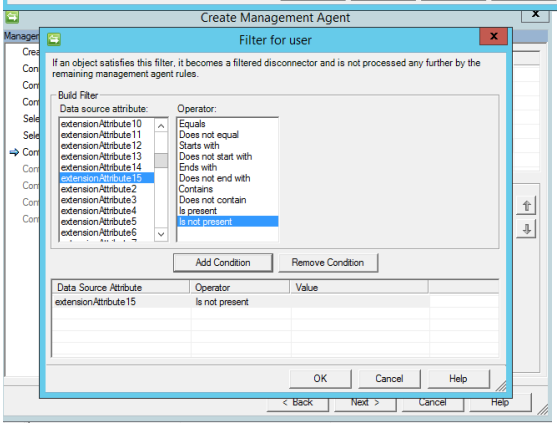
You must have prepare your schema for Exchange.

Select all default attributes.
Click on *Show all* box.
Select *ObjectSid*.

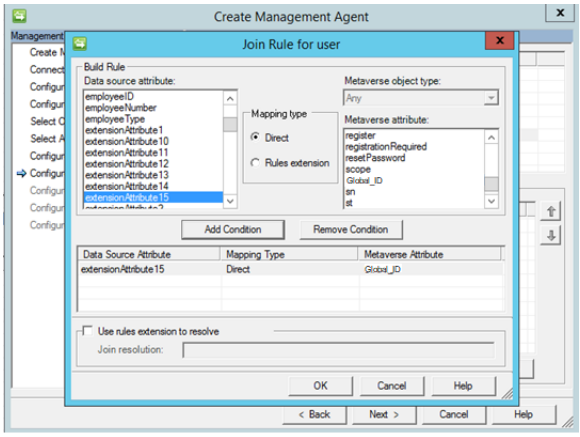
Select also all attributes used in this lab and add also attributes required for Exchange 2013 like *HomeMdb*, *MsExchHomeServer*



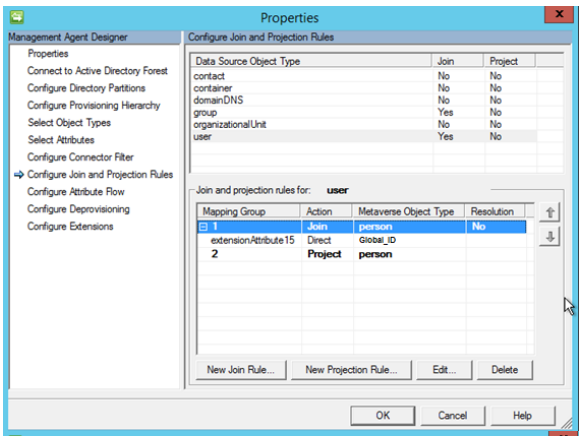
Add also attributes related to password and group management:
Unicodepwd
Pwdlastset
GroupType



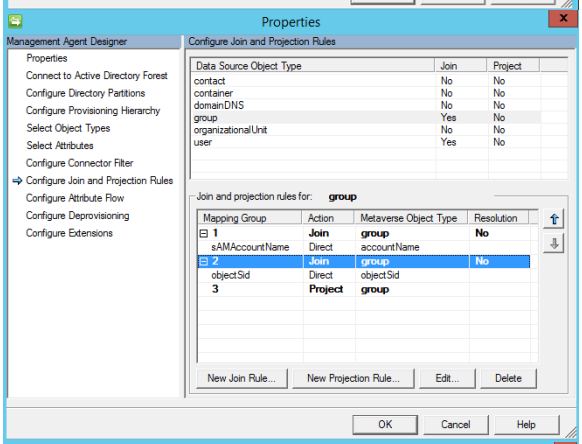
Configure as disconnector each user without *ExtensionAttribute15*. This attribute will store the Global_Id.



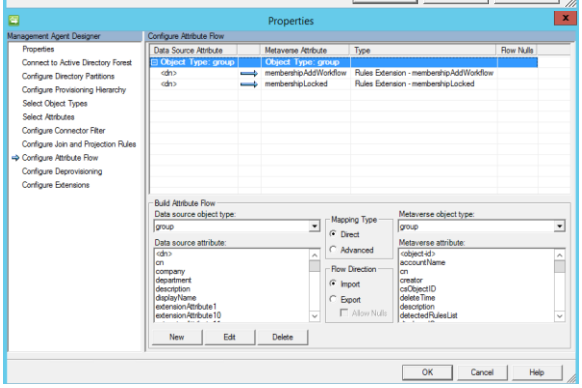
Configure ExtensionAttribute15 and Global_ID as join rule.



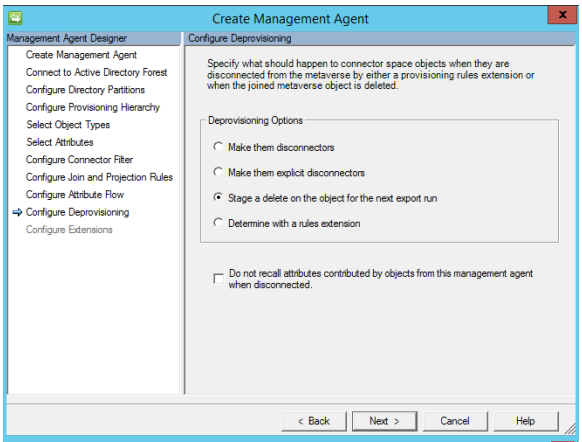
Configure user join and projection rules.



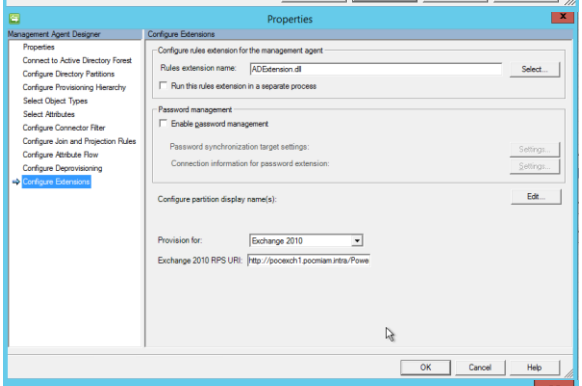
Configure group join and projection rules.



Define 2 advanced rules used for group synchronization.

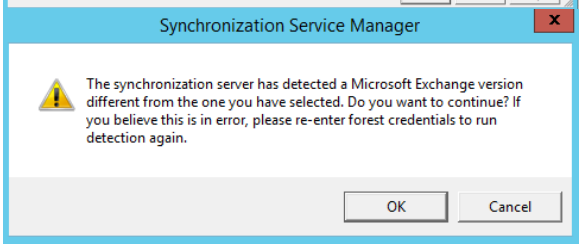


Select *Stage a delete on the object for the next export run*.



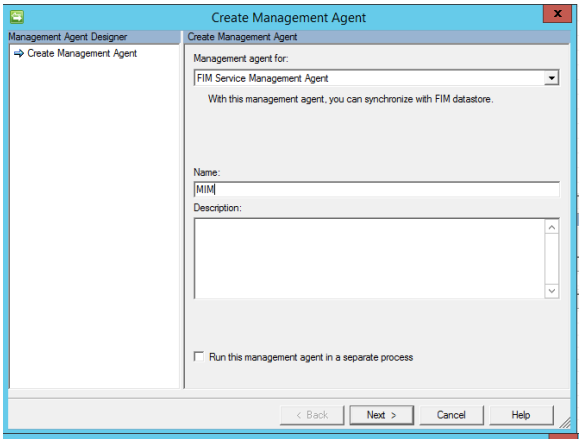
Select Provision for Exchange 2010 (based on your version).
http://pocexch1.pocmiam.intra/powershell

We will use a custom rule extension for group synchronization between Active Directory and the MIM 2016 portal.

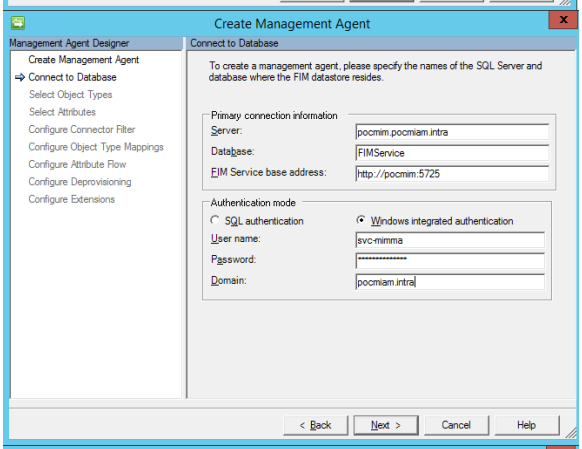


Click on the button *OK*.

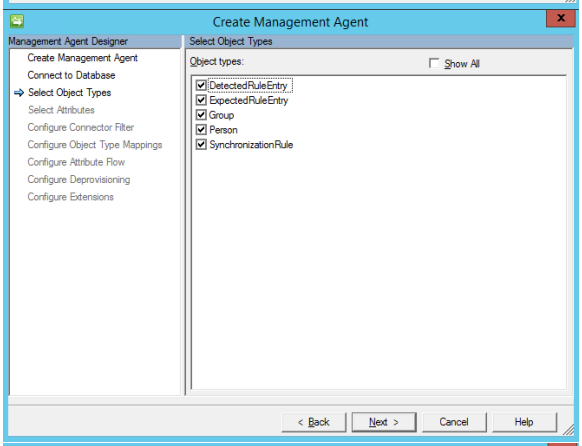
3.7 CONFIGURATION DU MANAGEMENT AGENT FIM SERVICE



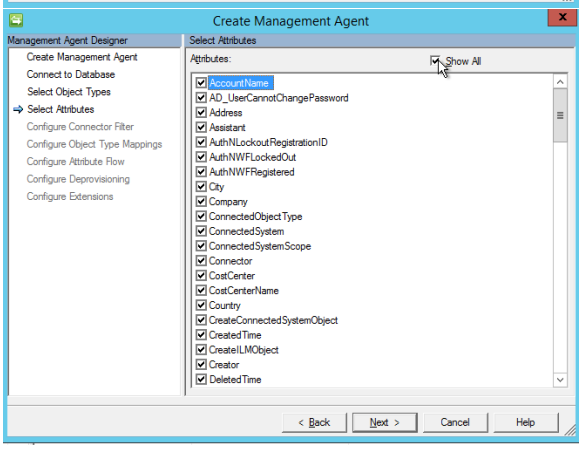
Create a *FIM service Management Agent* named *MIM*.



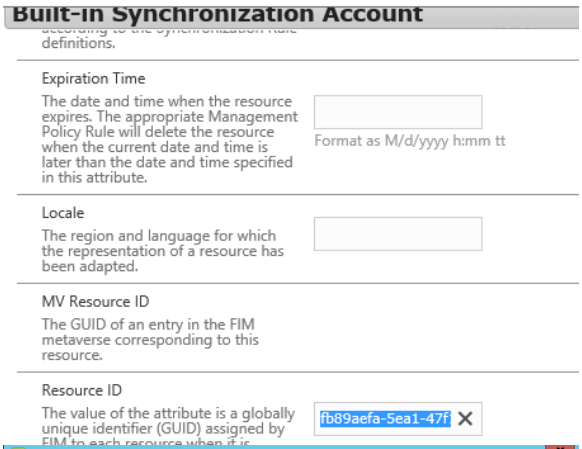
Server: *pocmim.pocmiam.intra*
Database: *FIMService*
FIM Service base address: *http://pocmim:5725*
Use the account *pocmiam\svc-mimma*.



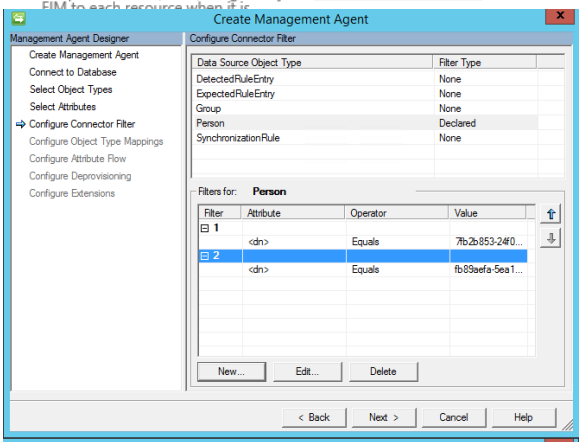
Add the *Group* and *Person* classes.



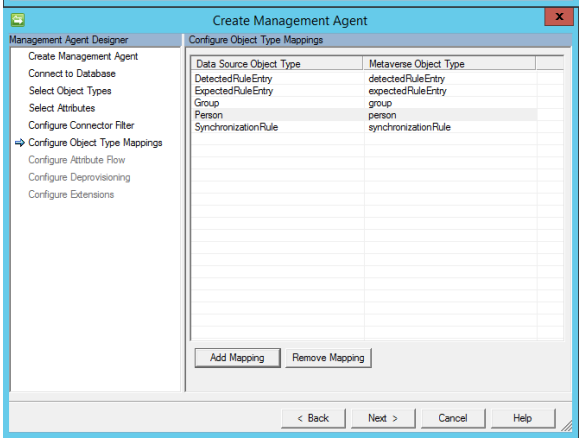
Select all attributes.



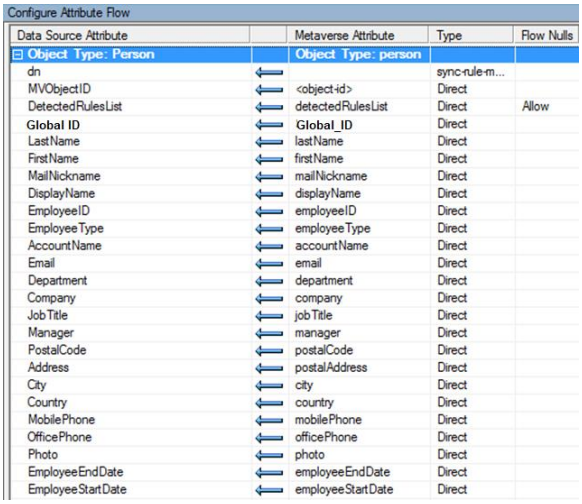
Filter resource based on *Resource ID* for person. We need to avoid the MIM service default administrative account to replicate to the Metaverse.



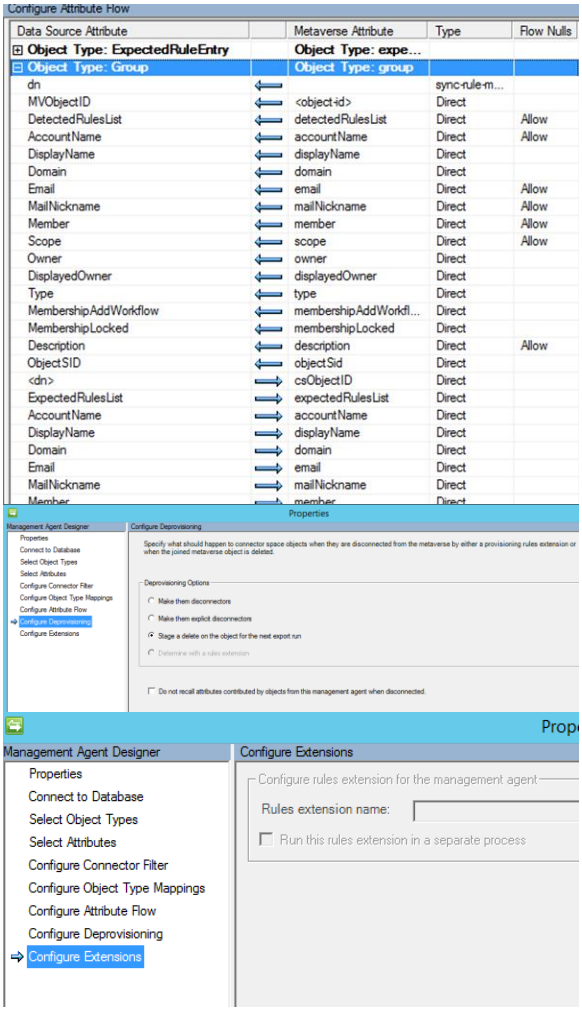
Configure the following filter
DN equals to *7fb2b853-24f0-4498-9534-4e10589723c4*
DN equals to *fb89aefa-5ea1-47f1-8890-abe7797d6497*



Add *Group* and *Person* type mappings.



Configure the following attributes rules for *User* class.



Configure the following attributes rules for Group class.

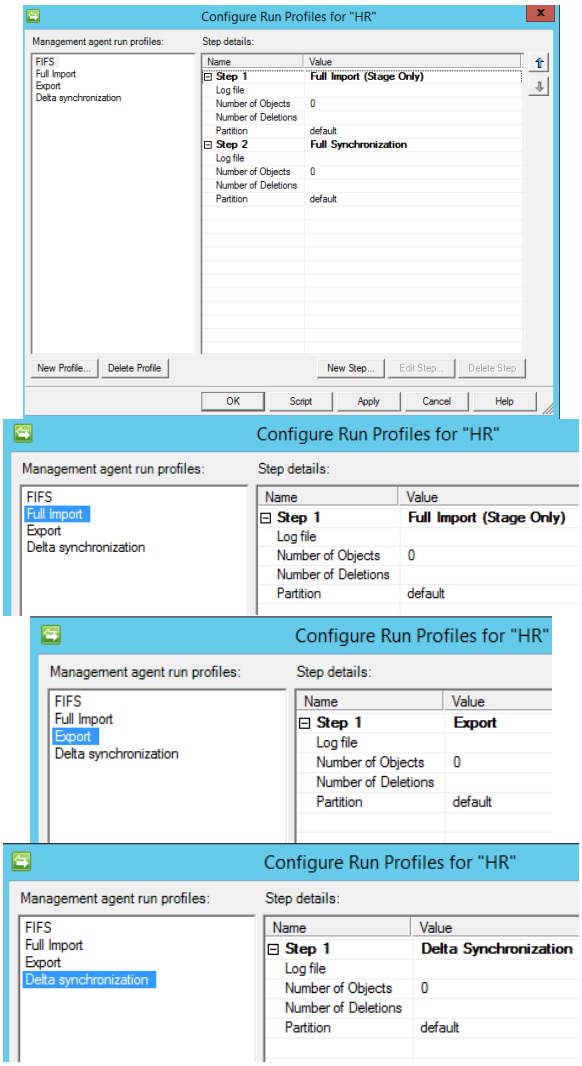
Refer to the table for the exact list of attributes to synchronize.

Select *Stage a delete*.

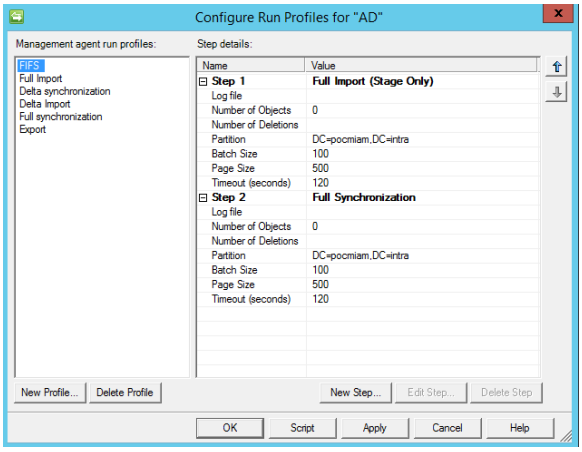
Click on *Finish*.

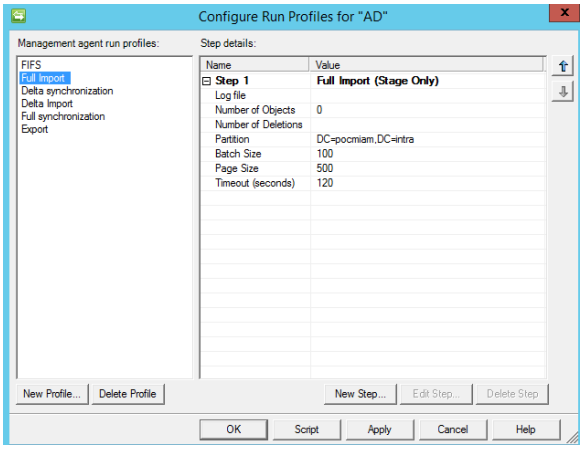
3.8 CONFIGURE THE RUN PROFILES FOR EACH MANAGEMENT AGENT

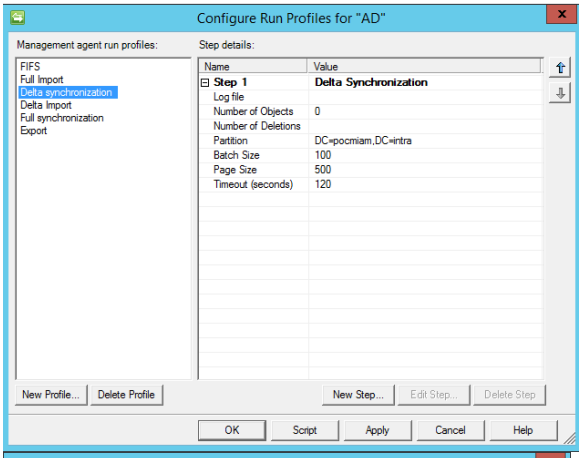
Create for the HR Management Agent the following profiles: *FIFS, Import*, *Delta Synchronization*, *Export* and *Full Import*.

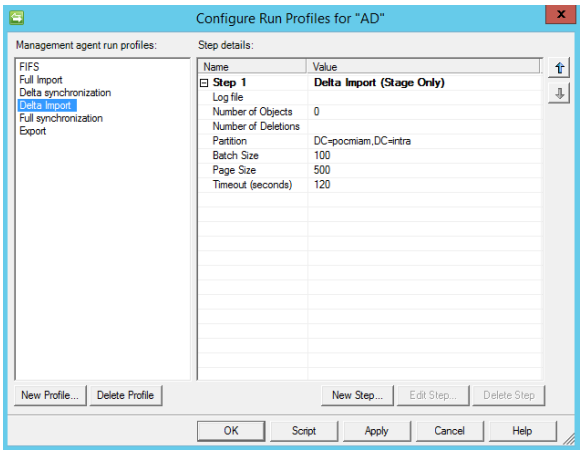


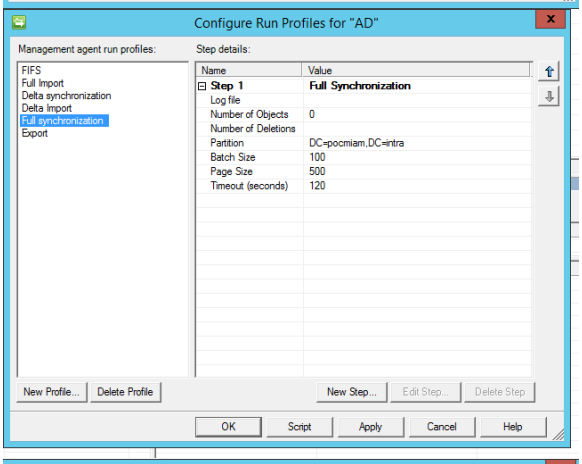
Create for the AD Management Agent the following profiles: *FIFS*, *Delta Import*, *Full Import*, *Delta synchronization*, *Full Synchronization* and *Export*.
You can limit the number of object processing and the number of deletions.

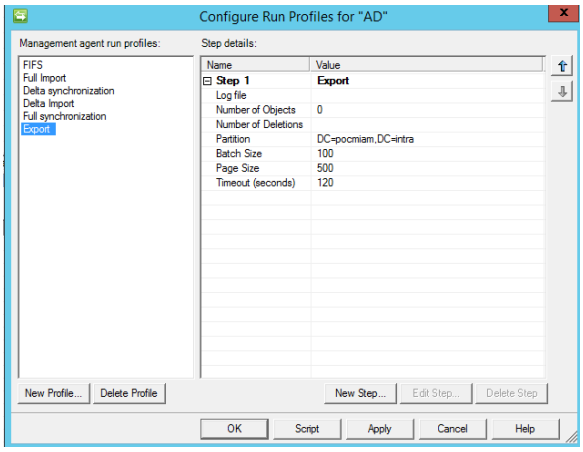


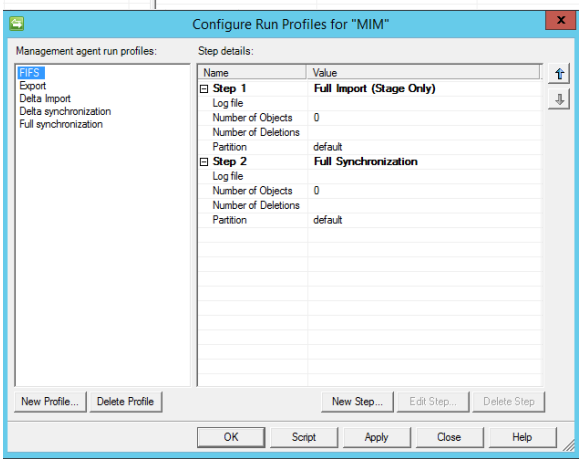










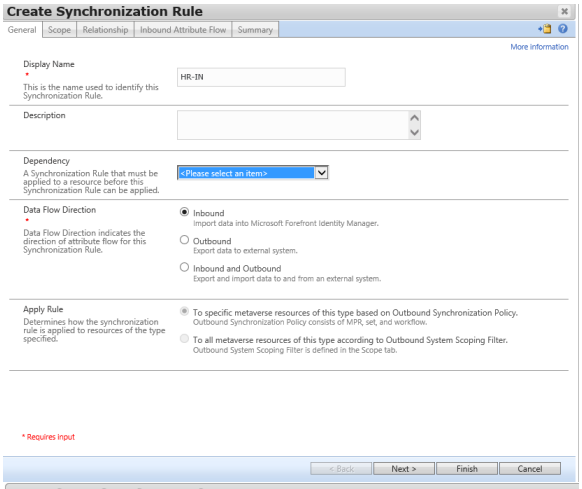


Create for the AD Management Agent the following profiles: *FIFS*, *Delta Import*, *Full Import*, *Delta synchronization*, *Full Synchronization* and *Export*.

3.9 CREATE SYNCHRONIZATION RULES

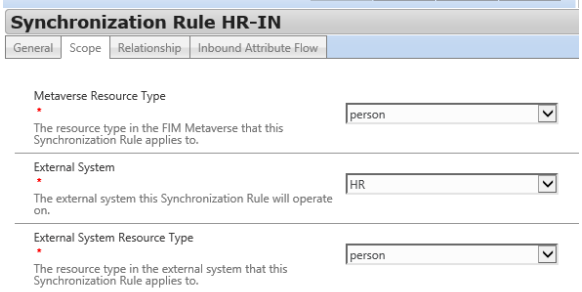
3.9.1 Create HR-IN synchronization rules

This synchronization rule allows to synchronize HR database and the Metaverse.



Enter *HR-IN*.

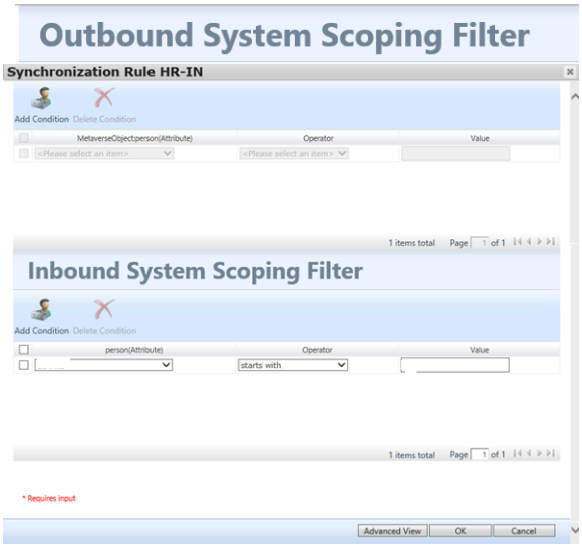
Select *Inbound*.



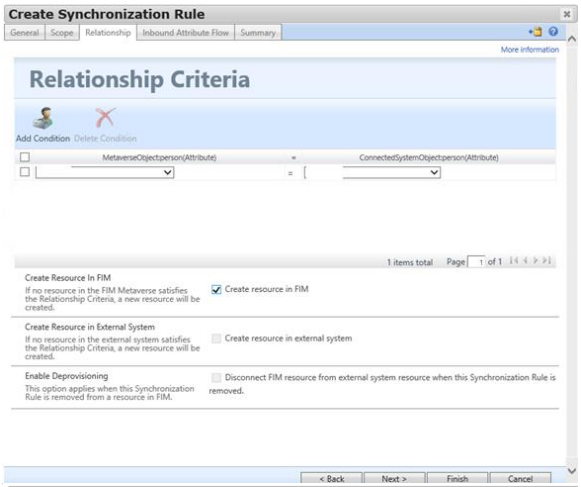
Metaverse Resource type: *person*

External System: *HR*

External System Resource Type: *person*

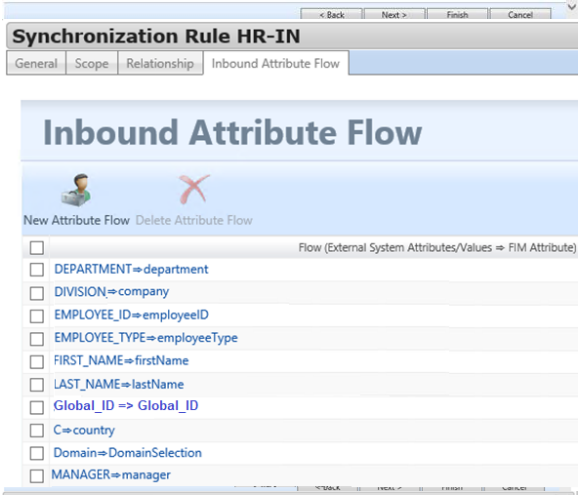


Define an *Inbound System Scoping Filter*.
Global_ID must exist / not null

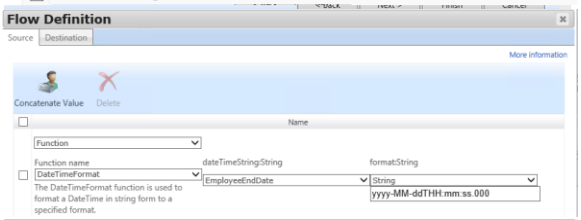


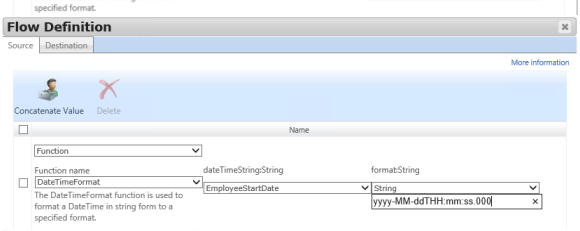
Define *Global_ID* = *Global_ID* as relationship criteria.

Check the box *Create Resource in FIM*.



Configure the mapping.
Add all attributes on which the HR database is authoritative. Refer to the tables at the beginning of this document.





You need to create an advanced flow definition to convert *Employee End Date* and *Employee Start date* (convert string to date).

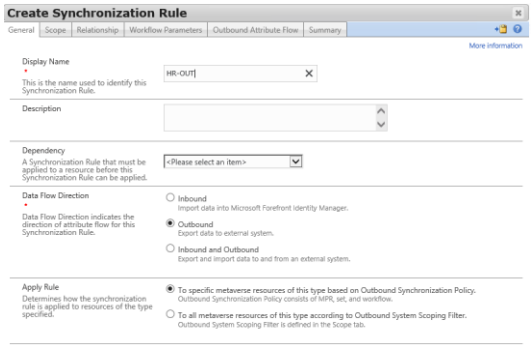
Use *Function | DateTimeFormat*.
Check the format of the date in the HR database.
Select the attribute and enter the following value in "*String"* field. IN this example:
yyyy-MM-ddTHH:mm:ss:000

This format is a prerequisite to replicate *Employee End Date* / *Employee Start date* from the Metaverse to MIM service (MIM portal).

Replication for *Employee End Date* / *Employee Start* attributes:
HR -> Metaverse -> MIM Service (MIM portal)

3.9.2 Create HR-OUT synchronization rule

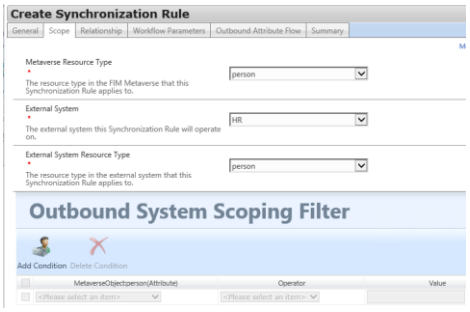
This synchronization rule allows to update HR database from MIM portal via the FIM Metaverse attributes *mobile*, *telephoneNumber* and *EmployeeTypeMim*.



Enter HR-OUT.

Select Outbound.

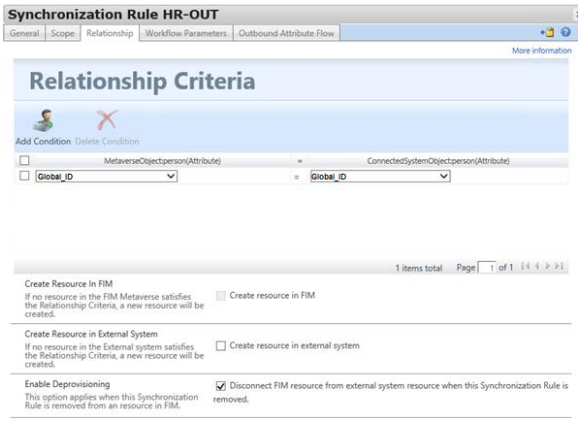
Select *To a specific Metaverse resources of this type based on Outbound Synchronization Policy*.



Metaverse Resource Type: *person*

External System: *HR*

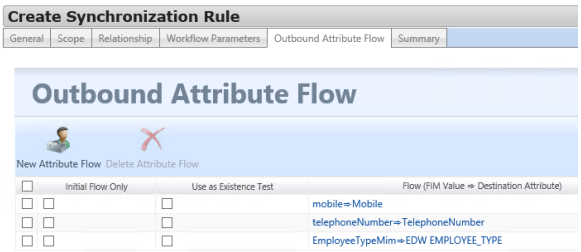
External System Resource Type: *person*



We want only perform update or delete in the SQL database (HR).

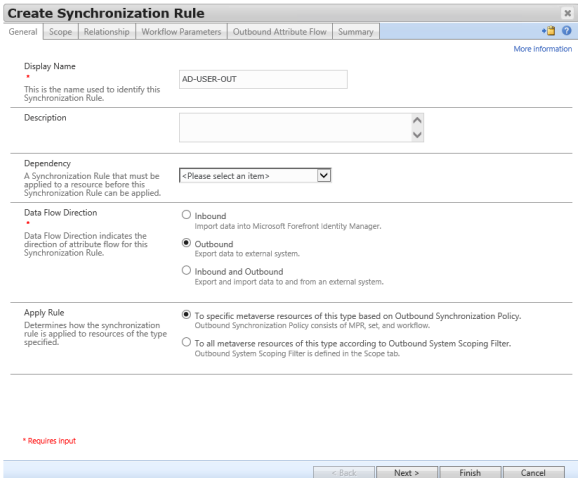
That's why we need to only check the box *Disconnect FIM resources from external system resource when this Synchronization Rule is removed*.

Click *Next*.

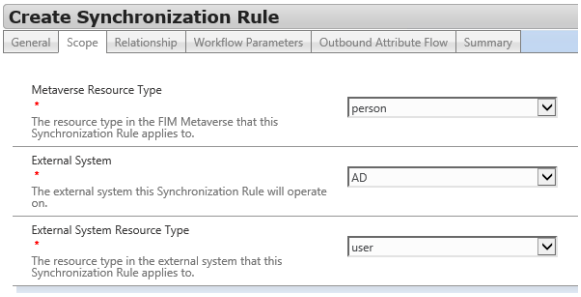


Only 3 attributes are replicated to HR database from the Metaverse.
In the Metaverse, we have also the attributes *MobilePhone*, *Office Phone*, and *EmployeeType*.
The use of the attributes *mobile*, *telephoneNumber* and *EmployeeTypeMim* allows to change the fields *Employee Type*, *Mobile phone* and *Office phone* from both HR and MIM 2016 portal.
In case of conflicts, the last change wins.

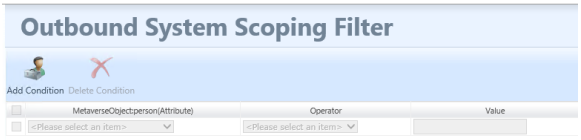
3.9.3 Create the synchronization rule AD-USER-OUT

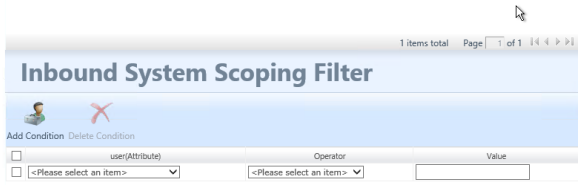


Name: *AD-USER-OUT*
Data flow Direction: *Outbound*.
Apply Rule: *to specific Metaverse resources of this type based on Outbound Synchronization Policy*

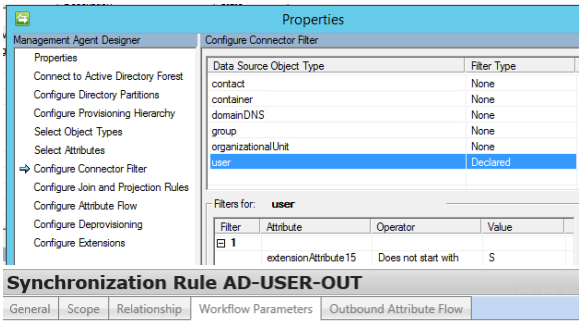


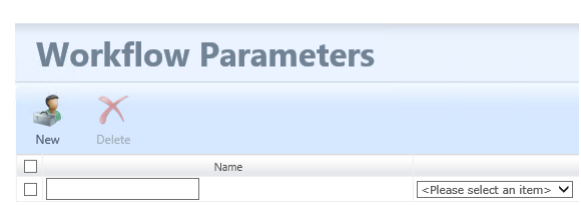
Metaverse Resource type: *person*
External System: *AD*
External System Resource Type: *user*



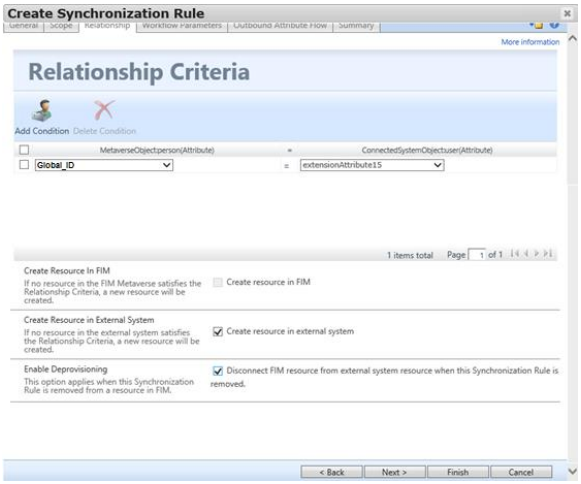


Don't define filter in the synchronization rule. We will use the filter defined on the *AD* management agent instead.



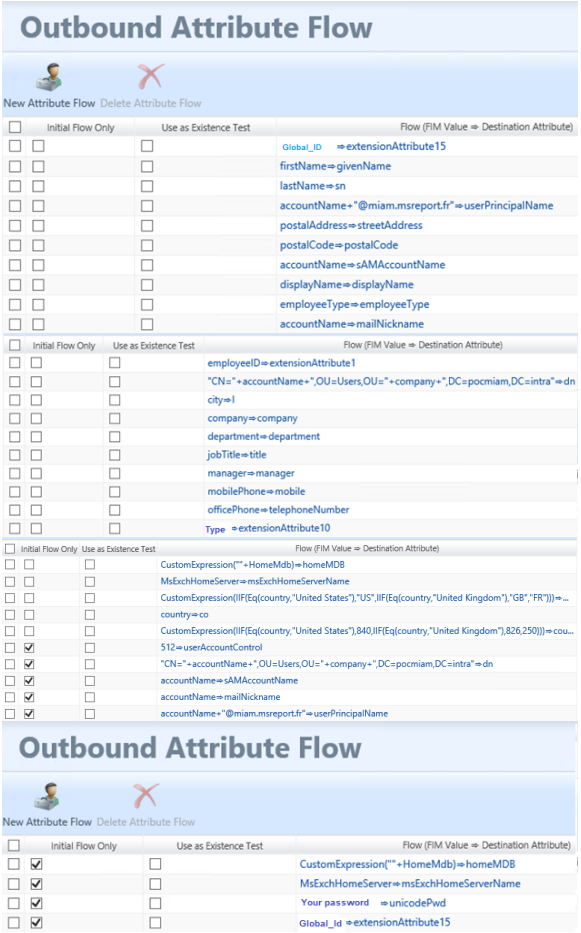


Do not define workflow parameters.



Global_ID / *ExtensionAttribute15* will be used as Relationship Criteria.

Check the boxes *Create resource in external system* and *Disconnect FIM resource from external system resource when this synchronization rule is removed*.

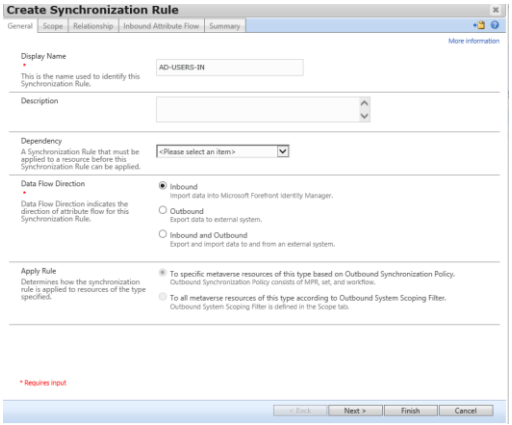


Notes:
The Metaverse attributes *Mobile* and *MobilePhone* will both update Active Directory *Mobile* attribute. We will use a custom synchronization rule to generate *C* and *CountryCode* Active Directory attributes based on *Country* Metaverse attribute. http://ithinkthereforeidam.com/synchronizing-country-from-fim-to-ad/

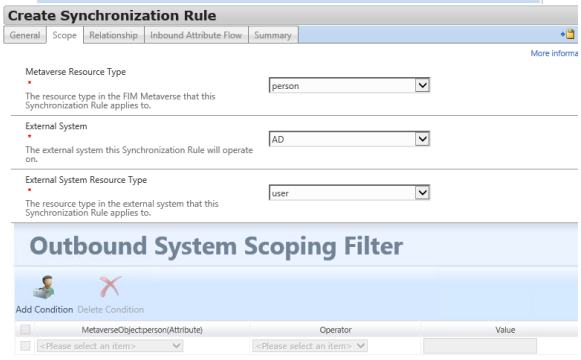
This attribute is populated from HR database via the synchronization rule HR-IN.
IIF(Eq(country,"United States"),840,IIF(Eq(country,"United Kingdom"),826,250))
IIF(Eq(country,"United States"),"US",IIF(Eq(country,"United Kingdom"),"GB","FR"))

Other solution:
Word(Word(ReplaceString("|United States|US|United Kingdom|GB|France|FR|","|"+country+"|",""),2,"*|"),1,"|")*

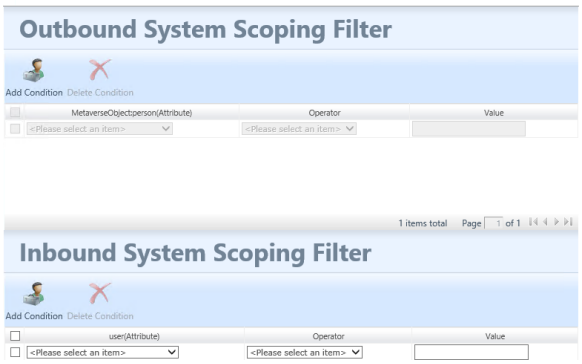
3.9.4 Create the synchronization rules AD-USERS-IN



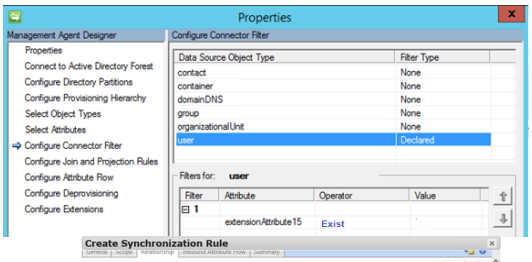
Name: *AD-USERS-IN*
Data Flow Direction: *Inbound*

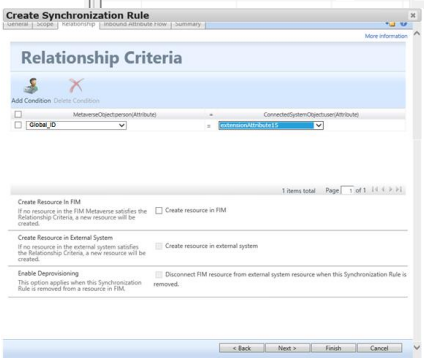


Metaverse Resource Type: *person*
External System: *AD*
External System Resource Type: *user*

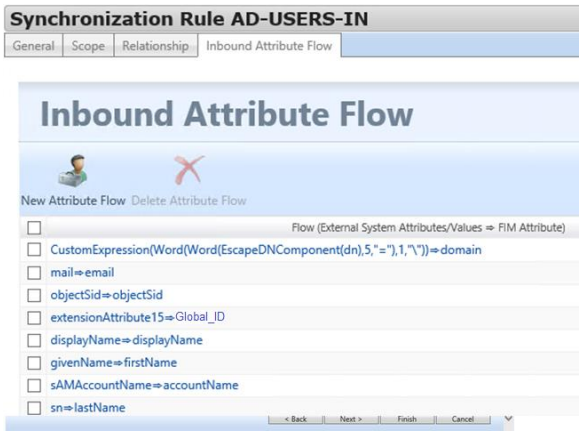


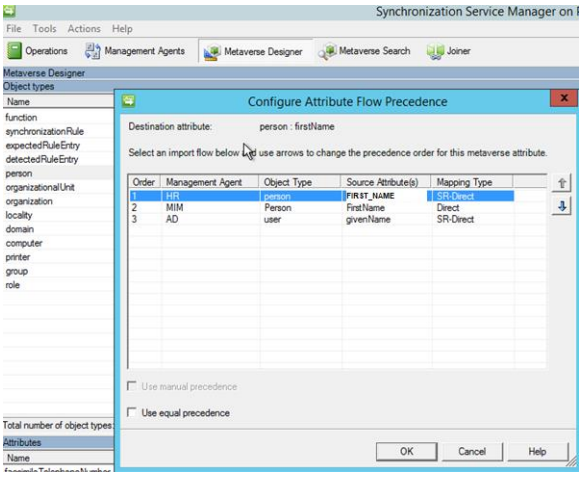
Do not use filter on this synchronization rule. We will use the filter defined on the AD management agent instead.





Do not create new user with this rule, only update.





To generate domain:
Word(Word(EscapeDNComponent(dn),5,"="),1,"\")

It's mandatory to copy ObjectSID, domain to allow user to connect to the MIM 2016 portal.

It's mandatory to import *ExtensionAttribute15* (Global_ID) to allow existing user account to be created on the MIM portal even if the user account his not created / synchronized from HR database.

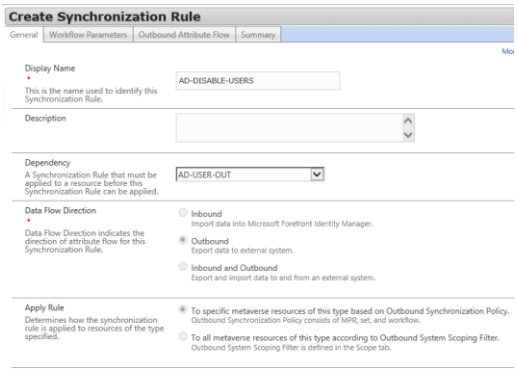
Email is generated by Exchange email address policy and is imported to MIM portal via the AD management agent.

GivenName, Sn, SamAccountName and *DisplayName* will be imported to the Metaverse but will not be replicated to others target system because of rule precedence.

HR is the main source of authority for *GivenName* and *Sn*.

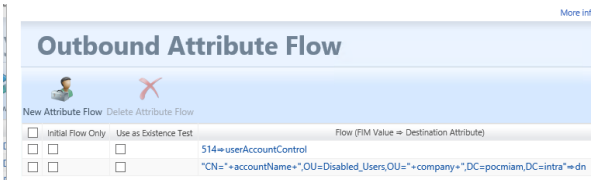
MIM portal is the main source of authority for *DisplayName* and *SamAccountName* attributes.

3.9.5 Create the synchronization rules AD-DISABLE-USERS

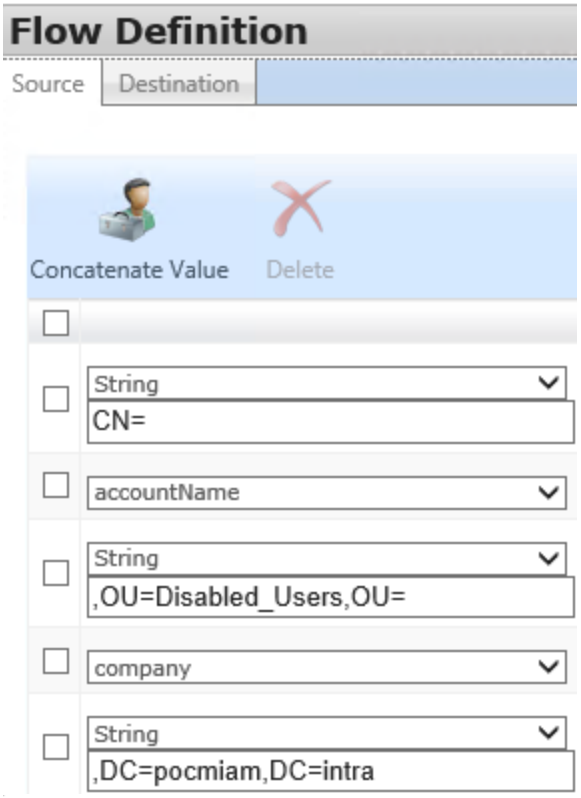


Enter the name *AD-DISABLE-USERS*.

Select dependency *AD-USER-OUT*.

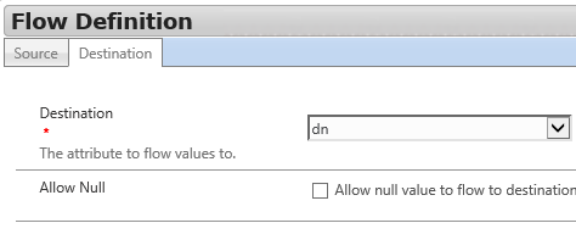


The main goal of this synchronization rule is to disable and move users in the OU *Disabled_users* of each entity.
Click on button *Submit*.

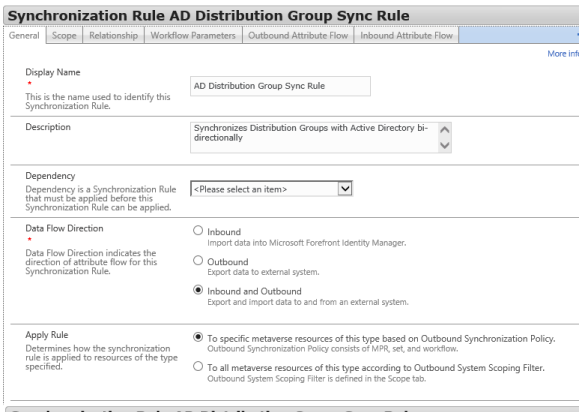


Change the DN of an object allows to move the object.

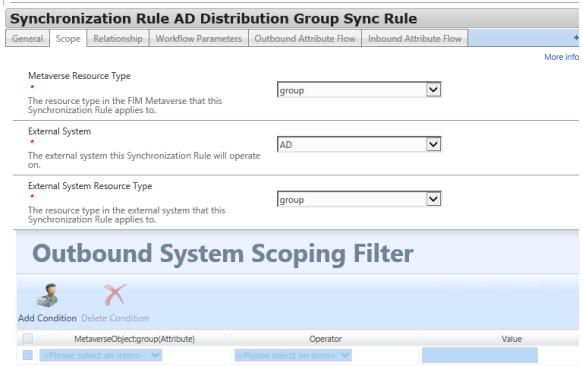
The rule to generate DN is based on the accountName and company attributes of the Metaverse.



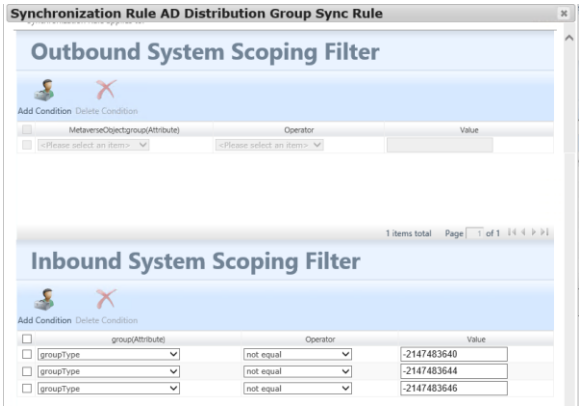
3.9.6 Create the synchronization rule for distribution group



Display Name: *AD Distribution Group Sync Rule*.
Data Flow Direction: *Inbound and Outbound*

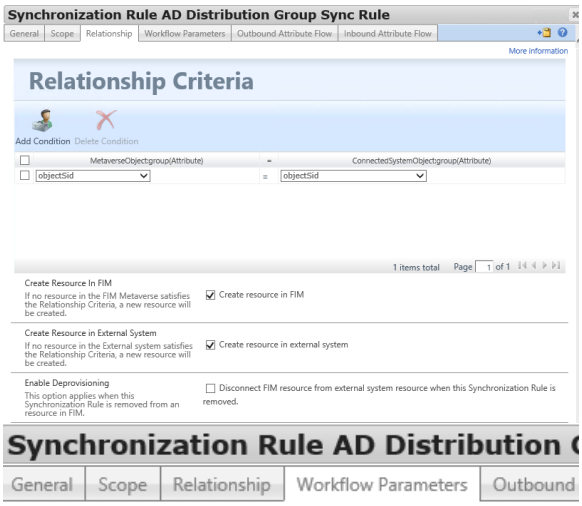


Metaverse Resource Type: *group*
External System: *AD*
External System Resource Type: *group*



GroupType attribute in Active Directory allows to define the type of a group.
We need to filter local security, global security and universal security groups.
https://blogs.technet.microsoft.com/heyscriptingguy/2004/12/21/how-can-i-tell-whether-a-group-is-a-security-group-or-a-distribution-group/

Value	GroupType
2	Global distribution group
4	Domain local distribution group
8	Universal distribution group
-2147483646	Global security group
-2147483644	Domain local security group
-2147483640	Universal security group

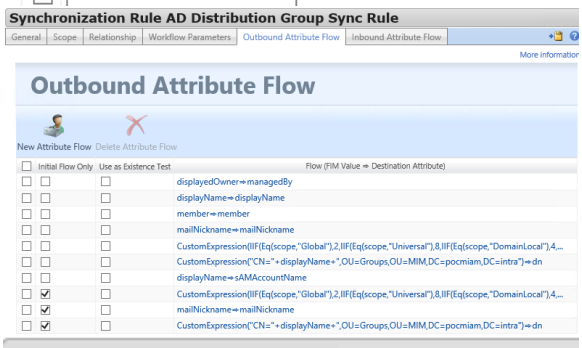


Select *ObjectSID* as relationship criteria.

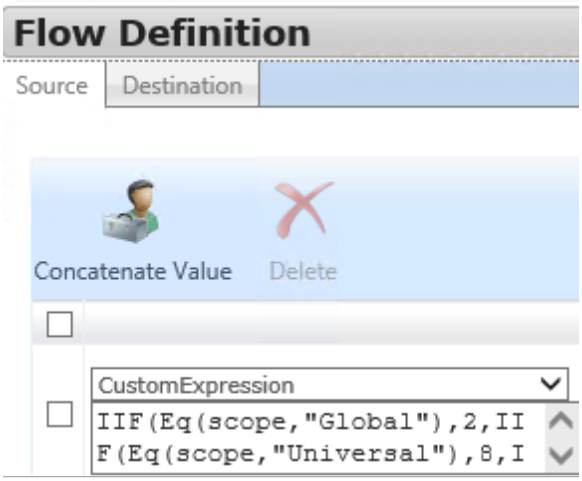
Use of this attribute will allow to rename group both from Active Directory and from MIM 2016 portal.

Check the boxes *Create resource in FIM* and *Create resource in external system*.

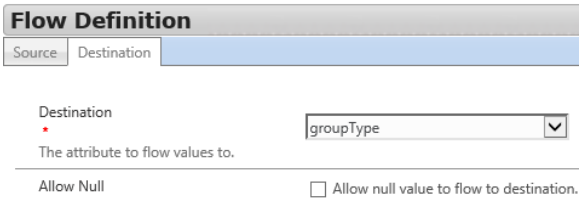
We will not use workflow parameters.

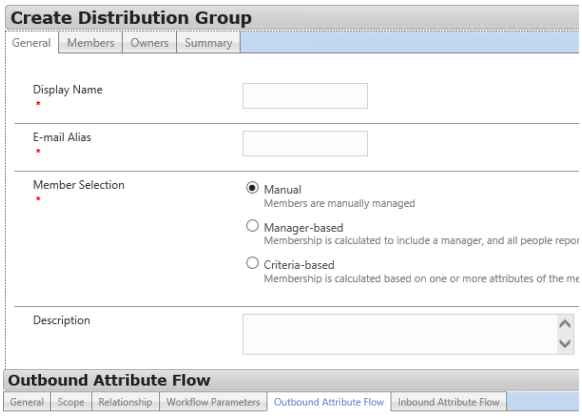


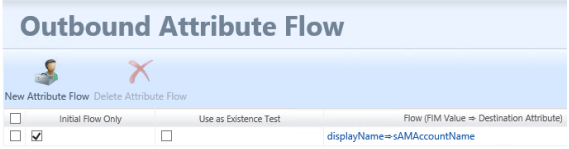
We will use the following rule to generate the DN attribute:
"CN="+displayName+",OU=Groups,OU=MIM,DC=pocmiam,DC=intra"



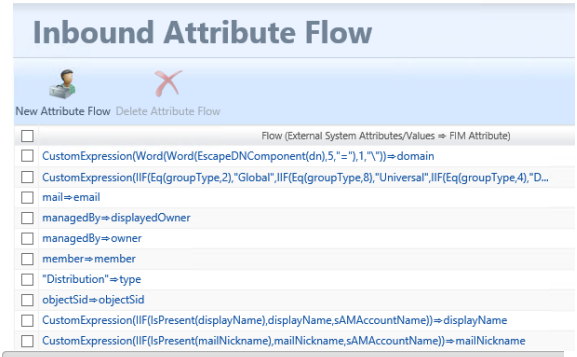
We will use this rule to generate Active Directory *groupType* attribute:
IIF(Eq(scope,"Global"),2,IIF(Eq(scope,"Universal"),8,IIF(Eq(scope,"DomainLocal"),4,"")))







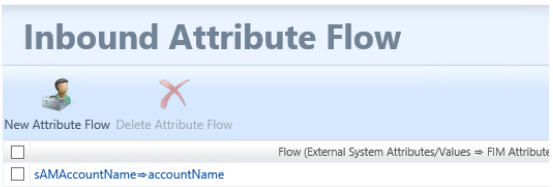
The MIM 2016 creation distribution group form doesn't display accountName attribute. That's why we will use Metaverse *DisplayName* attribute to generate Active Directory *SamAccountName* attribute.



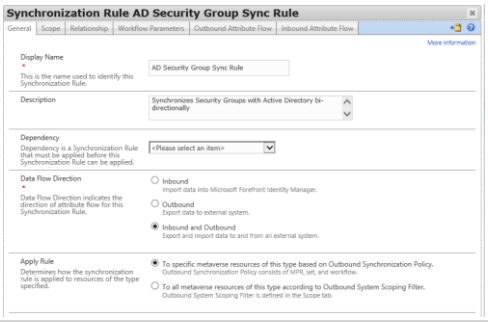
This rule will be use to generate the name of the domain:
Word(Word(EscapeDNComponent(dn),5,"="),1,"\")
We will use Active Directory attribute *displayName* or the attribute *SamAccountName* (if *displayName* is empty is Active Directory) to generate the Metaverse *DisplayName* attribute:
IIF(IsPresent(displayName),displayName,sAMAccountName)

We will use a similar method to generate Metaverse *mailnickname* attribute.

It's also mandatory to import *ObjectSid* which will be use as join rule.



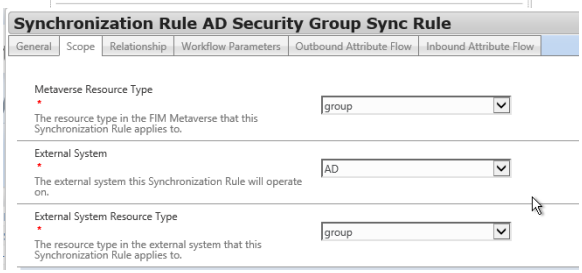
3.9.7 Create the synchronization rule for security group



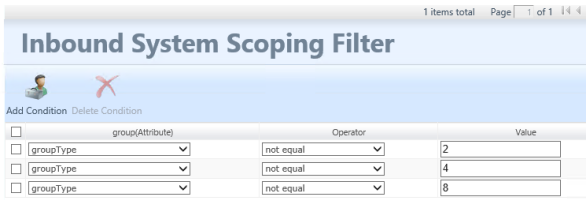
Display Name: *AD Security Group Sync Rule*

Data Flow Direction: *Inbound and Outbound*

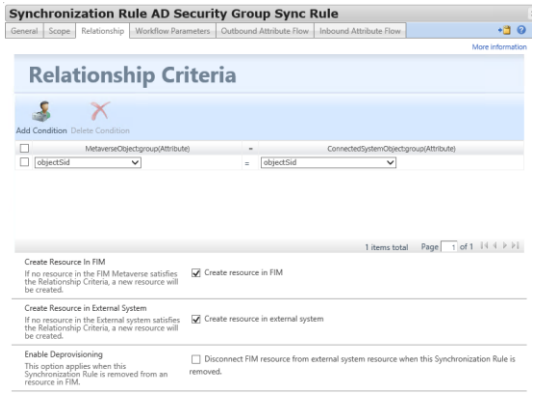
Apply rule: *to specific Metaverse resources of this type based on Outbound Synchronization Policy*.



Metaverse Resource Type: *group*
External System: *AD*
External System Resource Type: *group*

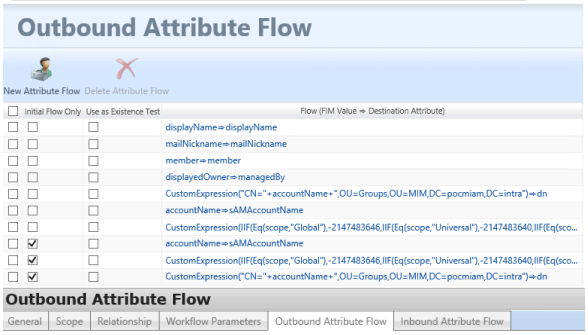


GroupType attribute in Active Directory allows to define the type of a group.
We need to filter local distribution, global distribution and universal distribution groups.
https://blogs.technet.microsoft.com/heyscriptingguy/2004/12/21/how-can-i-tell-whether-a-group-is-a-security-group-or-a-distribution-group/

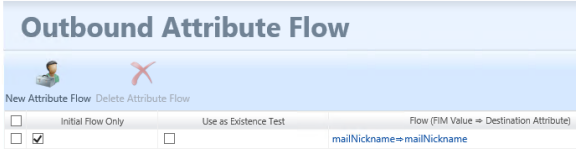


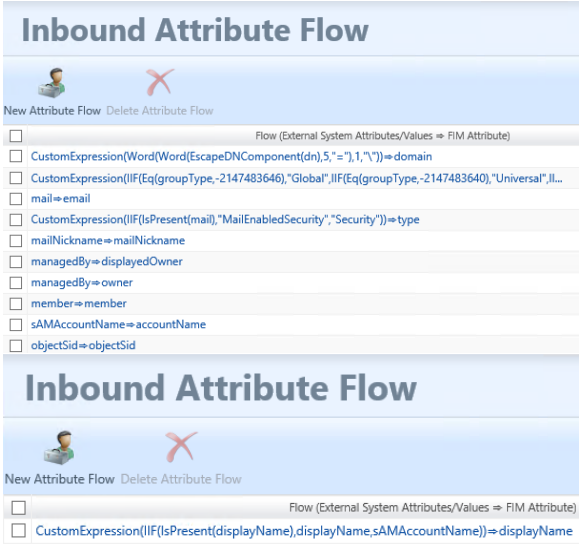
Select *ObjectSID* as relationship criteria.

Use of this attribute will allow to rename group both from Active Directory and MIM 2016 portal. Check the boxes *Create resource in FIM* and *Create resource in external system*.



We will use the following rule to generate the DN attribute:
"CN="+displayName+",OU=Groups,OU=MIM,DC=pocmiam,DC=intra"





ObjectSID attribute (Active Directory) must be imported. It's the join rule.

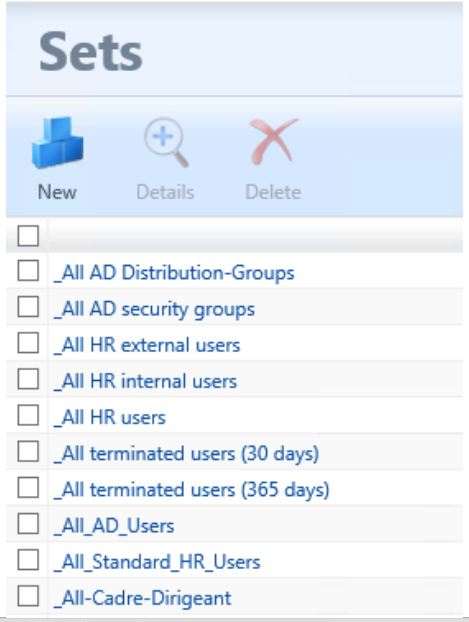
DisplayName attribute is not a default attribute for group. If *displayName* attribute (Active Directory) doesn't exist, we will use *SamAccountName* instead: *IIF(IsPresent(displayName),displayName,sAMAccountName)*

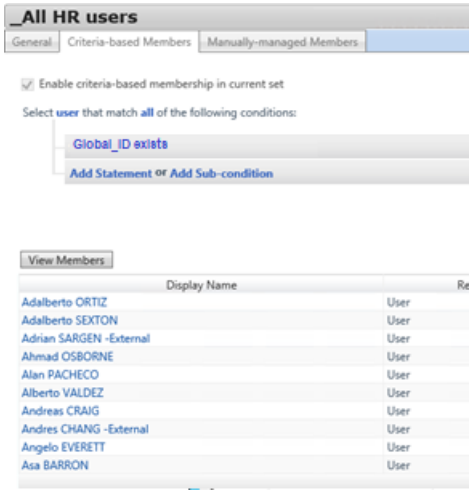
3.10 CONFIGURE ALL SETS

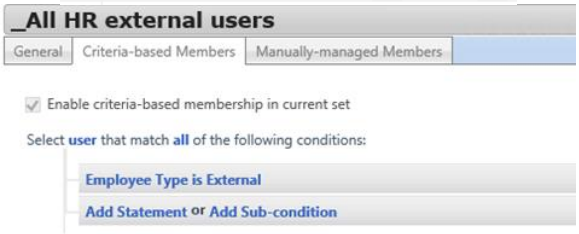
MIM 2016 SET allows to filter *Initiator* and *Target objects* in management policy rules.

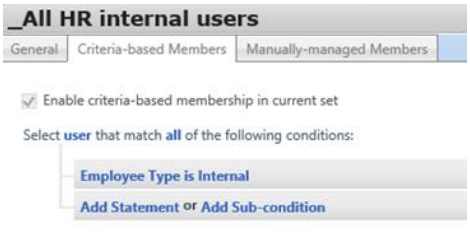
MIM 2016 allows to apply a policy when an object is added or removed of a MIM 2016 sets (*transition in* rules or *transition out* rules).

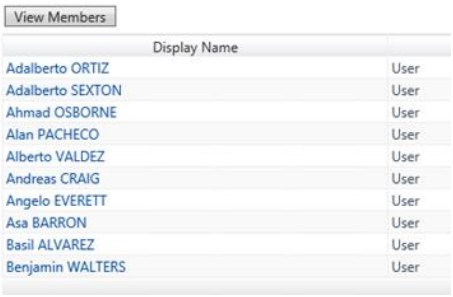
The following sets will use for the POC environment.

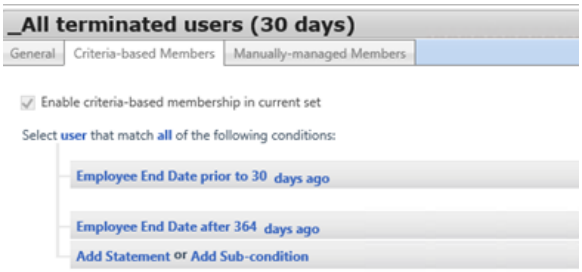


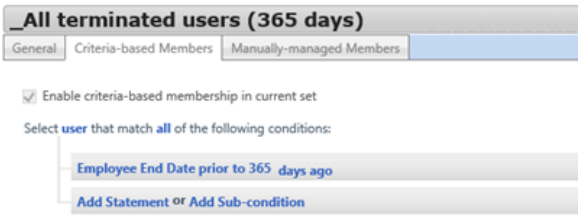


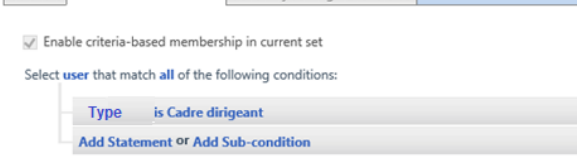


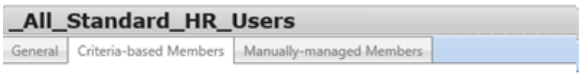


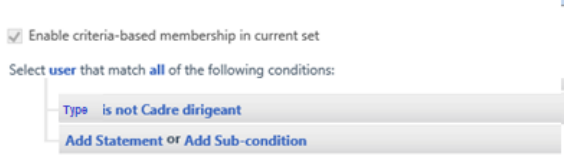












We will create an advanced set by manually define
Go to Advanced views and modify manually the filer.
Backup the previous filter.

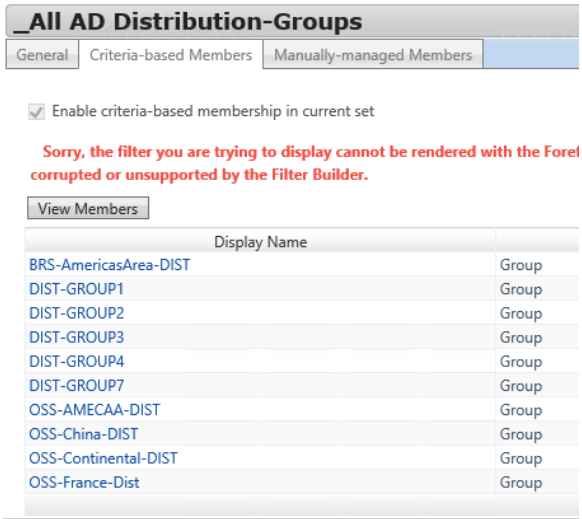
<Filter xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Dialect="http://schemas.microsoft.com/2006/11/XPathFilterDialect" xmlns="http://schemas.xmlsoap.org/ws/2004/09/enumeration">/Person[(AccountName = 'Test') and (starts-with(Global_ID, '1'))]</Filter>

Copy this new entry:

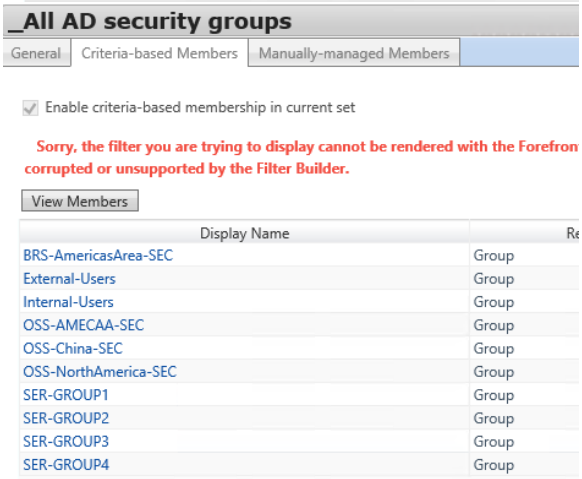
<Filter xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Dialect="http://schemas.microsoft.com/2006/11/XPathFilterDialect" xmlns="http://schemas.xmlsoap.org/ws/2004/09/enumeration">/Person[(AccountName != '$$$') and (Company != '$$$') and (starts-with(Global_ID, 'S'))]</Filter>

Perform the same thing for the set *_All AD Distribution-Groups*. Backup the previous value and replace it by:

<Filter xmlns:xsd="http://www.w3.org/2001/XMLSchema"



xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Dialect="http://schemas.microsoft.com/2006/11/XPathFilterDialect" xmlns="http://schemas.xmlsoap.org/ws/2004/09/enumeration">/Group[(Type = 'Distribution') and (DisplayName != '$$$') and (MailNickname != '$$$')]</Filter>

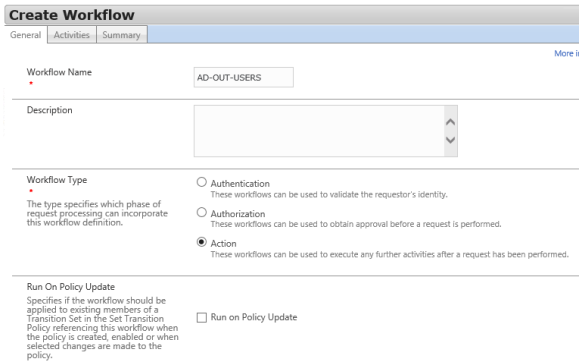


Perform the same thing for the set *_All AD Security-Groups*. Backup the previous value and replace it by:
<Filter xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Dialect="http://schemas.microsoft.com/2006/11/XPathFilterDialect" xmlns="http://schemas.xmlsoap.org/ws/2004/09/enumeration">/Group[((Type = 'Security') and (DisplayName != '$$$') and (AccountName != '$$$')) or ((Type ='MailenabledSecurity') and (DisplayName != '$$$') and (AccountName != '$$$'))]</Filter>

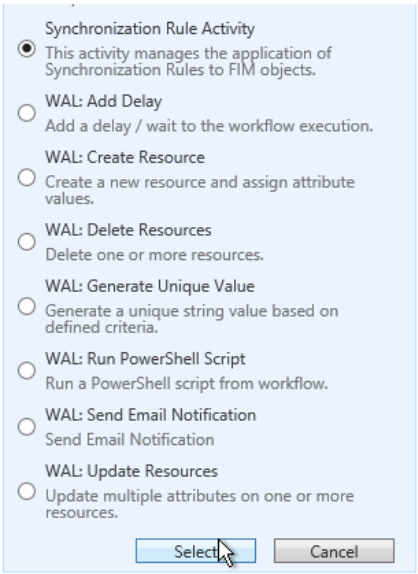
3.11 CONFIGURE ALL MIM WORKFLOWS

3.11.1 Create workflow AD-USERS-OUT

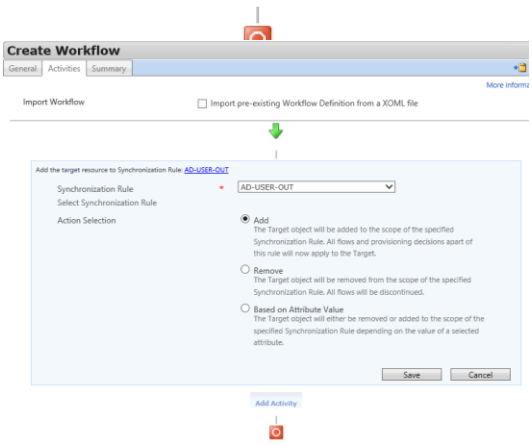
This workflow will start the synchronization rule *AD-USER-OUT*.



Workflow type: *action*

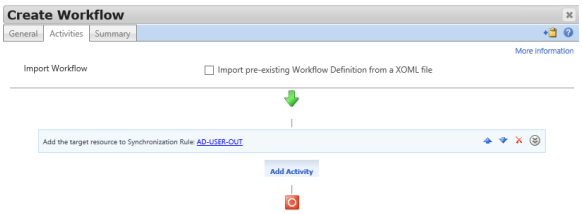


Select *Synchronization Rule Activity*.



Select the synchronization rule *AD-USER-OUT*
Click on *Add*.

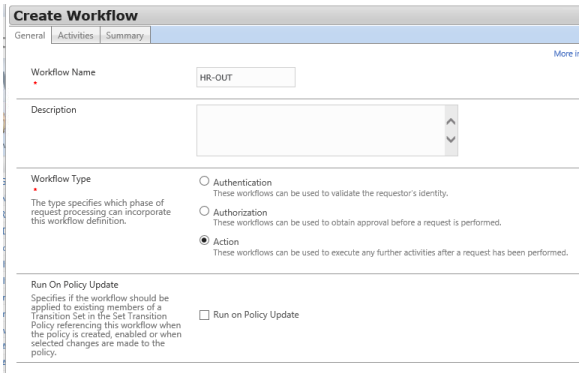
This workflow will allow to generate ERE (Expected Rule Entry) for user which must be synchronized to Active Directory.



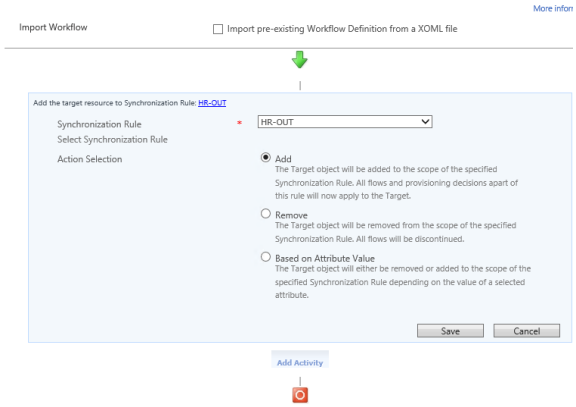
Click on *Finish*.

3.11.2 Create the workflow HR-OUT

This workflow will start the synchronization rules *HR-OUT*.

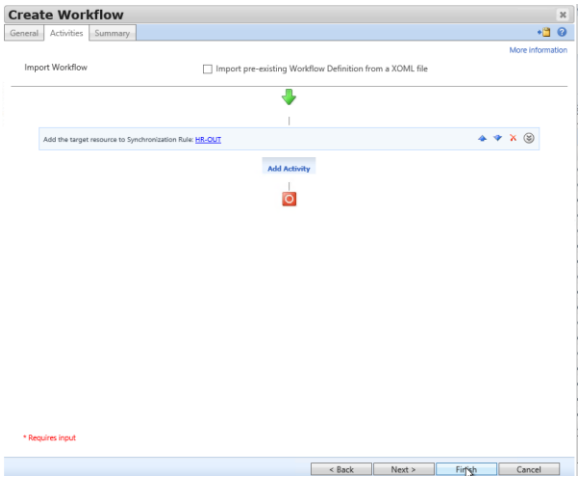


Workflow type: *action*



Select *HR-OUT* and *Add*.

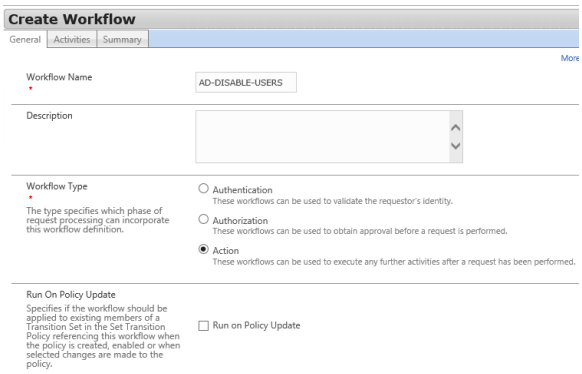
This workflow will allow to generate ERE (*Expected Rule Entry*) for user objects to synchronize mobile phone, office phone and employee type values to HR database.



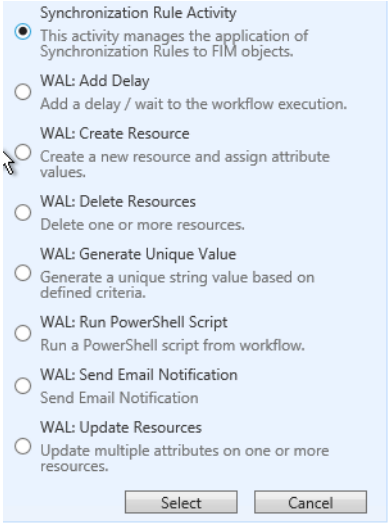
Click on *Finish*.

3.11.3 Create the workflow AD-DISABLE-USERS

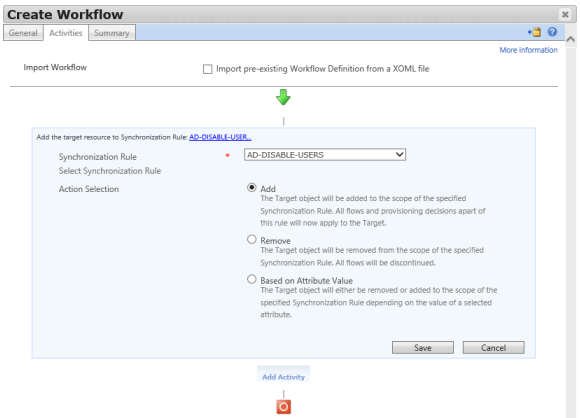
This workflow will allow to start the synchronization rule *AD-DISABLE-USERS* which will disable an Active Directory user account and move it in the OU *Disabled_Users*.



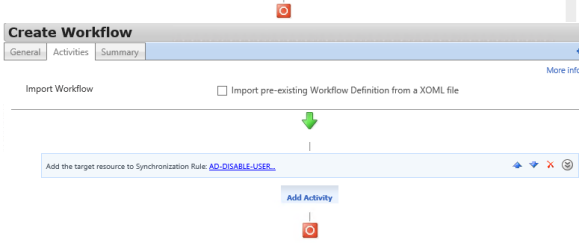
Workflow type: *action*



Select *Synchronization Rules Activity*.

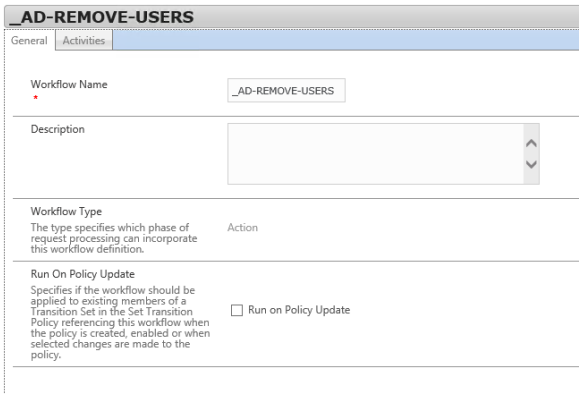


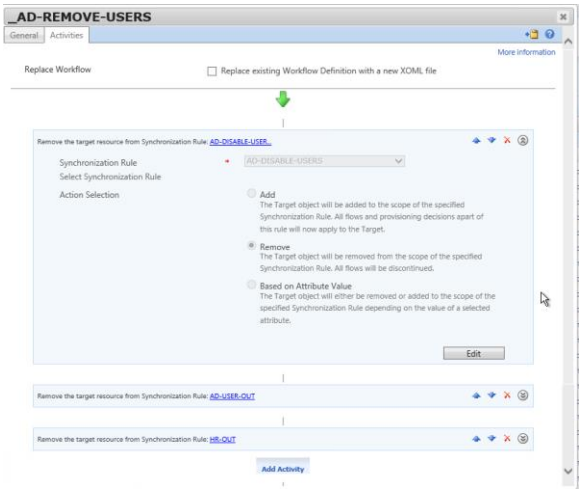
Select the synchronization rules *AD-DISABLE-USERS* and then click *Add*.



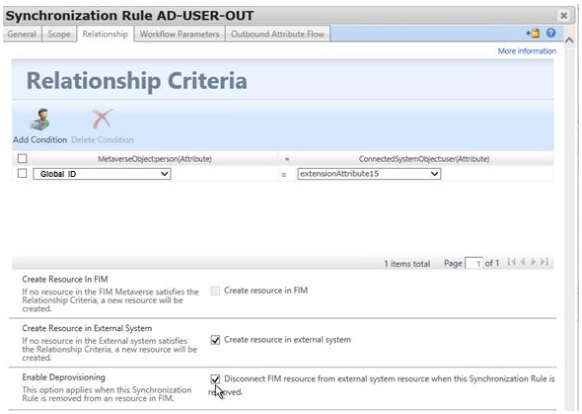
Click on *Finish*.

3.11.4 Create and configure the Workflow _AD-REMOVE-USERS



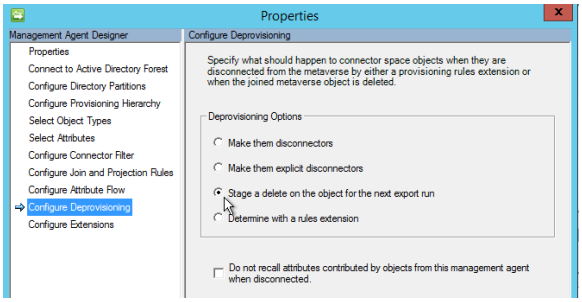


This workflow will remove ERE (*Expected Rule entry*) on user object.

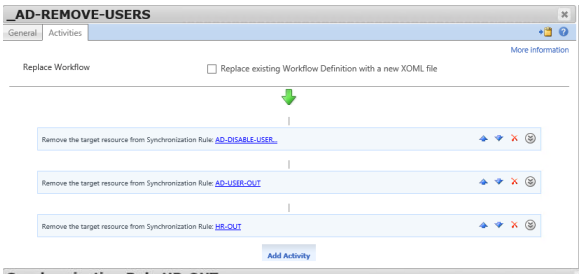


<u>When ERE is removed, the object is mark as disconnect in the AD management Agent.</u>

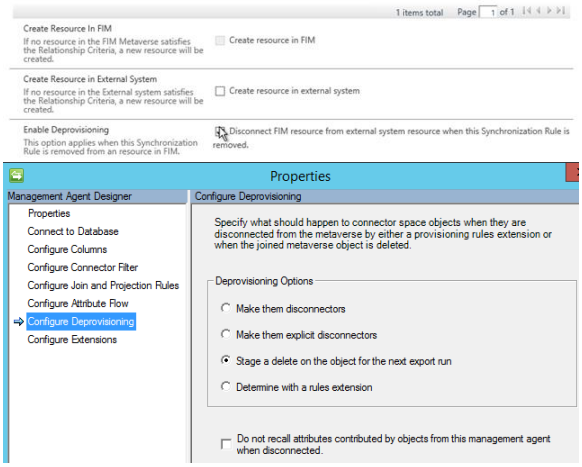
This setting is defined in the synchronization rule *AD-USERS-OUT*.



In fact, the object will be removed at the next *Export* on the *AD* management agent because we configure this option on the AD management agent.



This workflow is also configured to remove ERE for the synchronization rule *AD-DISABLE-USER* (to avoid orphan ERE) and for *HR-OUT* synchronization rule.



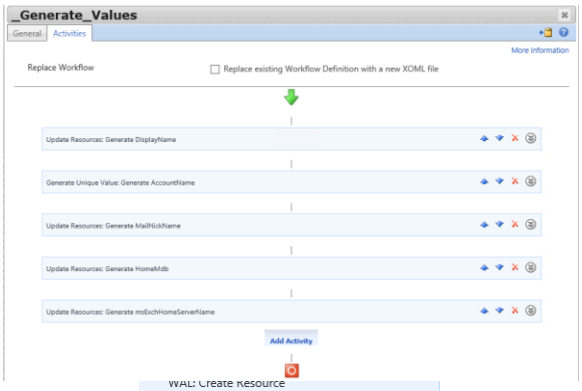
Remove the *HR-OUT* ERE will also remove the object in the HR SQL database.

3.11.5 Generate attributes from MIM portal

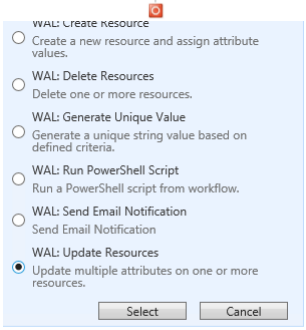
This workflow will generate values on the MIM 2016 services for attributes *AccountName*, *DisplayNames*, *MailNickName* and *HomeMdb* and *MsExchHomeServer*.

This workflow will have 5 activities (workflow type equal to *Action*).
We will use *WAL:Update Resources activities* to generate the value of the MIM service attributes *displayName*, *mailNickname*, *HomeMdb* and *msExchHomeServerName*.

We will use *WAL:Generate unique value* to generate the value of the MIM service attribute *accountName*.



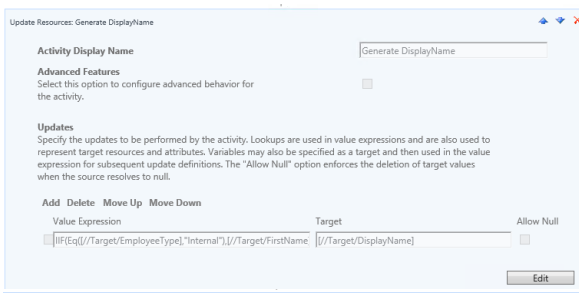
You must obtain the following result at the end of the configuration.

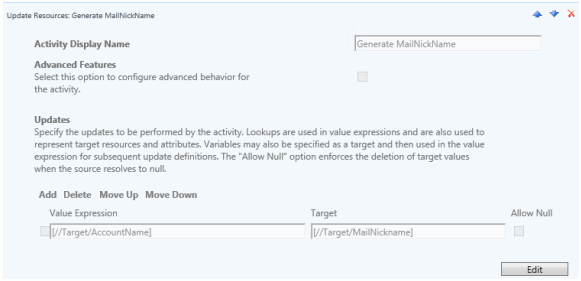


To generate *DisplayName* MIM service attribute:

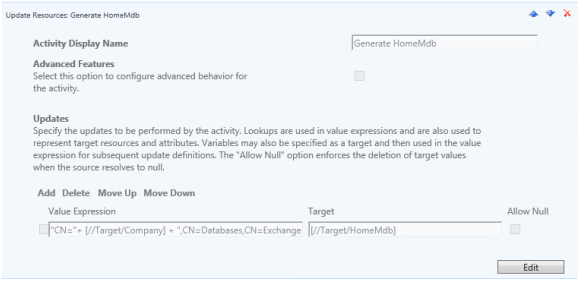
Value expression:
IIF(Eq([//Target/EmployeeType],"Internal"),[//Target/FirstName] + " " +[//Target/LastName],[//Target/FirstName] + " " +[//Target/LastName] + " -External")

Target:
[//Target/DisplayName]



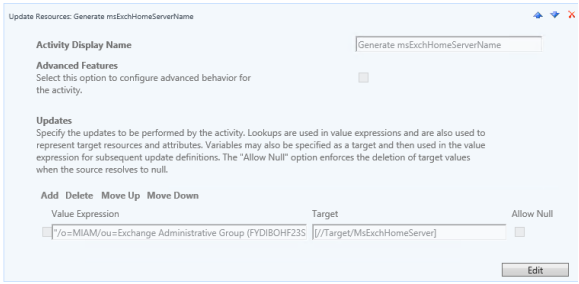


To generate *MailNickname* value, we use the value of *AccountName* attribute.



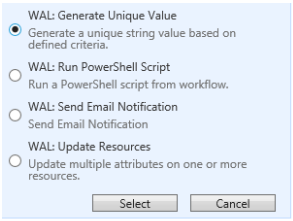
To generate the value of *HomeMdb* (Exchange database LDAP path):
"CN="+ [//Target/Company] + ",CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=MIAM,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=pocmiam,DC=intra"

To generate value for the attribute *MsExchHomeServer*



"/o=MIAM/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=POCEXCH1"

Notes:
In MIM service the attribute has been created with the name *msExchHomeServer*.
In Active Directory, the name of this attribute is *msExchHomeServer<u>Name</u>*.



To generate *AccountName* MIM service attribute:
Target for generated value: *[//Target/AccountName]*
Conflict filter:
This setting allows to perform a request in the MIM service database to check unicity.
/Person[AccountName = '[//Value]' and not(ObjectID='[//Target/ObjectID]')]

We will also check unicity in Active Directory with this request:

Directory path:
GC://DC=POCMIAM,DC=INTRA

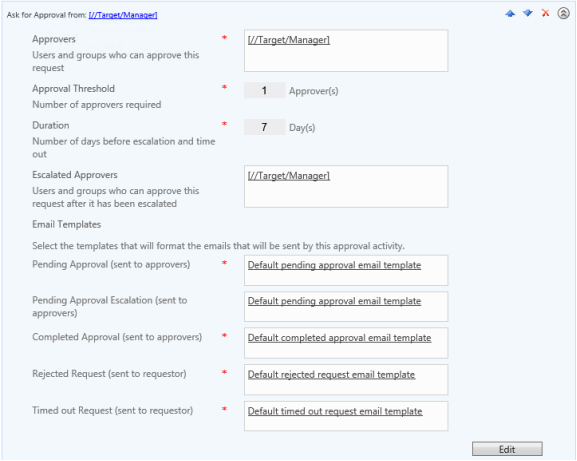
LDAP filter:
(&(objectClass=user)(objectCategory=person)(sAMAccountName=[//Value])(!(Extensionattribute15=[//Target/Global_ID])))

Then we will generate the value of *AccountName* attributes based on these rules:

NormalizeString([//Target/FirstName] + "." + [//Target/LastName])

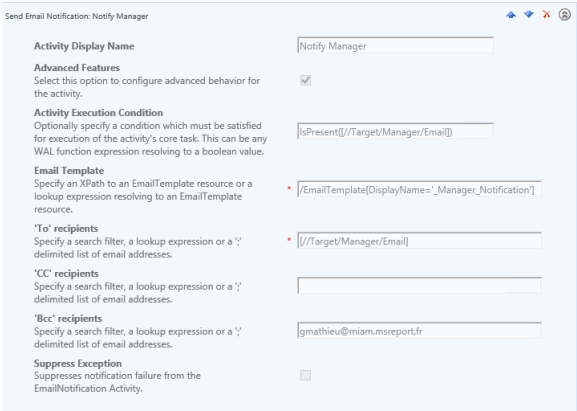
NormalizeString([//Target/FirstName] + "." + [//Target/LastName]) + [//UniquenessKey]

3.11.6 Create the workflow Manager_Approval_Classic



This workflow will allow to request an approval of the manager (authorization workflow).

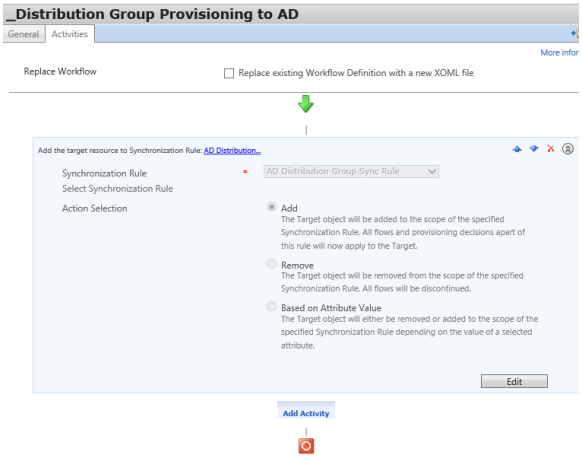
3.11.7 Create the workflow Notify Manager

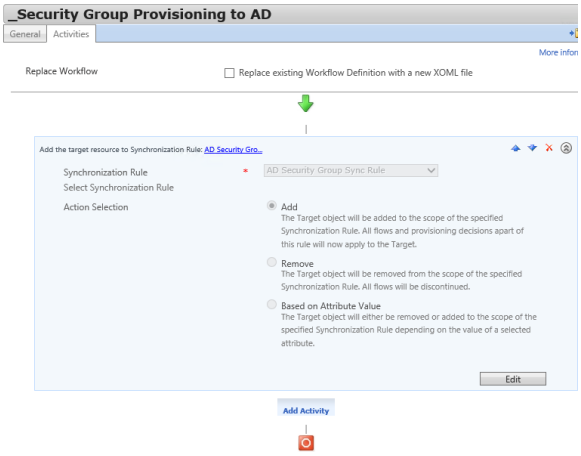


This workflow will allow to send a notification to the manager (action workflow).

3.11.8 Create the workflow _Distribution Group Provisioning to AD and _Security Group Provisioning to AD

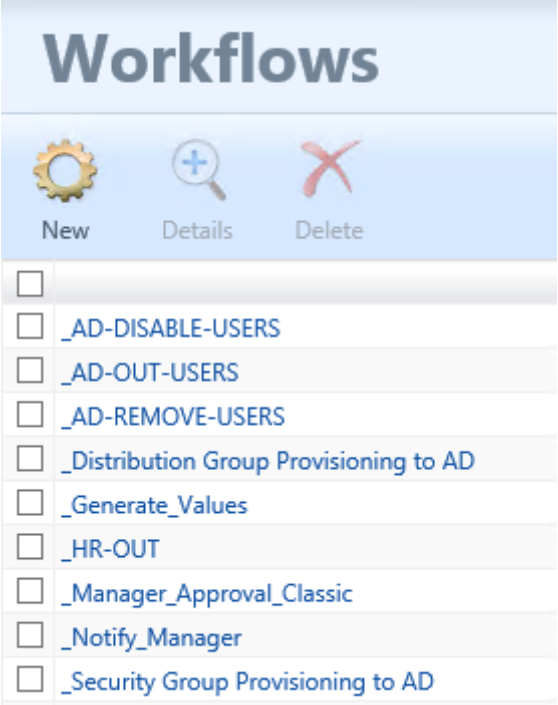
These 2 workflows will allow to generate ERE (Expected rule Entry) to synchronization distribution and security groups.





3.11.9 Workflows Result

You must obtain these results.

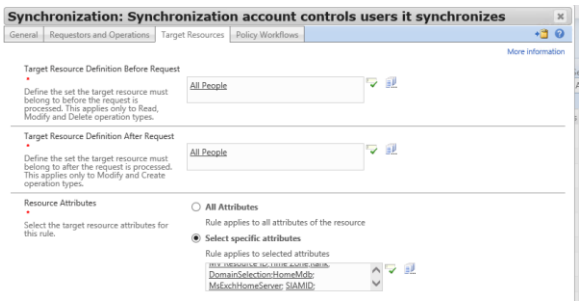


3.12 MANAGEMENT POLICY RULES

3.12.1 Configure Synchronization: Synchronization account controls users it synchronizes Management Policy rule

If you don't configure this Management Policy rule, the Management Agent MIM doesn't have the right to replicate the attribute *Type*, *Domain*, *HomeMdb*, *MsExchHomeServer* and *Global_ID*.

When you try to perform an *Export* on the MIM management agent, the following error appears:
Fault Reason: Policy prohibits the request from completing.\r\n\r\nFault Details: <RequestFailures xmlns="http://schemas.microsoft.com/2006/11/ResourceManagement" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><RequestAdministratorDetails><FailureMessage>Exception: ManagementPolicyRule
Stack Trace: Microsoft.ResourceManagement.WebServices.Exceptions.PermissionDeniedException: ManagementPolicyRule ---> System.Data.SqlClient.SqlException: Reraised Error 50000, Level 16, State 1, Procedure DoEvaluateRequestInner, Line 1319, Message: ***Permission denied:***
*<ai><Name>**Domain**</Name></ai><ai><Name>**Type**</Name></ai><ai><Name>Global_ID</Name></ai>*

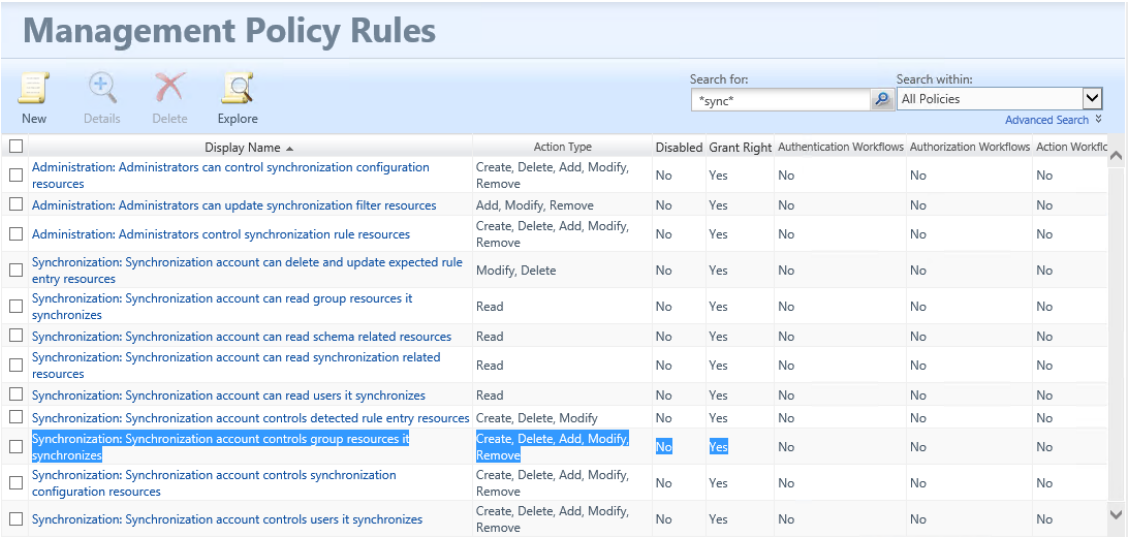


Add the following attributes in the rule.

Type;Domain;HomeMdb;MsExchHomeServer; Global_ID;

3.12.2 Enable the rules to synchronize groups

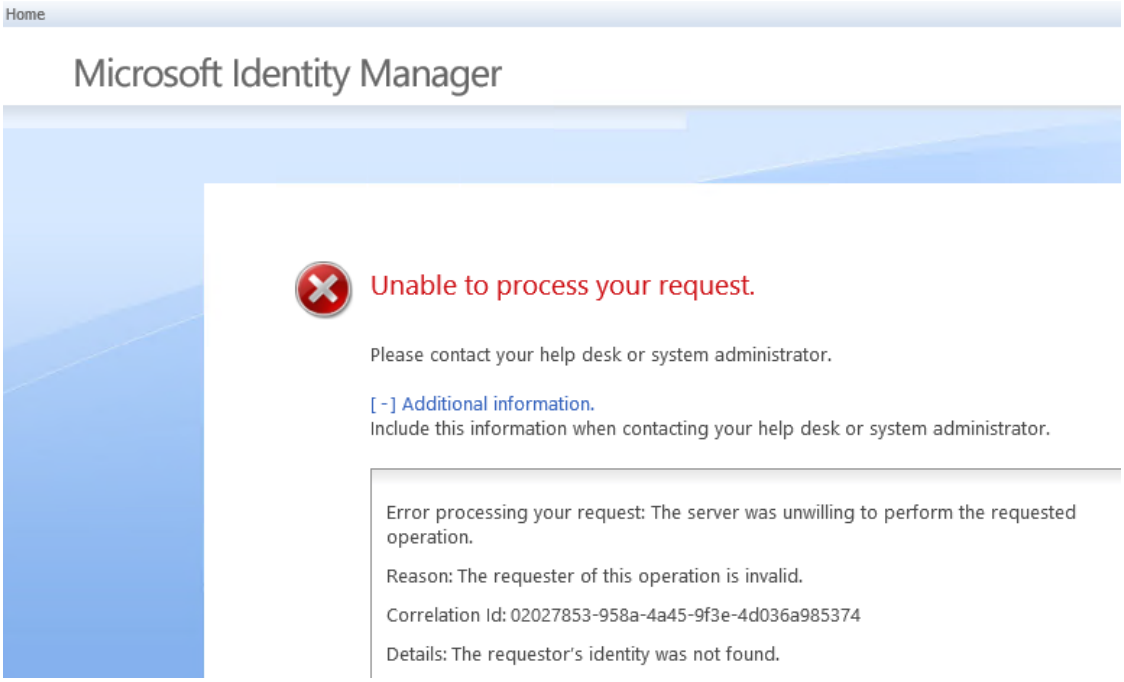
Enable the management policy rules (disabled by default):
Synchronization: Synchronization account controls group resources it synchronizes
Synchronization: Synchronization account can read group resources it synchronizes



Display Name	Action Type	Disabled	Grant Right	Authentication Workflows	Authorization Workflows	Action Workflc
Administration: Administrators can control synchronization configuration resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No
Administration: Administrators can update synchronization filter resources	Add, Modify, Remove	No	Yes	No	No	No
Administration: Administrators control synchronization rule resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No
Synchronization: Synchronization account can delete and update expected rule entry resources	Modify, Delete	No	Yes	No	No	No
Synchronization: Synchronization account can read group resources it synchronizes	Read	No	Yes	No	No	No
Synchronization: Synchronization account can read schema related resources	Read	No	Yes	No	No	No
Synchronization: Synchronization account can read synchronization related resources	Read	No	Yes	No	No	No
Synchronization: Synchronization account can read users it synchronizes	Read	No	Yes	No	No	No
Synchronization: Synchronization account controls detected rule entry resources	Create, Delete, Modify	No	Yes	No	No	No
Synchronization: Synchronization account controls group resources it synchronizes	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No
Synchronization: Synchronization account controls synchronization configuration resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No
Synchronization: Synchronization account controls users it synchronizes	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No

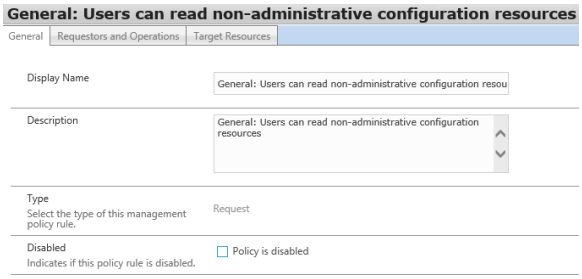
3.12.3 Allow user to connect to the MIM 2016 portal

If a non-administrator tries to connect to MIM portal, he encounters the following error:



To solve this problem, you must fill the attributes *AccountName*, *ObjectSID* and *domain* on the MIM 2016 portal. This will allow MIM 2016 portal to find the MIM user to Active Directory (to perform authentication).
https://social.technet.microsoft.com/wiki/contents/articles/36399.fim-2010-mim-2016-troubleshooting-the-requestor-s-identity-was-not-found.aspx

You need to enable these management policy rules which are disabled by default:
General: Users can read non-administrative configuration resources
User management: Users can read attributes of their own



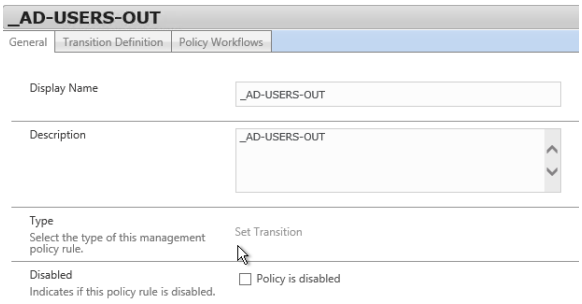
Enable *General: Users can read non-administrative configuration resources*

More information
https://social.technet.microsoft.com/Forums/en-US/35ebc6a7-5ee7-4306-a126-1117a04383e9/error-when-loading-fim-portal-in-new-installation-the-requestors-identity-was-not-found?forum=ilm2
https://social.technet.microsoft.com/wiki/contents/articles/36399.fim-2010-mim-2016-troubleshooting-the-requestor-s-identity-was-not-found.aspx

3.12.4 Create the management policy rule _AD-USERS-OUT

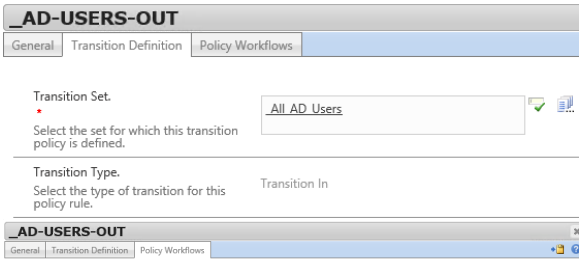
The management policy rule will allow to start the workflow which start a synchronization rule.

A Management Policy used to generate *ERE* (*Expected Rule Entry*) must use *Set transition* because the ERE must only generate once. If you use a *Request* type, you will generate lots of unwanted ERE objects and you increase the workload of MIM 2016 solution.



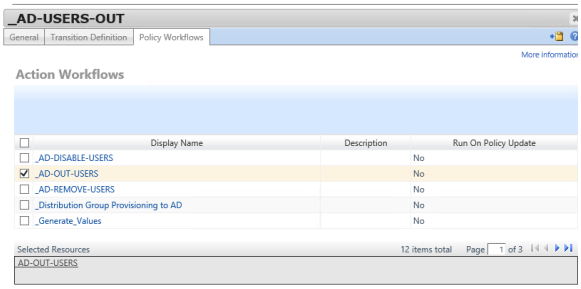
Display Name: *_AD-USERS-OUT*

Type: *Set Transition*.



The management policy rule will only generate ERE when a user becomes member of the *_All AD users* MIM 2016 set.

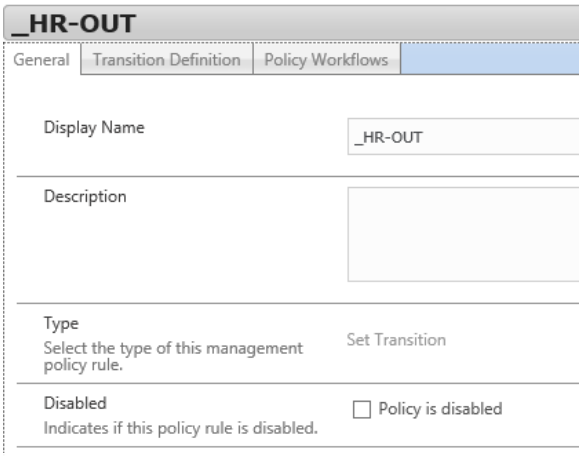
This set contains all users with a *Global_ID*, a *company* value and a *Display Name*.



Select the workflow *_AD_OUT-USER*.

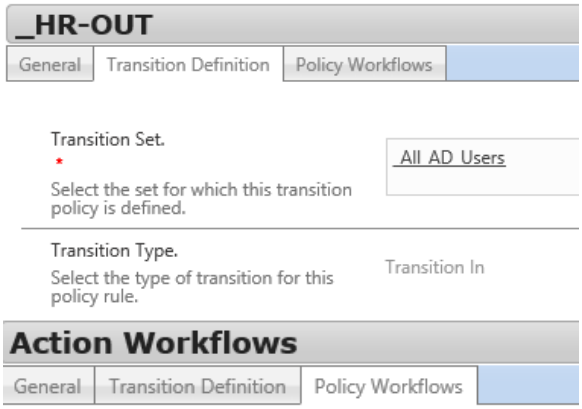
Click on *Submit*.

3.12.5 Create the management policy rule _HR-OUT

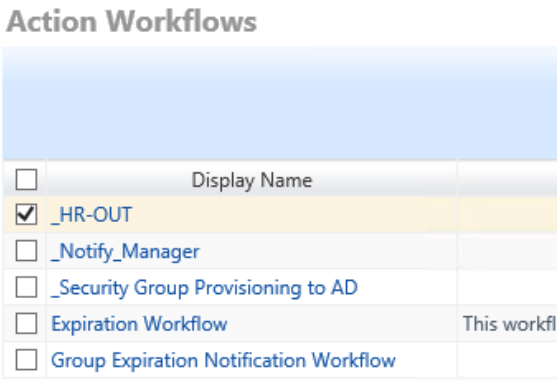


Display Name: *_HR-OUT*.

Type: *Set Transition*.

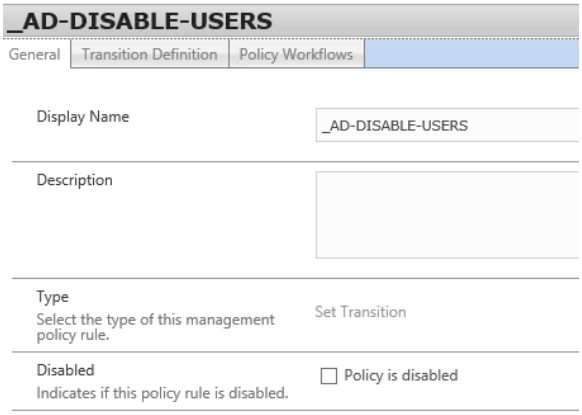


The management policy rule will only generate ERE when a user becomes member of the *_All AD users* MIM 2016 set.



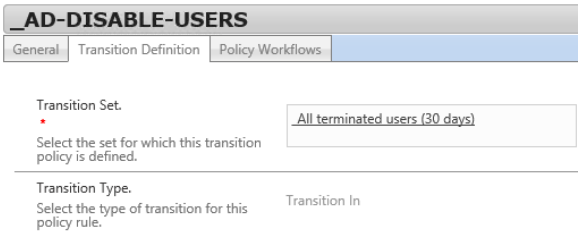
Select *HR-OUT* workflow.

3.12.6 Create the management policy rule AD-DISABLE-USERS



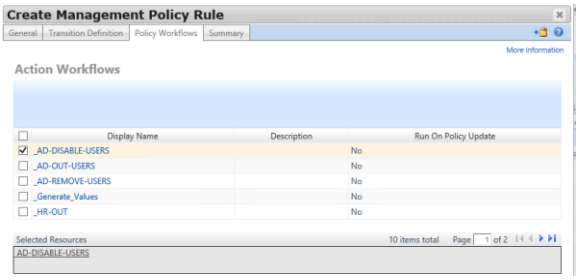
Display Name: *_AD-DISABLE-USERS*

Type: *Set Transition*.



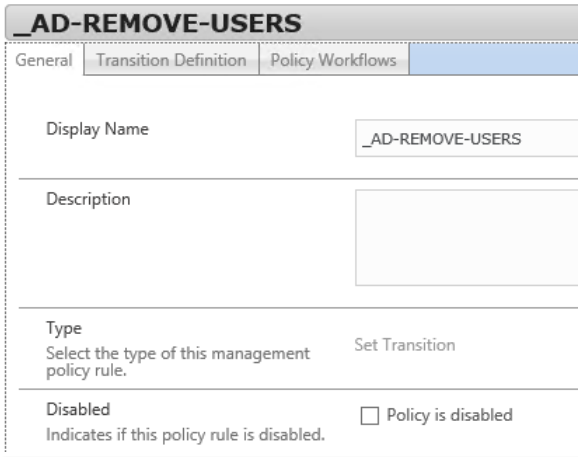
Transition Set: *_All terminated users (30 days)*

Transition Type: *Transition In*



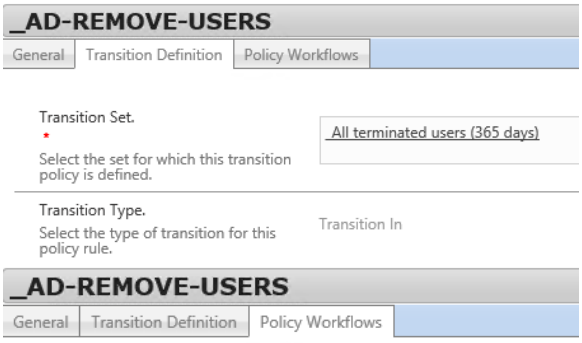
Select the workflow *_All_Disable_users*.

3.12.7 Create the management Policy rule AD-REMOVE-USERS



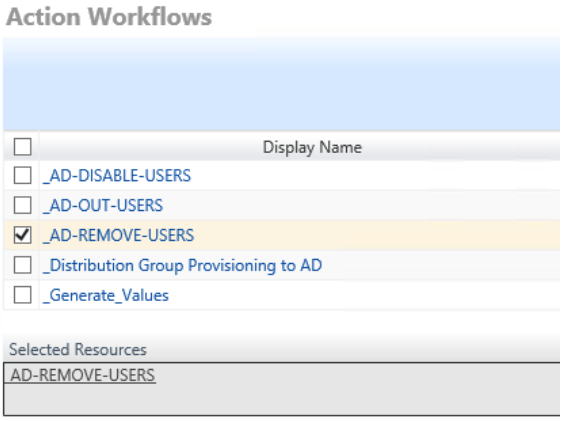
Display Name: *_AD-REMOVE-USERS*

Type: *Set Transition*.



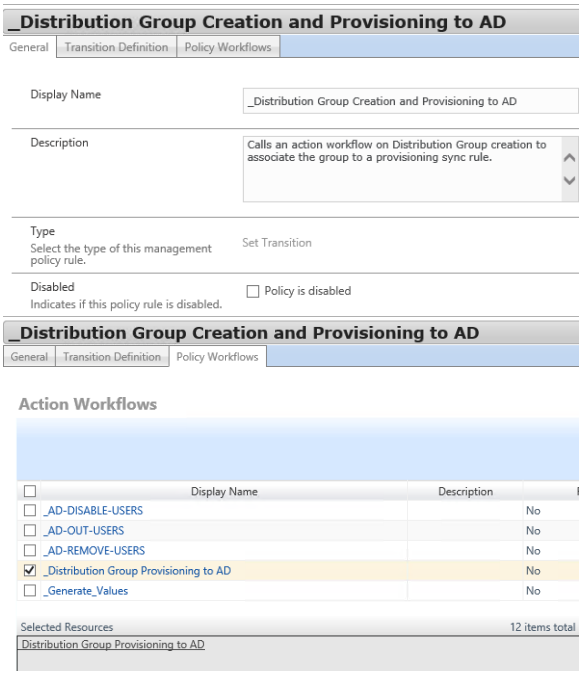
Transition Set: *_All terminated users (365 days)*

Transition Type: *Transition In*

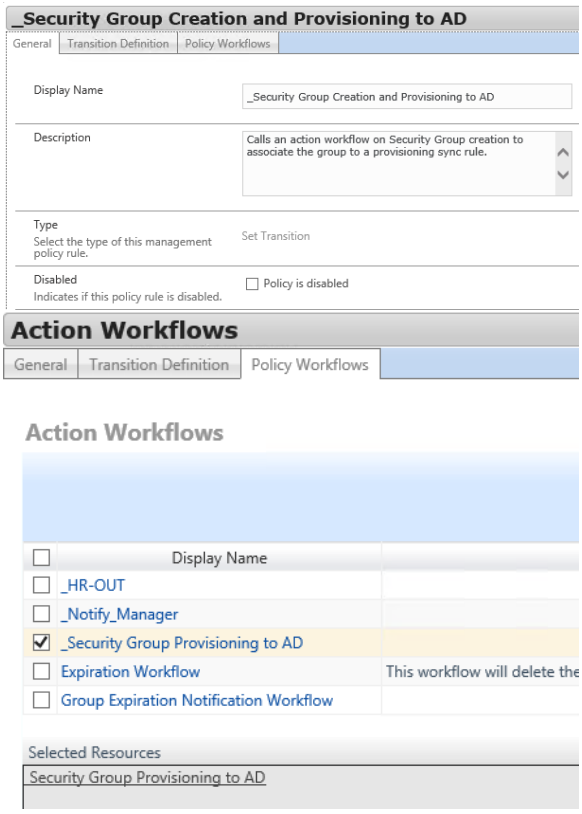


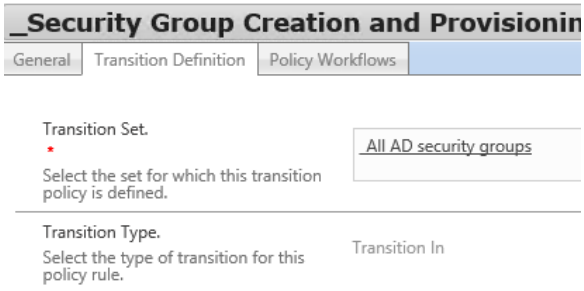
Select the workflow *_All_REMOVE_USERS*.

3.12.8 Create the management rule policy _Distribution Group Creation and Provisioning to AD



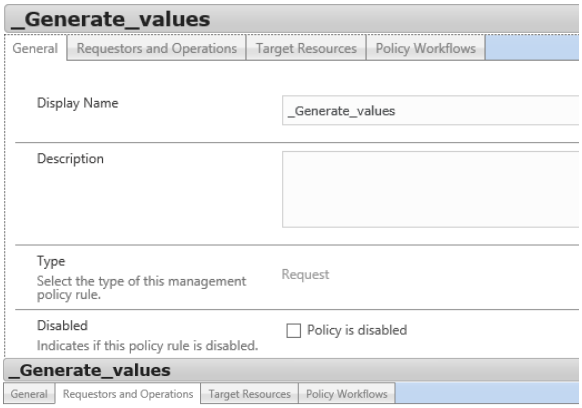
3.12.9 Create the management rule policy _Security Group Creation and Provisioning to AD



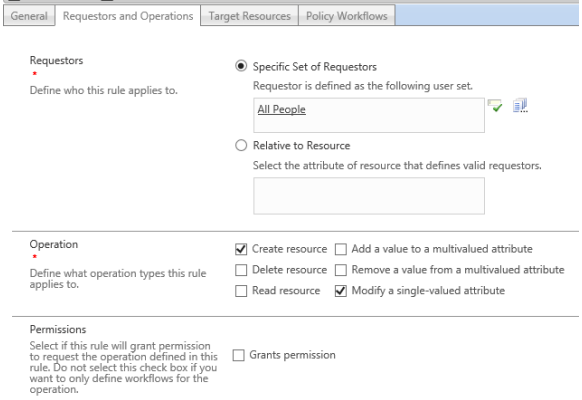


3.12.10 Create the management policy rule which start the workflow _Generates values

This management policy rule must start the workflow *Generates Values* when the synchronization engine or a user changes the value of the MIM service attributes *Company, Employee Type, First name* and *Last Name*.



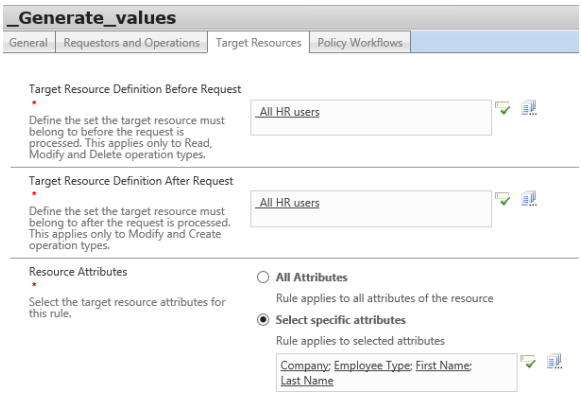
Display Name: *_Generate_values*
Type: ***Request***



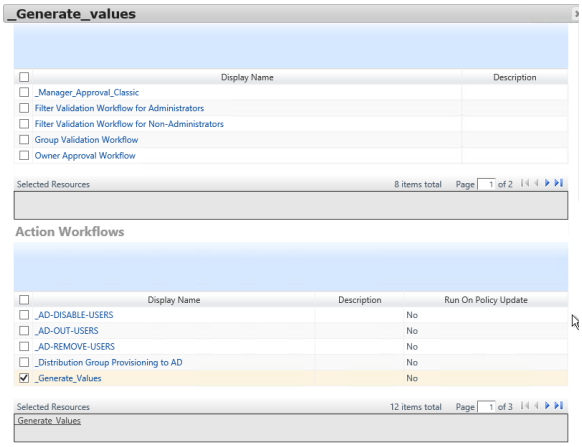
Requestors: *All People*

Operation: *Create resource and Modify a single-valued attribute*

The requestor *All People* includes all standard users and the user *Built-in Synchronization Account* which is used to perform synchronization between Metaverse and MIM service management agent.



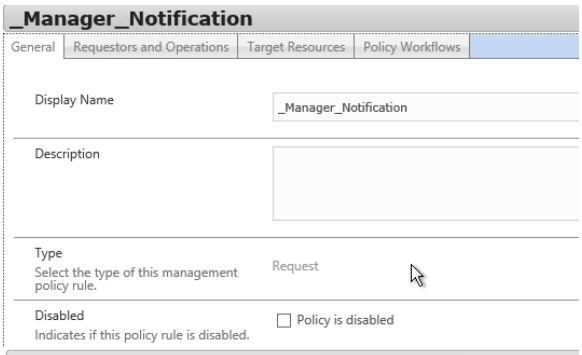
Use *_All_HR_Users* to start the workflow only for user with a valid Global_ID. This avoid starting the workflow for the MIM administrative user like *Built-in Synchronization Account.*



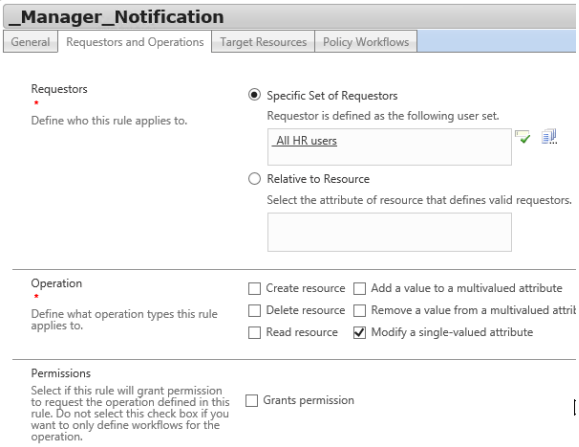
Select the action workflow *_Generates_Values*.

3.12.11 Start the workflow which send an email to manager (Type not equal to ***Cadre dirigeant***)

This management policy rule will start the workflow which send notification.

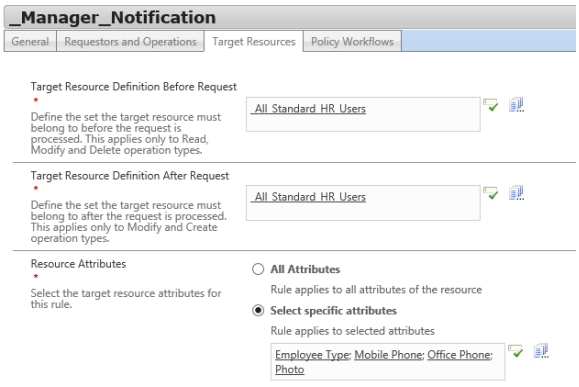


Type: *Request*

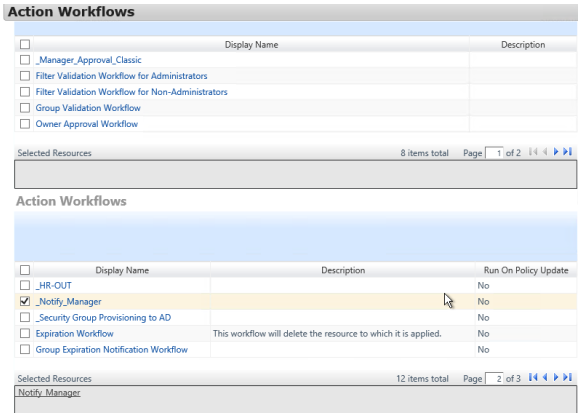


Requestor must be *_All_HR_users*.

No notification will be sent when the change is performed by the synchronization engine user (*Built-in Synchronization Account*) which is not in this set.

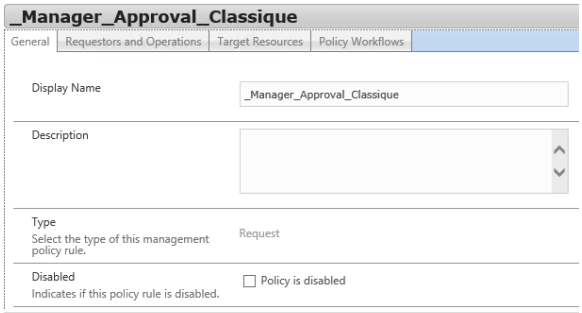


The notification must only be sent to user with a Type not equal to *Cadre dirigeant* when the MIM service attributes *Mobile Phone*, *Office Phone*, *Employee Type* or *Photo* are changed.

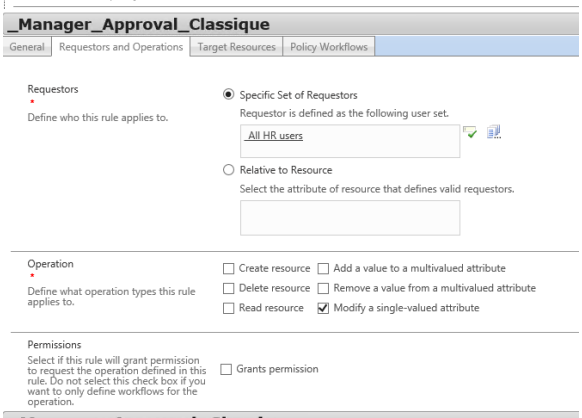


Select the action workflow named *_Notify_Manager*

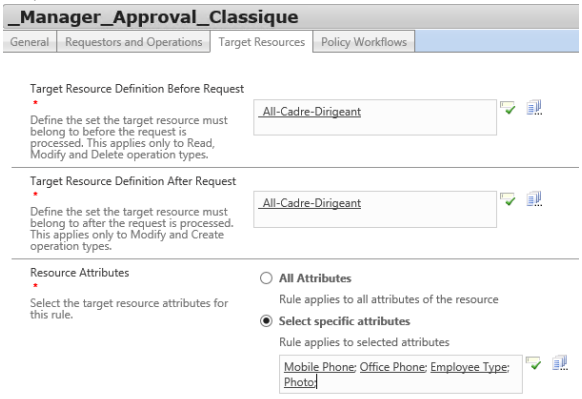
3.12.12 Start the workflow which requires approval of manager (Type equal to ***Cadre dirigeant***)



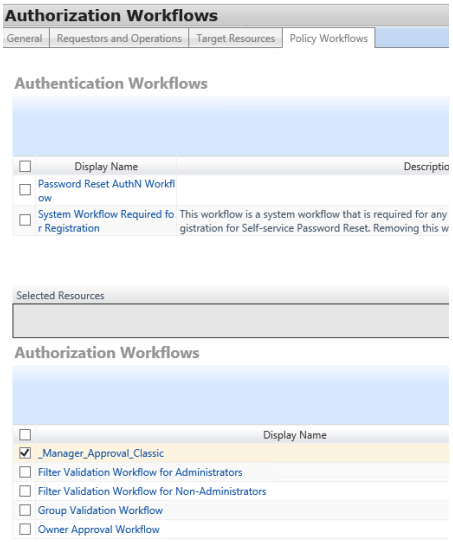
Type: *Request*



Requestor must be *_All_HR_users*.

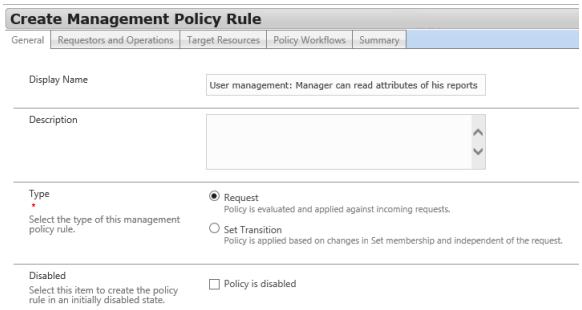


The approval must only be required if you modify a user with a Type equal to *Cadre dirigeant* when the MIM service attributes *Mobile Phone*, *Office Phone*, *Employee Type* or *Photo* are changed.



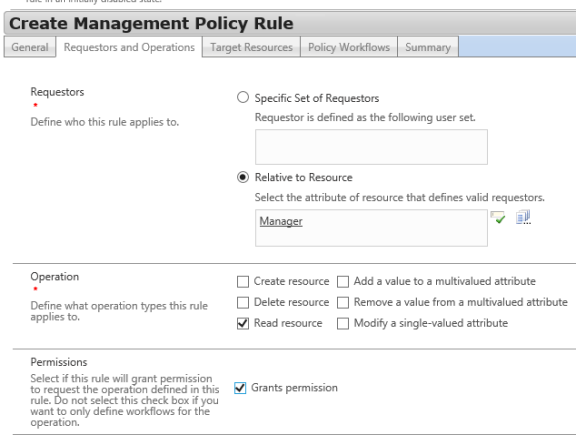
Check the box *_Manager_Approval_Classic* to select the approval workflow.

3.12.13 Allow a manager to read attributes of his reports



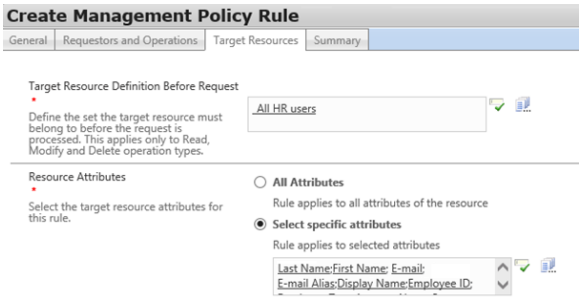
Display Name: *_User management: Manager can read attributes of his reports*

Type: *Request*



Select *Relative to Resource* | *Manager*.

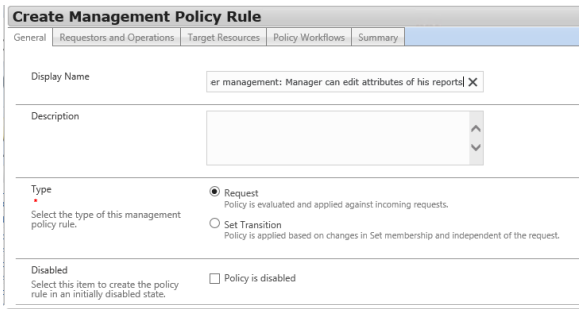
Check the boxes *Read resource* and *Grants permission*.



Use the set _All HR users.

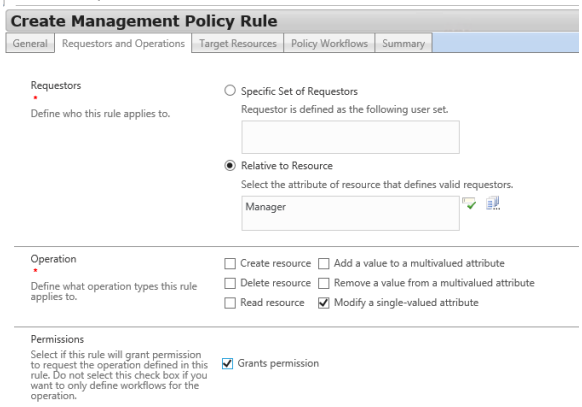
Use *Select specifics attributes* and copy the following attributes in the field *Global_ID; Last Name; First Name;E-mail; E-mail Alias; Display Name;Employee Id;Employee Type; AccountName; Company; department; Job Title; Manager;Address; Postal Code; City; Country; Mobile Phone; Office Phone; Photo; Employee End Date;Employee Start date; Type; Domain*

3.12.14 Allow a manager to change EmployeeType, Mobile Phone, Office Phone and Photo of his reports



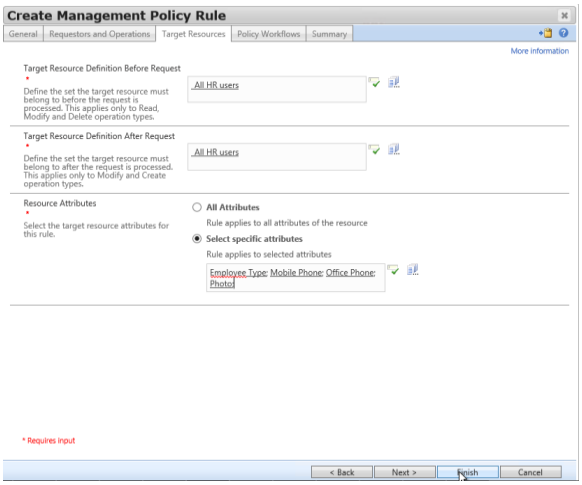
Display name: *_User management: Manager can edit attributes of his reports*

Type: *Request*



Select *Relative to Resource | Manager*.

Check the boxes *Modify a single-valued attribute* and *Grants permission*.

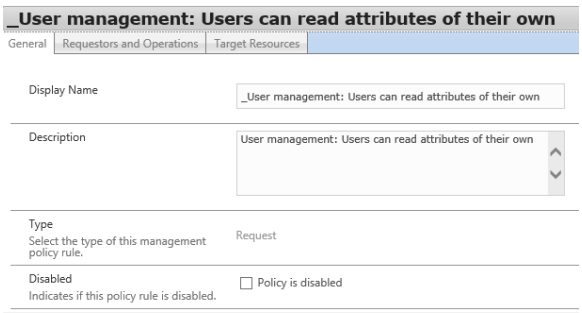


Use the set *_All HR users*.

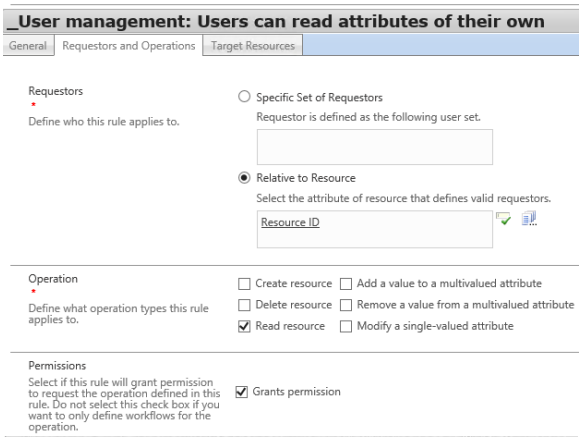
Use *Select specifics attributes* and enter the attributes *Employee Type*, *Mobile Phone*, *Office Phone* and *Photo*.

3.12.15 Allow a user to read attributes of his own user account

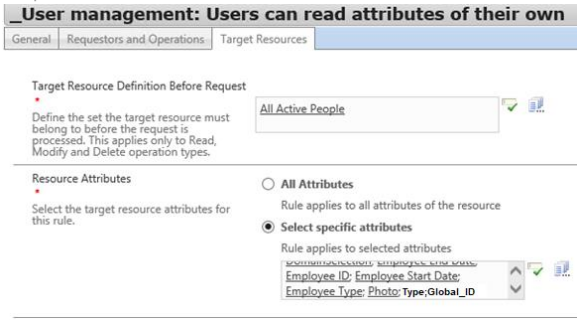
The Management Policy Rule *User management: Users can read attributes of their own* allows a user to read his attributes. You must define the list of attributes based on your attributes rules.



Uncheck the box *Disabled*.



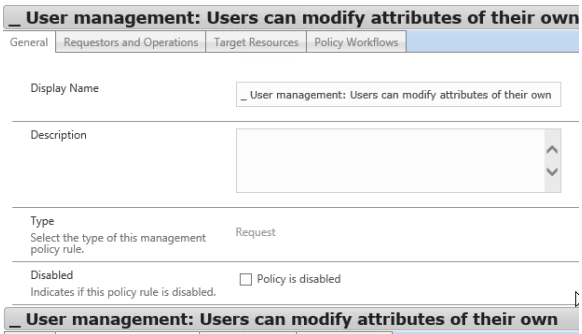
Let all default settings.



Add the following values in the fields select specifics attributes.
Global_ID; Last Name; First Name;E-mail; E-mail Alias; Display Name;Employee Id;Employee Type; AccountName; Company; department; Job Title; Manager;Address; Postal Code; City; Country; Mobile Phone; Office Phone; Photo; Employee End Date;Employee Start date; Type; Domain

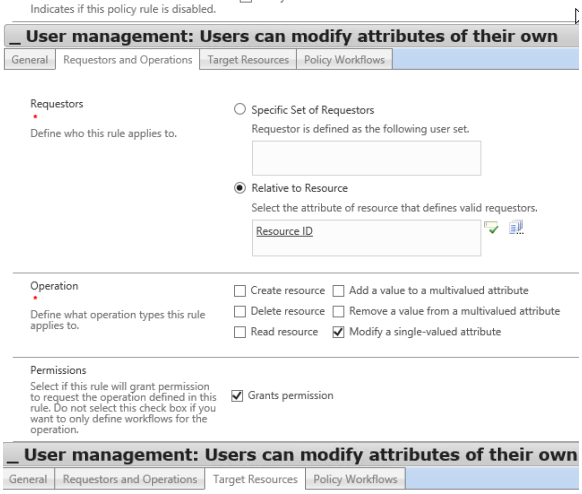
3.12.16 Allow user to modify attributes of his own user account

User could change his office phone, his mobile phone and his photo (with approval if Type is equal to *Cadre dirigeant*).



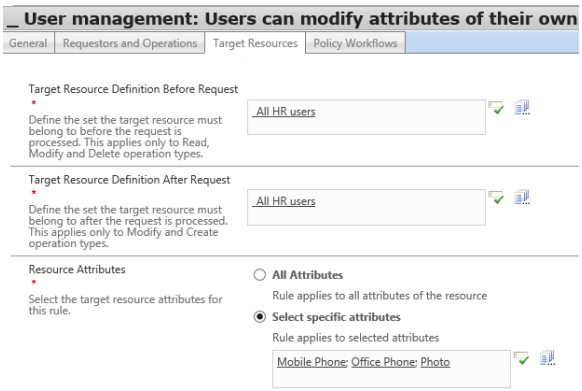
Display Name: *_ User management: Users can modify attributes of their own*

Type: *Request*



Select the Relative to *Resource*.
Use the attribute *ResourceID*.

Check the boxes *Modify a single-valued attribute* and *Grant permissions*.

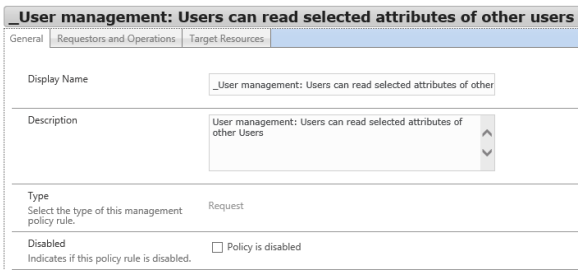


Use the set *_All HR users*.

Add the following attributes:
Mobile Phone, Office Phone, Photo.

3.12.17 Allow users to read attributes of other users

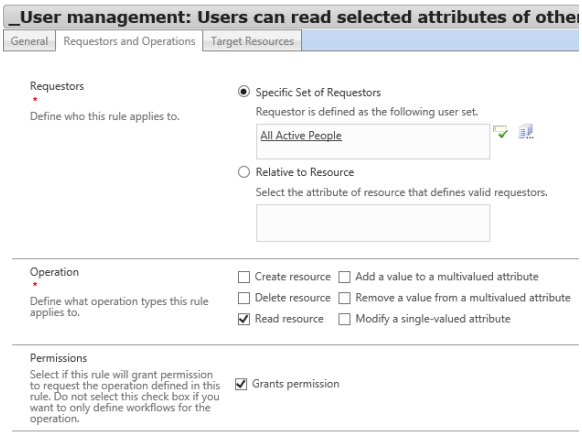
You need to enable and reconfigure the Management Policy rule.
_User management: Users can read selected attributes of other users



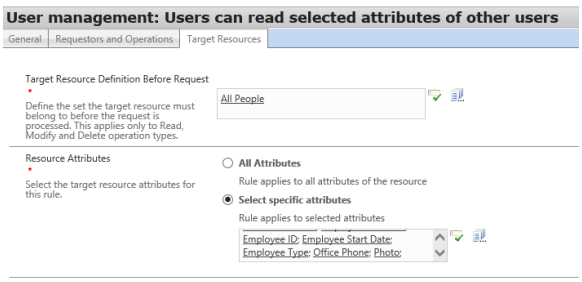
Display Name: *_User management: Users can read selected attributes of other users*

We have renamed existing management policy rule.

Type: Request



Let default settings.

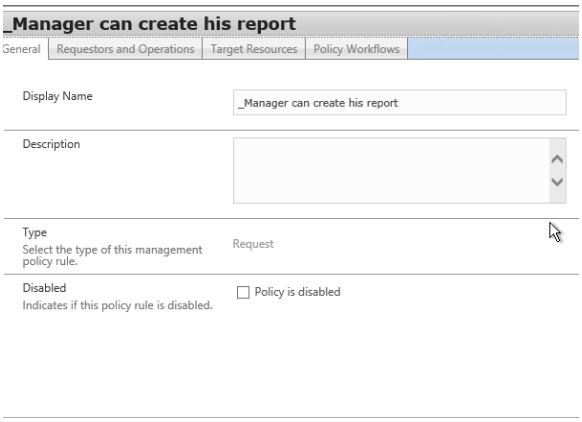


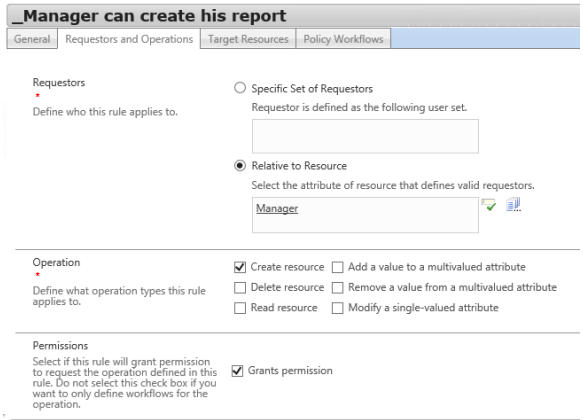
Default setting is:
Display Name; Resource ID; Resource Type; Account Name; Address; City; Company; Cost Center; Cost Center Name; Country/Region; Department; Domain; Domain Configuration; E-mail; First Name; Job Title; Last Name; E-mail Alias; Manager; Middle Name; Mobile Phone; Time Zone

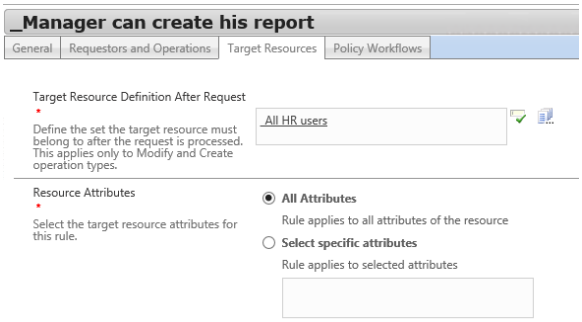
Add the following attribute
Global_ID;Employee Id;Employee Type;Address; Postal Code; City; Country; Mobile Phone; Office Phone; Photo; Employee End Date;Employee Start date; Type; Domain

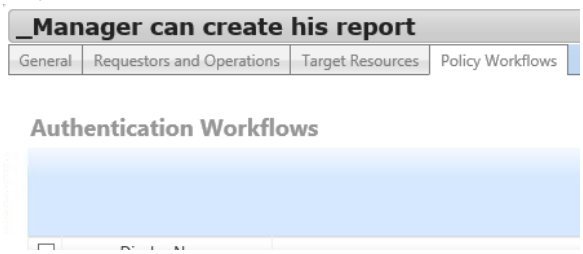
3.12.18 Allow a manager to create his reports

We delegate the permission to manager to add user only if the requestor is the manager of the target user. No workflow is used with this management policy rule.

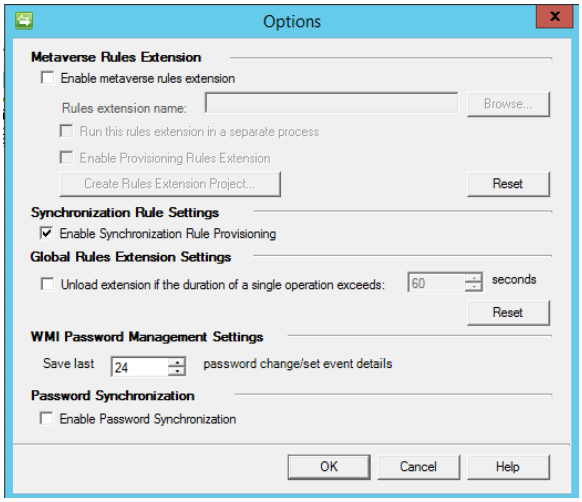








3.13 CONFIGURE PROVISIONNING

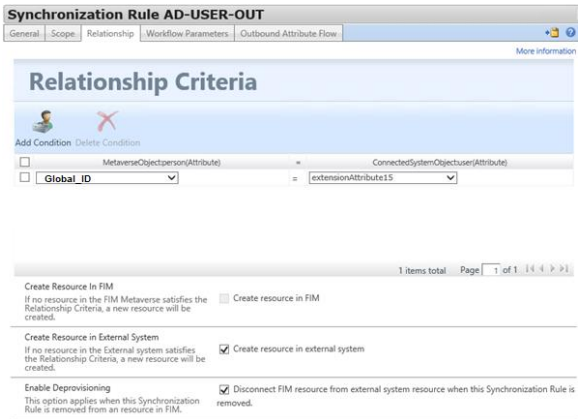


Go to *Tools | Options* in the MIIS.EXE console (MIM 2016 Synchronization Service).

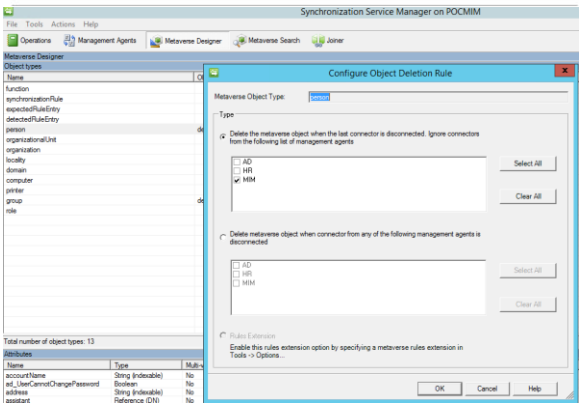
Check the box *Enable Synchronization Rules Provisionning*.

3.14 CONFIGURE DEPROVISIONNING FOR USER

A *management policy rule* named *AD-DELETE-USERS* will start a workflow which will remove the ERE *AD-USERS-OUT* if the user enters in the set *_All users 365 days*.

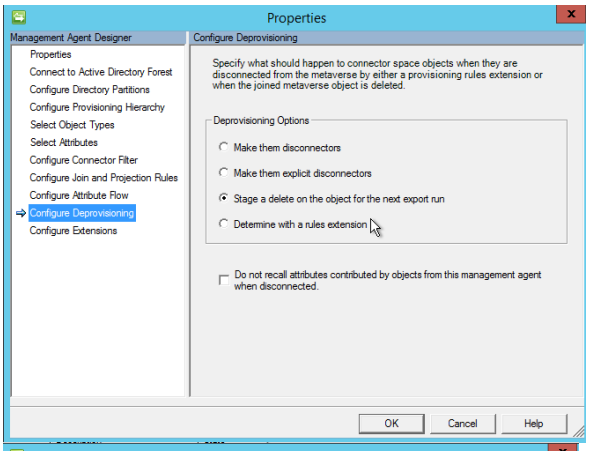


When an ERE is removed, this generate a disconnect in the *AD* management agent Connector space.

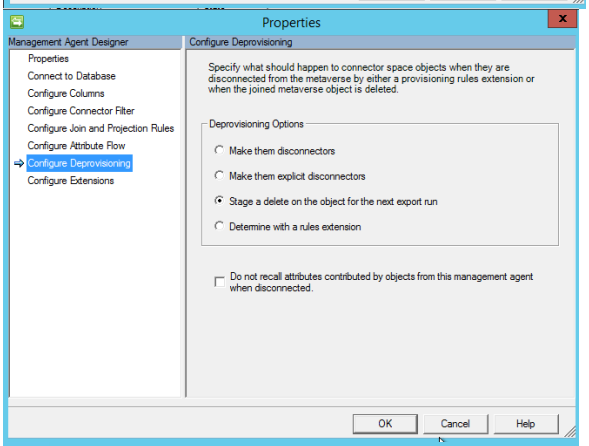


You can configure how the object is delete in the Metaverse.

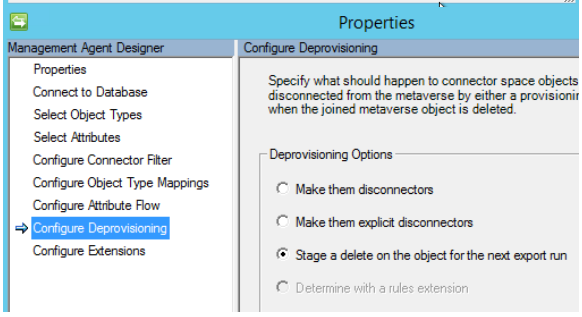
The selected option explain that the object is deleted from the Metaverse when the object is disconnected from the last connector. If the object is still connected to MIM portal, the object will be removed even so.



In the tab *Configure Deprovisionning* of the *AD* Management Agent, you have also a setting which explains that you perform a deletion in Active Directory at the next *Export* when the Metaverse object is disconnected (deleted).



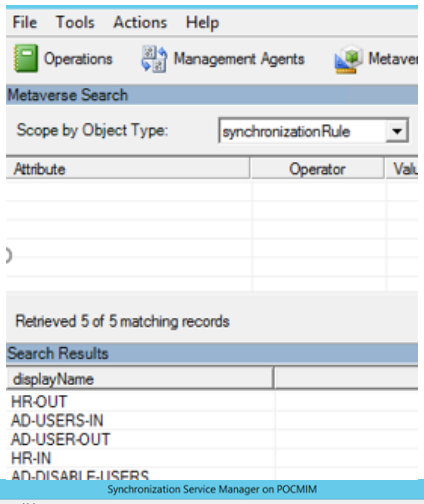
The same setting has been defined on the *HR* and *MIM* management agents.



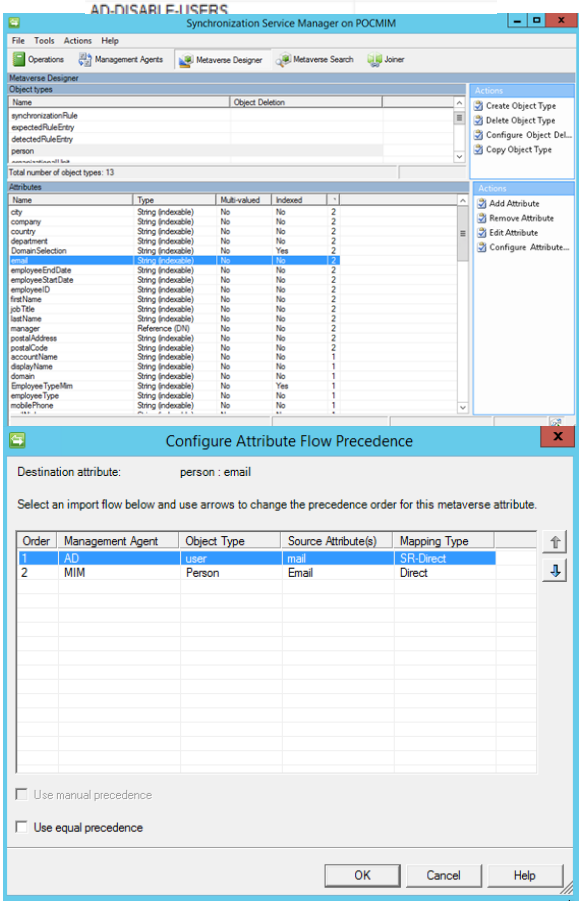
3.15 CONFIGURE RULES PRECEDENCE FOR USER CLASS (METAVERSE SCHEMA)

Perform a full import then a full synchronization only the MIM Management agent to import all synchronization rules from the MIM service to the MIM synchronization rules.

Rule precedence allows to define priority to update value of a **Metaverse** attribute when multiples management agents could perform changes on this attribute.



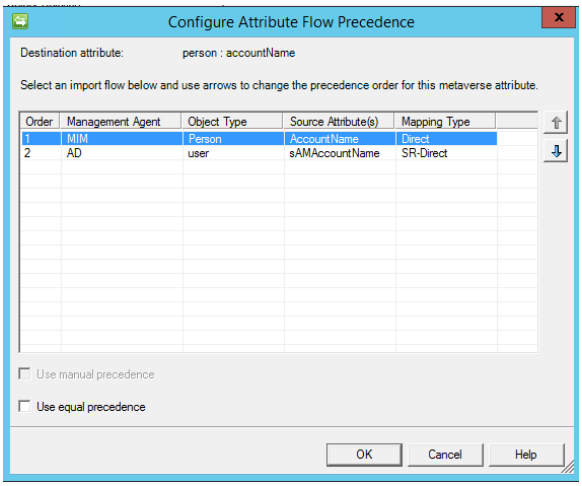
All the synchronization rules must appear.



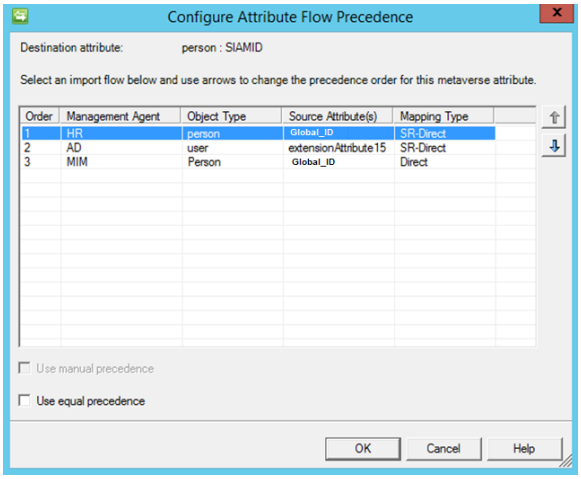
Configure rules precedence for the user class.

Go to the tab *Metaverse Designer*. Select the class person then click on Configure *Attribute Rules Precedence*.

Active Directory is authoritative for attribute *Email*.

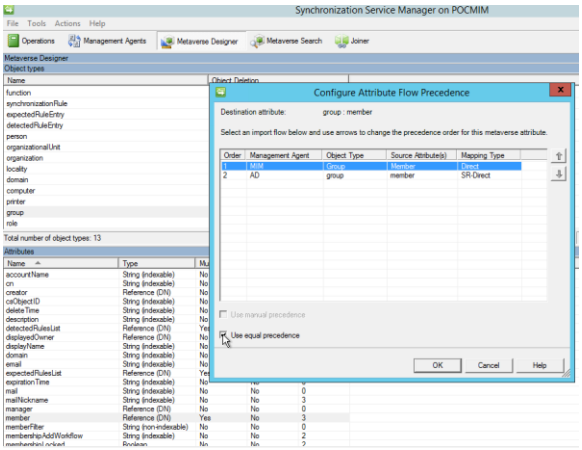


MIM portal is authoritative for the attribute *displayName* and *accountName*.



HR is authoritative on all other attributes like Global_ID.

3.16 CONFIGURE RULES PRECEDENCE FOR GROUP CLASS (METAVERSE SCHEMA)



You must configure equal precedence for all group attributes managed via the MIM 2016 portal and via Active Directory like *member*, *displayName*.

3.17 CONFIGURE RESOURCE CONTROL DISPLAY CONFIGURATION

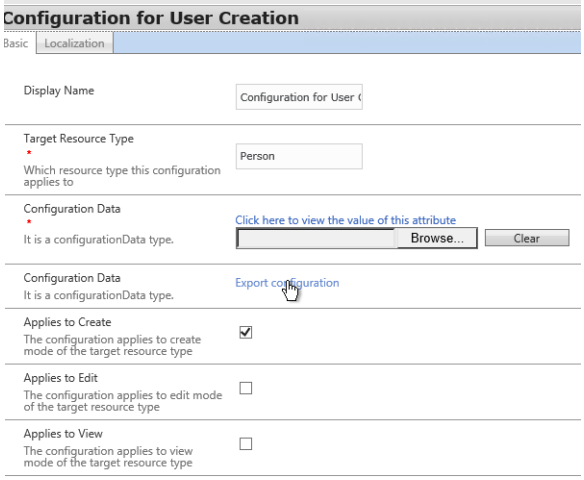
We need to configure the following fields as mandatory in the New user form: *First Name, Last Name, Company, Employee ID, Employee Type* and *Global_ID*.
To perform this action, we will use RCDC (*Resource Control Display Configuration*).

You can customize creation, editing and viewing form of each object type with resource Control Display Configuration as explained here:
https://social.technet.microsoft.com/wiki/contents/articles/24421.forefront-identity-manager-rcdc-regular-expression.aspx
https://social.technet.microsoft.com/Forums/en-US/4ec97bd5-c8bc-4c8c-be4b-8773c620355f/fim-2010r2-regular-expression-restrictions-for-dropdown-list?forum=ilm2

You can generate REGEX with this website https://regex101.com/

Go to *Administration | Resource Control Display Configurations*.

Enter *user* in the Search field.



Click on Export configuration link to backup the RCDC configuration.

Download the file
http://msreport.free.fr/articles/User-Creation V7.xml

Import the new RCDC (browse button).

Click on *Submit*.

Restart IIS with the command IISRESET.

In this example, we will define the rule on the RCDC and not in the attributes or binding to avoid applying this rule on all MIM 2016 forms.

You can define attribute format from the schema, but the validation field has a limit of 128 characters (the workaround is to edit the proper attribute in advance mode).
For specific attribute, we prefer to define rule only a specific form.
That's why we will define the format directly on the RCDC.
For Global_ID: *^[S][0-9]{9}[E][0-9]{9}$*
For EmployeeID: *^[H][R][S][0-9]{9}[E][0-9]{9}$*
For Company attribute, we must choose a value from this list: *ENTITY1, ENTITY2,* and *ENTITY3*
Each tab of the form is a tag named *<My:Grouping>*
Each field of a form is a tag named *<My:control>*

To define Global_ID and Employee ID, we will use a regex directly in the RCDC.

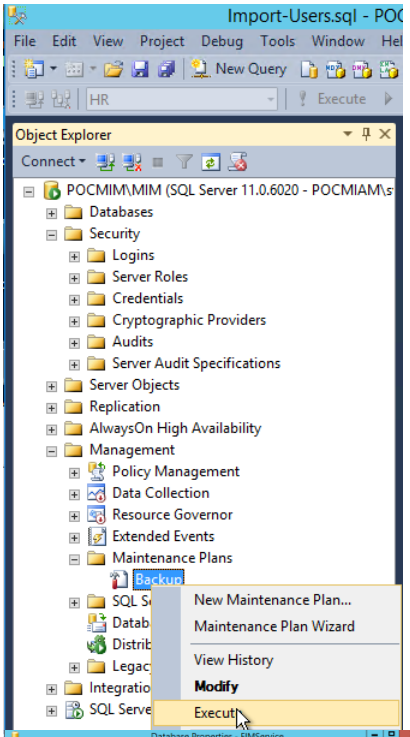
```
<my:Control my:Name="Global_ID" my:TypeName="UocTextBox" my:Caption="{Binding Source=schema, Path=Global_ID.DisplayName}" my:Description="">
<my:Properties>
<my:Property my:Name="Required" my:Value="true"/>
<my:Property my:Name="Columns" my:Value="34"/>
<my:Property my:Name="MaxLength" my:Value="20"/>
<my:Property my:Name="Text" my:Value="{Binding Source=object, Path=Global_ID, Mode=TwoWay}"/>
<my:Property my:Name="RegularExpression" my:Value="^[S][0-9]{9}[E][0-9]{9}$"/>
</my:Properties>
</my:Control>
```

For the company attribute, we will define the list of values directly on the RCDC.
http://www.wapshere.com/missmiis/listing-choices-in-rcdc-dropdowns
https://social.technet.microsoft.com/wiki/contents/articles/24421.forefront-identity-manager-rcdc-regular-expression.aspx
It's not possible to use Constant specifier because the synchronization engine doesn'nt have access to this information and could not translate the regex.
https://social.technet.microsoft.com/Forums/en-US/4ec97bd5-c8bc-4c8c-be4b-8773c620355f/fim-2010r2-regular-expression-restrictions-for-dropdown-list?forum=ilm2
Enter the following information in the RCDC.

```
<my:Control my:Name="Company" my:TypeName="UocDropDownList" my:Caption="{Binding Source=schema, Path=Company.DisplayName}" my:Description="">
<my:Options>
<my:Option my:Value="ENTITY1" my:Caption="ENTITY1" my:Hint="ENTITY1"/>
<my:Option my:Value="ENTITY2" my:Caption="ENTITY2" my:Hint="ENTITY2"/>
<my:Option my:Value="ENTITY3" my:Caption="ENTITY3" my:Hint="ENTITY3"/>
<my:Option my:Value="ENTITY1" my:Caption="ENTITY1" my:Hint="ENTITY1"/>
<my:Option my:Value="ENTITY2" my:Caption="ENTITY2" my:Hint="ENTITY2"/>
<my:Option my:Value="ENTITY3" my:Caption="ENTITY3" my:Hint="ENTITY3"/>
<my:Option my:Value="ENTITY1" my:Caption="ENTITY1" my:Hint="ENTITY1"/>
<my:Option my:Value="ENTITY3" my:Caption="ENTITY3" my:Hint="ENTITY3"/>
</my:Options>
<my:Properties>
<my:Property my:Name="Required" my:Value="true"/>
<my:Property my:Name="ValuePath" my:Value="Value"/>
<my:Property my:Name="CaptionPath" my:Value="Caption"/>
<my:Property my:Name="HintPath" my:Value="Hint"/>
<my:Property my:Name="ItemSource" my:Value="Custom"/>
<my:Property my:Name="SelectedValue" my:Value="{Binding Source=object, Path=Company, Mode=TwoWay}"/>
</my:Properties>
</my:Control>
```

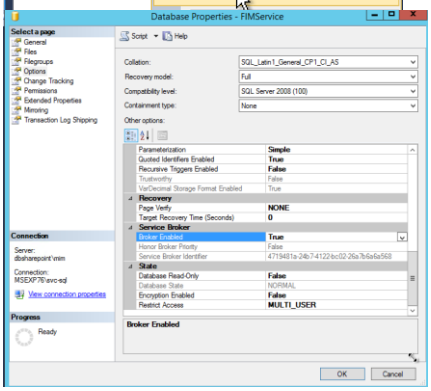
Perform the same thing for the edit form with the following file.
You can download the file http://msreport.free.fr/articles/User-Editing-V7.xml.

3.18 BACKUP THE POC ENVIRONMENT



A backup of the 4 virtual machines is performed every day at 3 AM. You could also perform a manual backup of SQL Server databases of POCMIM.

Start SQL Server Management Studio.
Go to *Management | Maintenances Plans* and right click on *Backup* then click on *Execute*.



To restore the MIM Synchronization service, https://technet.microsoft.com/en-us/library/fim-service-backup-and-restore-fim-2010-backup-and-restore-guide(v=ws.10).aspx

You must also enable again the broker on the *FIMService* database.
https://social.technet.microsoft.com/wiki/contents/articles/16834.fim-troubleshooting-the-sql-server-service-broker-must-be-enabled-on-the-forefront-identity-manager-service-database.aspx

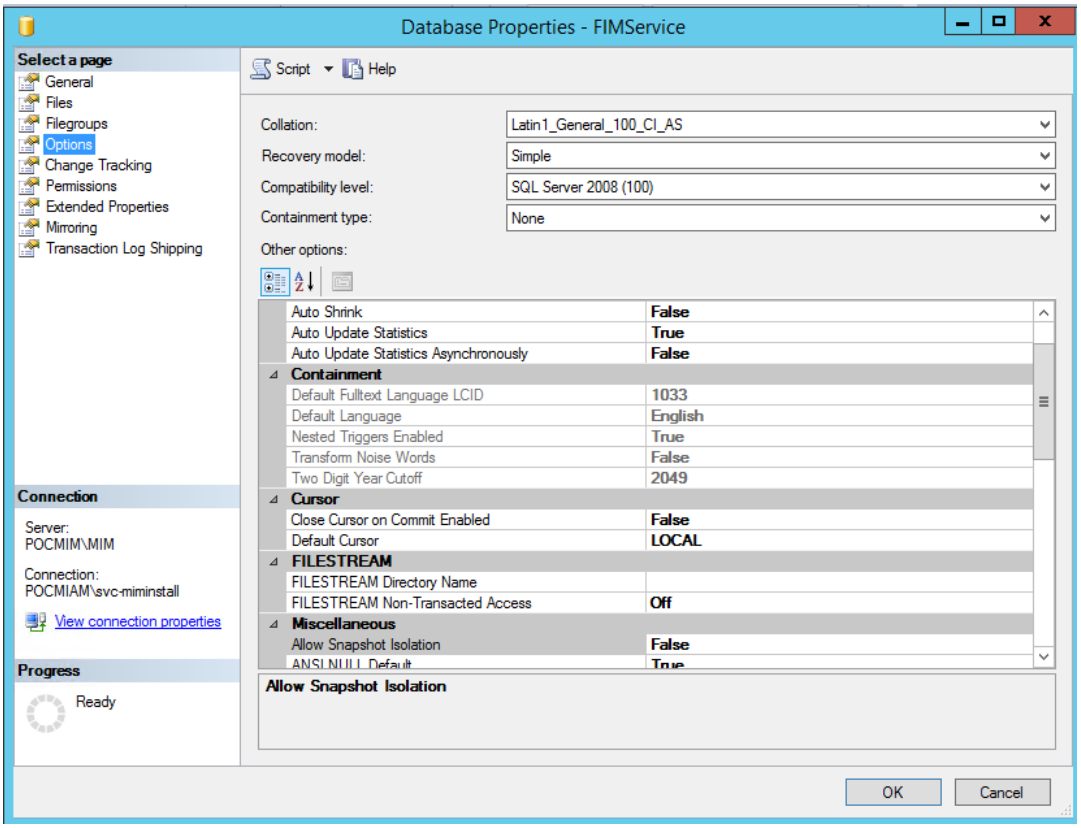
The following error appears if you don't enable the brocker service.

Log Name: Forefront Identity Manager
Source: Microsoft.ResourceManagement
Date: 05/02/2017 16:39:32
Event ID: 3
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: POCMIM.msexp76.intra
Description:
Microsoft.ResourceManagement.Service: System.InvalidOperationException: The SQL Server Service Broker must be enabled on the Forefront Identity Manager Service database. Refer to the documentation of the SQL Server Service Broker, or the Transact-SQL ALTER DATABASE statement, for instructions on how to enable it.
at Microsoft.ResourceManagement.Data.DataAccess.ValidateConnectionString(String connectionString, Boolean validateBroker)
at Microsoft.ResourceManagement.Data.DatabaseConnection.InitializePrimaryStoreConnectionString()
at Microsoft.ResourceManagement.Data.DatabaseConnection.get_ConnectionString()
at Microsoft.ResourceManagement.Data.DatabaseConnection.Open(DataStore store)

at Microsoft.ResourceManagement.Data.TransactionAndConnectionScope..ctor(Boolean createTransaction, IsolationLevel isolationLevel, DataStore dataStore)
at Microsoft.ResourceManagement.Data.TransactionAndConnectionScope..ctor(Boolean createTransaction)
at Microsoft.ResourceManagement.Data.DataAccess.GetDatabaseVersion(Int32& databaseVersion, String& databaseBinaryVersion)
at Microsoft.ResourceManagement.Service.PlatformBasics.CheckDatabaseVersion()
at Microsoft.ResourceManagement.Service.PlatformBasics.Initialize(Boolean isService)
at Microsoft.ResourceManagement.Service.Application.CreatePlatformBasics(Boolean initialize, Boolean isService)
at Microsoft.ResourceManagement.Service.Application.Start()

3.19 DATABASE SIZE

MIM Service database will generate lots of log file.
To avoid this, go to the properties of the SQL Server database named *FIMService*.
Go to the tab *Options* then select Simple for *Recovery model*.

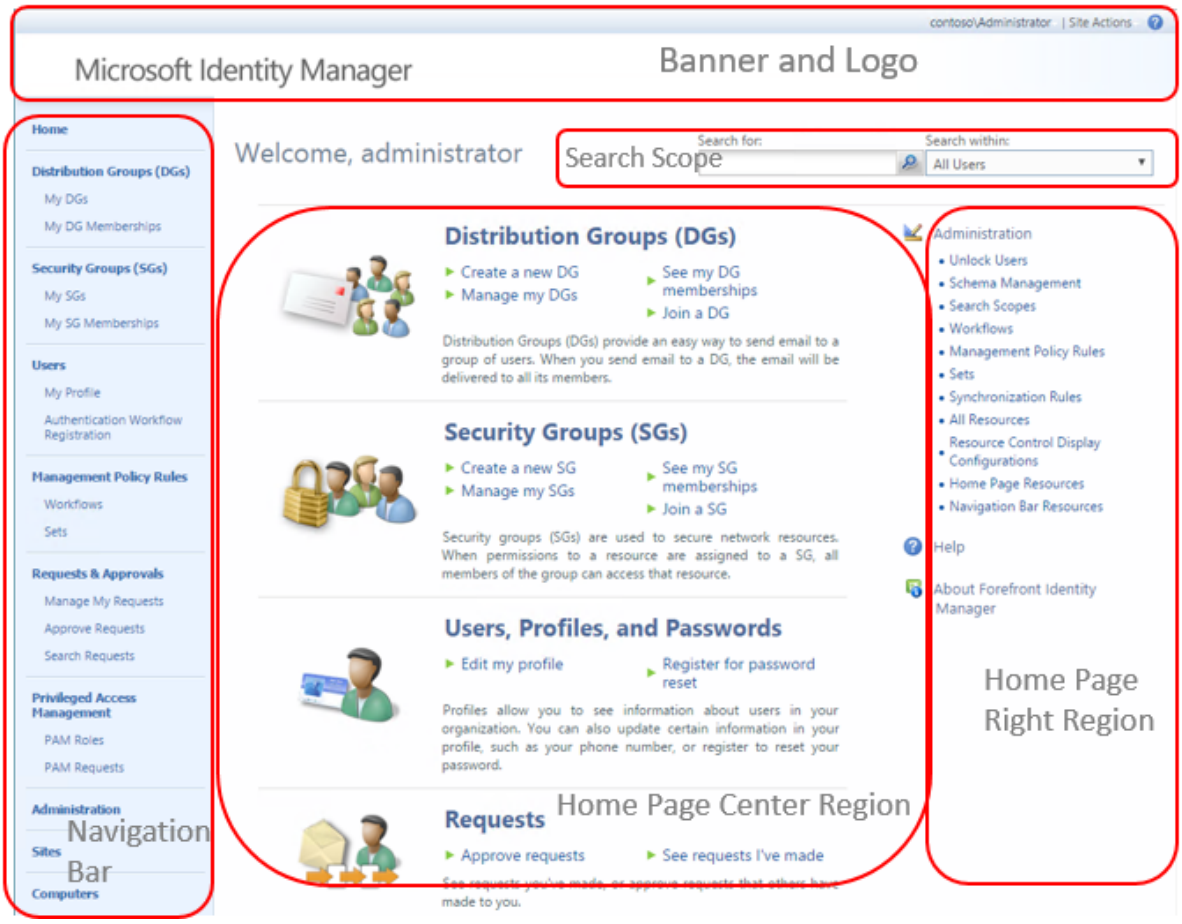


Create also a task which will save the database then remove the log (maintenance plans).

3.20 MIM PORTAL CUSTOMIZATION

3.20.1 MIM Portal components

MIM Portal is made of several components that can be configured through the UI.

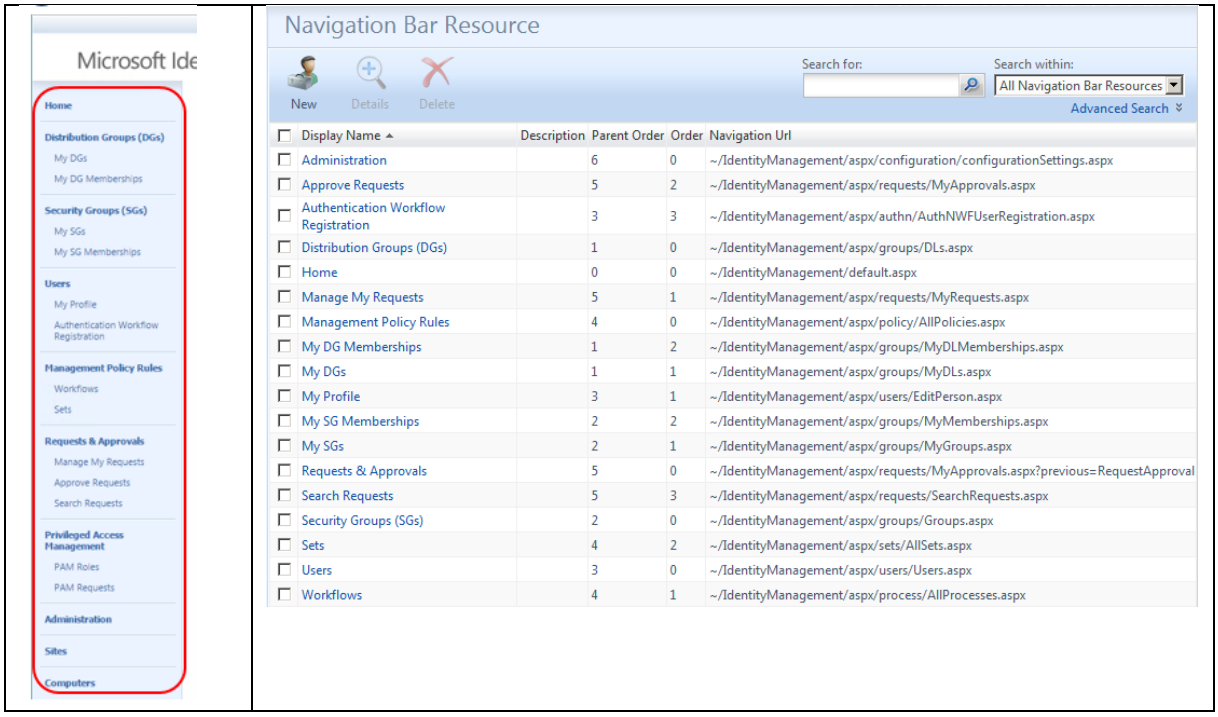


The Banner and Logo appear at the top of each MIM Portal page.
You can set them in the Portal Configuration resource. There is only one Portal Configuration resource for each MIM deployment. It also contains other MIM Portal global settings, such as cache duration.

The Navigation Bar is the vertical menu on the left side of the MIM Portal. The Navigation Bar helps the user move among various self-service and information technology professional (IT pro) tasks. The list consists of selected Navigation Bar resources. Each item in the list points to a unique URL.

Search scopes appear on the upper right area of each MIM Portal page. A search scope includes a search input box and a search scope drop-down list. The search scope is critical for controlling what appears in a page list view, that is, the main area of a portal page where resources are listed. For example, the search scope **All Distribution Groups (DGs)** displays all the DGs in the system, while the search scope **My Distribution Groups (DGs)** displays only the DGs for which the requesting user is an owner. Users can enter their search string in the search input box and click the search icon beside the box to look for matches within the search scope that is defined in the drop-down box. Each entry in the search scope drop-down box maps to a Search Scope resource. IT pros can define the behavior of different search scopes and show different search scopes on different MIM pages by creating and modifying a Search Scope resource.

3.20.2 Navigation bar configuration



Display Name	Description	Parent Order	Order	Navigation Url
Administration	6	0		~/IdentityManagement/aspx/configuration/configurationSettings.aspx
Approve Requests	5	2		~/IdentityManagement/aspx/requests/MyApprovals.aspx
Authentication Workflow Registration	3	3		~/IdentityManagement/aspx/authn/AuthNWFUserRegistration.aspx
Distribution Groups (DGs)	1	0		~/IdentityManagement/aspx/groups/DLs.aspx
Home	0	0		~/IdentityManagement/default.aspx
Manage My Requests	5	1		~/IdentityManagement/aspx/requests/MyRequests.aspx
Management Policy Rules	4	0		~/IdentityManagement/aspx/policy/AllPolicies.aspx
My DG Memberships	1	2		~/IdentityManagement/aspx/groups/MyDLMemberships.aspx
My DGs	1	1		~/IdentityManagement/aspx/groups/MyDLs.aspx
My Profile	3	1		~/IdentityManagement/aspx/users/EditPerson.aspx
My SG Memberships	2	2		~/IdentityManagement/aspx/groups/MyMemberships.aspx
My SGs	2	1		~/IdentityManagement/aspx/groups/MyGroups.aspx
Requests & Approvals	5	0		~/IdentityManagement/aspx/requests/MyApprovals.aspx?previous=RequestApproval
Search Requests	5	3		~/IdentityManagement/aspx/requests/SearchRequests.aspx
Security Groups (SGs)	2	0		~/IdentityManagement/aspx/groups/Groups.aspx
Sets	4	2		~/IdentityManagement/aspx/sets/AllSets.aspx
Users	3	0		~/IdentityManagement/aspx/users/Users.aspx
Workflows	4	1		~/IdentityManagement/aspx/process/AllProcesses.aspx

Each entry in the Navigation Bar has a corresponding Navigation Bar resource that you can use to customize. You can customize the following attributes in a navigation bar resource:

- Display Name

This is the displayed label of the Navigation Bar resource. This attribute is mandatory, and it takes a string of up to 448 characters, inclusive

- Description

This attribute is a field where Portal Administrators can enter comments on the Navigation Bar resource. It does not appear anywhere else in the portal other than in the detail view of a Navigation Bar resource. This attribute is optional. It takes a string of up to 448 characters, inclusive

- Navigation URL

IT pros can use this field to specify the URL of the target page. This URL must be unique among all Navigation Bar resources. If it is a duplicate of another Navigation Bar Resource, neither Navigation Bar resource will appear in the Navigation Bar. This field does not support new pop-up URLs, and will not appear in the Navigation Bar if a pop-up URL is used. It supports only relative URLs, such as *~/identitymanagement/default.aspx*

- Usage Keyword (optional)

Used to customize which set of users can see a given Navigation Bar resource

- Resource Count (optional):

An XPath expression that shows the count of matches the XPath expression satisfies

Arrange Navigation Bar Resource Positions

- Parent Order

There are two levels of order in Navigation Bar. Navigation Bar resources in the first-level order appear as section titles, bold and indented towards the left
Parent Order determines which first-level Navigation Bar resource the current Navigation Bar resource appears under. The lower the Parent Order, the higher in the Navigation Bar the resource appears

Zero is reserved for out-of-box Home Navigation Bar resources and cannot be reused for other Navigation Bar resources. Microsoft recommends that you leave some room between the numbers so that new Navigation Bar resources can be created between existing resources.

- Order

Order determines where a Navigation Bar resource will be placed under the first-level Navigation Bar resource. The lower the Order, the higher in the section it appears
Zero means that the Navigation Bar resource is a first-level Navigation Bar resource. Microsoft recommend that you leave some room between the numbers so that new Navigation Bar resources can be created between existing resources

When a language pack is installed, users can customize how Navigation Bar resources are localized via the **Localization** tab of the Navigation Bar resource. This tab consists of the following settings:

3.20.3 Home Page configuration

Home Page Resource

New Details Delete

Search for: Search within: All Home Page Resources

Advanced Search

Display Name	Description	Region	Parent Order	Order	Navigation Url
About Forefront Identity Manager		3	3	0	javascript:ILM2AboutWindow()
Administration		3	1	0	~/IdentityManagement/aspx/configuration/configurationSettings.aspx
All Resources		2	1	10	~/IdentityManagement/aspx/customized/AllCustomizedObjectTypes.aspx
Approve requests		1	4	1	~/IdentityManagement/aspx/requests/MyApprovals.aspx
Create a new DG		1	1	1	javascript:PopupPage("/IdentityManagement/aspx/groups/CreateDistributionList.aspx");
Create a new SG		1	2	1	javascript:PopupPage("/IdentityManagement/aspx/groups/CreateSecurityGroup.aspx");
Distribution Groups (DGs)	Distribution Groups (DGs) provide an easy way to send email to a group of users. When you send email to a DG, the email will be delivered to all its members.	1	1	0	~/IdentityManagement/aspx/groups/AllDLs.aspx
Domain Configurations		4	1	50	~/IdentityManagement/aspx/customized/CustomizedObjects.aspx?type=DomainConfiguration&display=Domain+Configurations
Edit my profile		1	3	1	javascript:PopupPage("/IdentityManagement/aspx/users/EditPerson.aspx");
Email Templates		4	1	70	~/IdentityManagement/aspx/customized/CustomizedObjects.aspx?type=EmailTemplate&display=Email+Templates
Filter Permissions		4	1	60	~/IdentityManagement/aspx/customized/CustomizedObjects.aspx?

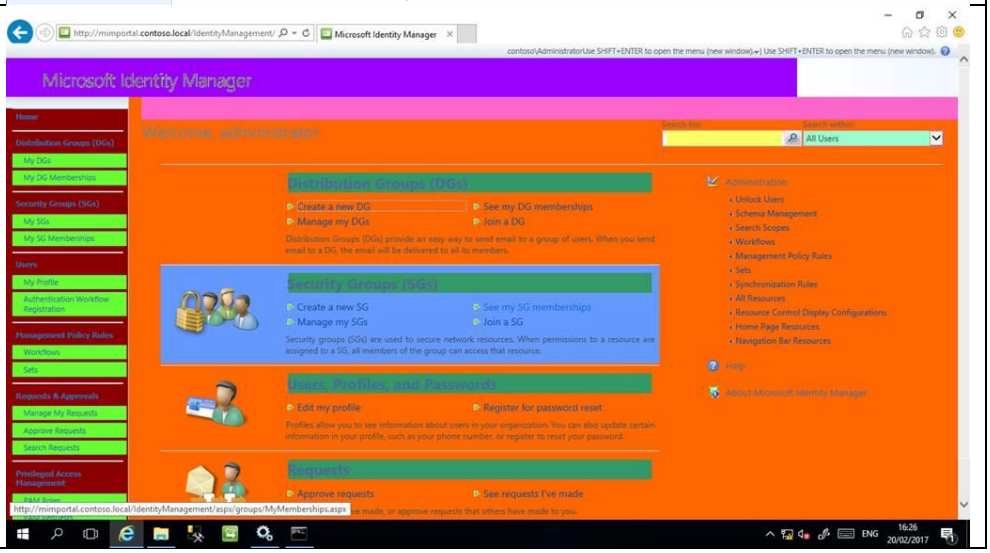
Home Page items are dynamically controlled by Management Policy Rules. Each entry on the Home Page has a corresponding customizable Home Page resource.
Home Page UI is divided into three regions:

- Center
- Right
- Administration

Position of each item is controlled by Parent Grouping and Order attributes within a given Region.
More details are available in this article [Understanding Configuring and Customizing the FIM Portal]

3.20.4 CSS customization

MIM portal, as a SharePoint solution, can also be leveraging SharePoint themes and CSS style sheet to customize the UI look and feel.
The colors, layout and spacing of MIM Portal items can be changed by editing the FIM.CSS style sheet.
The style sheet located in C:\Program Files\Common Files\Microsoft Shared\web server extensions\<12,14,16 depending on SharePoint Version>\TEMPLATE\LAYOUTS\1033\fim.css can be customized to match the company web sites branding.

Default CSS template	
Customized CSS template	

All the relevant information to edit and customize the CSS style sheet are available in this article [Introduction to Configuring and Customizing the FIM Portal]

4 USE CASES (STEP BY STEP)

4.1 PROVISION NEW USERS

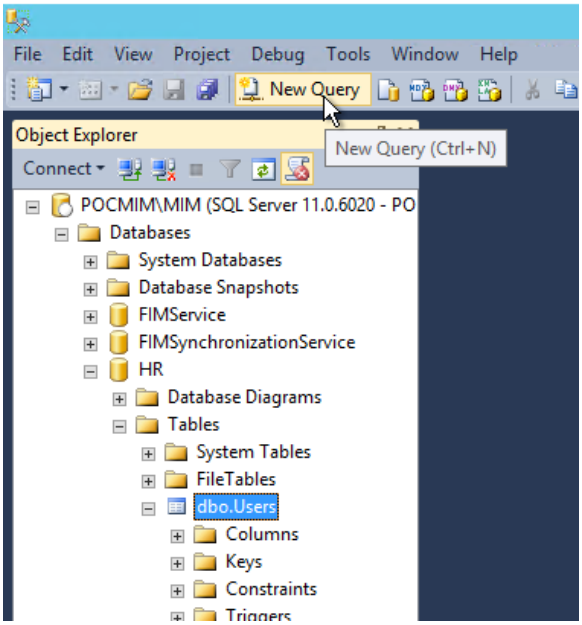
4.1.1 Global overview

Description:
Create a new user in the HR database.

Success criteria (after one hour):
User has an Active Directory user account and an Exchange 2013 mailbox.
User is created on MIM 2016 portal.
The SamAccountName must be generated based on these rules (the second rule is applied only in case of conflict).
FirstName + "." + LastName
FirstName + "." + LastName + "-" + random value
If EmployeeType is equal to External, DisplayName is updated based on this rule:
Last name + space + first name + -external
Else
Last name + space + first name
An Exchange 2013 mailbox is created on POCEXCH1.
The target database is determined based on the value of the HR entity (*DIVISION* attribute).
User is created in the OU corresponding to his company name.
All HR attributes has been copied in the MIM 2016 portal and in Active Directory.
Manager is updated properly in MIM 2016 portal and Active Directory based on the *EMPLOYEE_ID* reference.

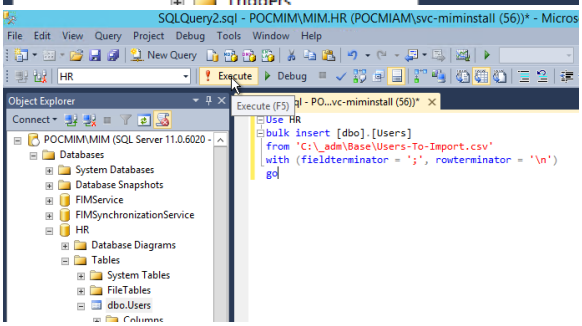
4.1.2 Step by step

Prepare two files: one with a list of entries to import, one with a list of available entries (for the next import).
Connect to the server pocmim.westeurope.cloudapp.azure.com with the user account *pocmiam\svc-miminstall*. Start SQL Server Management Studio.
Cut the line corresponding to the new user in the file *C:_adm\Base\Available-Users-To-Import.csv*.
Past the line to the file named *C:_adm\Base\Users-To-Import.csv*.



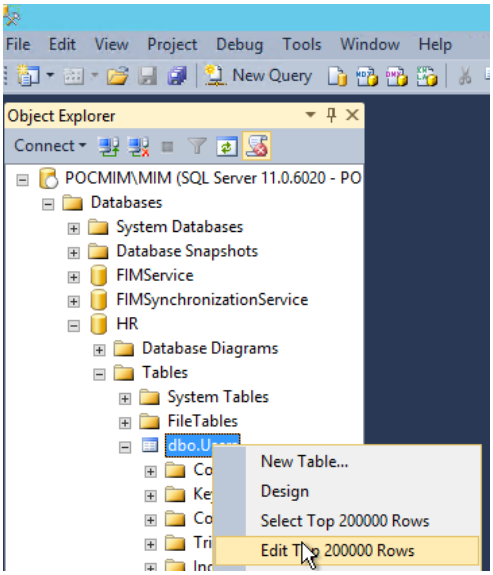
Insert the content of the file *C:_adm\Base\Users-To-Import.csv* in the existing table.

Click on the button *New Query*.

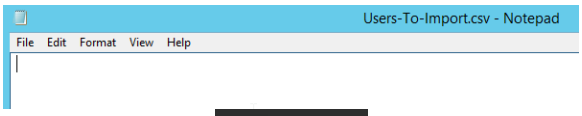


Copy the query below.
Use HR
bulk insert [dbo].[Users]
from 'C:_adm\Base\Users-To-Import.csv'
with (fieldterminator = ';', rowterminator = '\n')
go

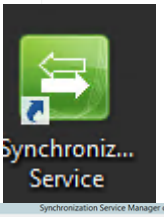
Click on the button *Execute*.



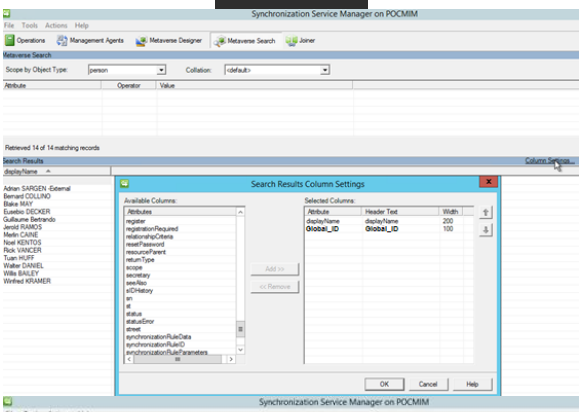
Edit the table to review the result.
A new line is created in the Users table (HR database).



Remove the content of the file *C:_adm\Base\Users-To-Import.csv*.

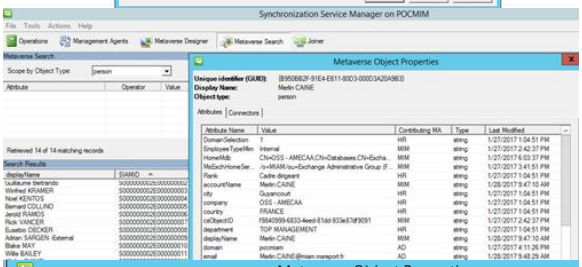


Start MIIS.EXE (synchronization Service) application.

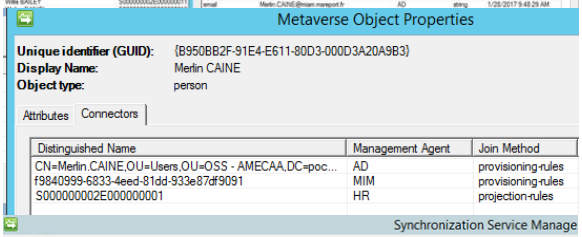


List all existing users in FIM Metaverse.

Configure the Column settings to display the *Global_ID* attribute.

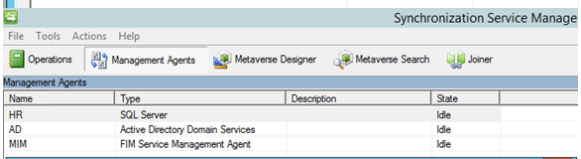


Display the setting of a user.



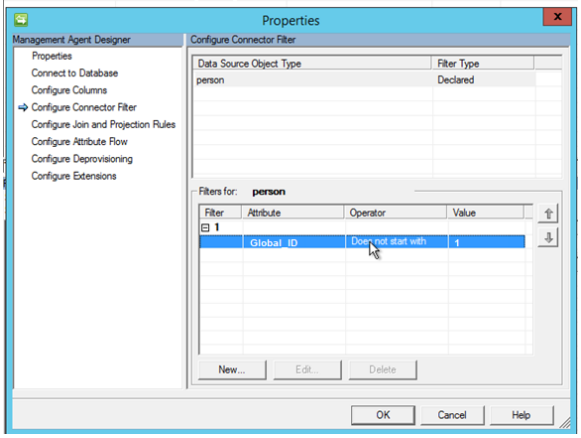
Go to the *Connector* tab.
You can review the values of each attribute in each Connector space (management agent read only copy of all objects of the target system).

You must now add the new user.

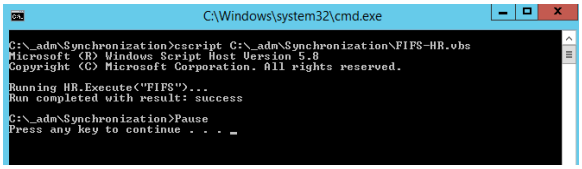


Go to the tab *Management Agents* tab.

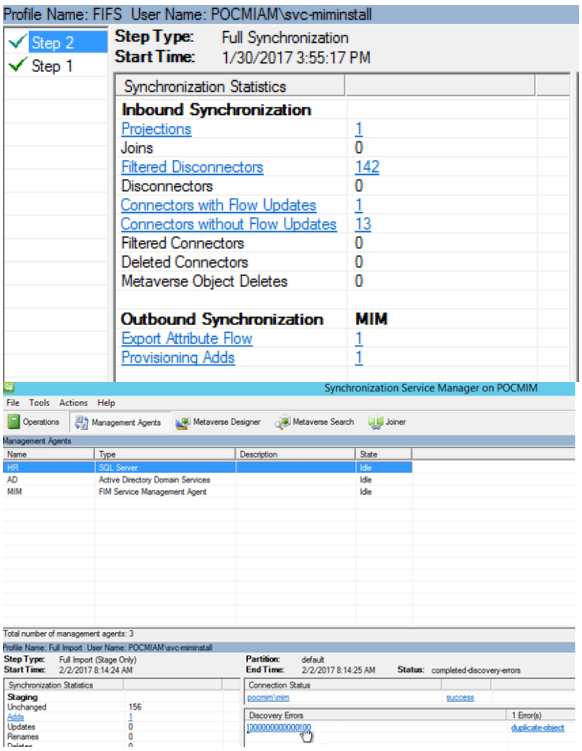
Go to the properties of the Management *HR* in then click on *Configure Connector Filter*.



Only user with a valid *Global_ID* will be added.
Global_ID start by the digit 1.



Start the script *C:_adm\Synchronization\StartFimSynchronization - manual.bat*.
This script will start the full synchronization cycle.
You need to press on a key to resume the script after each step.
Full Import HR /Full Synchronization HR
Export MIM
Full Import MIM / Full Synchronization MIM
Export AD
Export HR
Full Import AD / Full Synchronization AD
Full Import HR



Go to the *Operation* tab.
You can review the result of the step:
Full Import HR /Full Synchronization HR

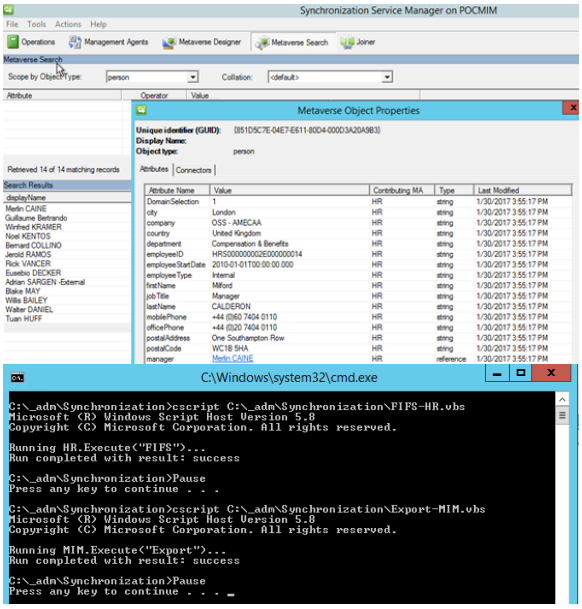
<u>Optional task (only in case of error):</u>

If MIM display the error *duplicate object*, you have imported the same user <u>multiple times</u>.

To solve a *duplicate object* error, list all the users with the Global_ID in conflict by starting this request.
use HR
*select * from [dbo].[Users] where Global_ID = '100000000001'*

Then remove the lines in conflict in SQL Server:
use HR
delete from [dbo].[Users] where Global_ID = '100000000001'

<u>Click on the Save button.</u>
You must add again the user in the HR SQL Server database.
<u>End of optional task.</u>

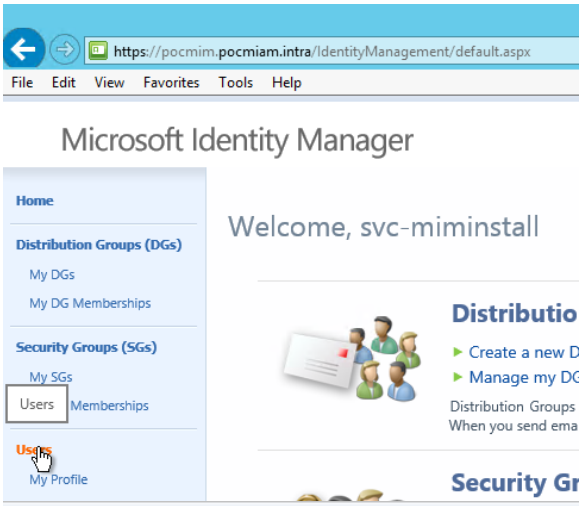


This new user doesn't have currently a DisplayName.

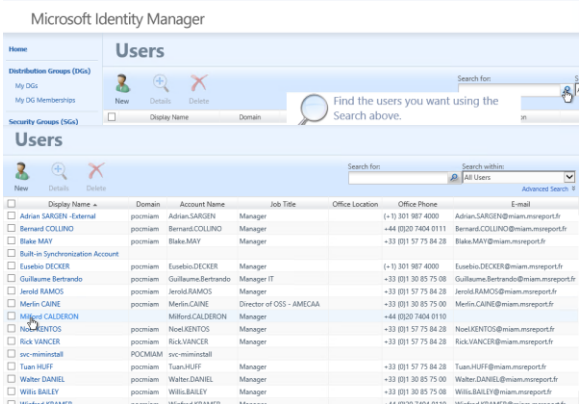
This attribute will be generated later by a MIM 2016 workflow.

Click on a key to resume the script.
An export is performed to the *MIM* management agent.

The new user has been created on the MIM service database and could be managed via the MIM 2016 web portal. The attribute *AccountName* or *DisplayName* are empty for the moment.



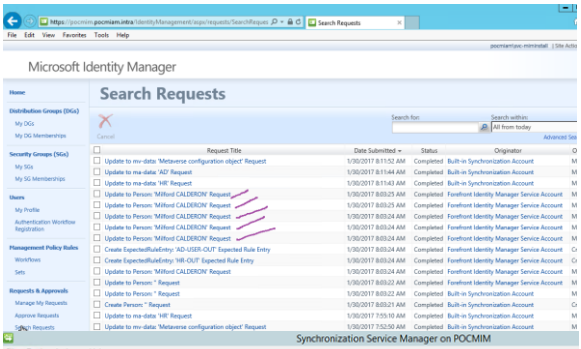
Connect to the website:
https://pocmim.pocmiam.intra/IdentityManagement



Click on Search button.

You can see the new user.

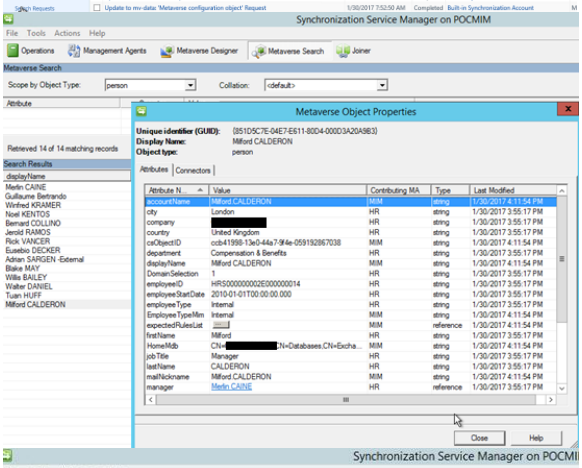
The user has no email, domain or SID for the moment.



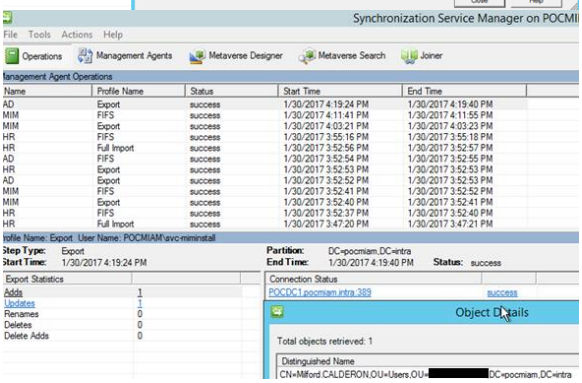
Press a key to continue synchronization script.

You will now import the MIM service configuration. A workflow has generated values for *DisplayName*, *HomeMdb* (Exchange database) and *AccountName*.

You can review the workflow activities by click on *Request & Approvals*.

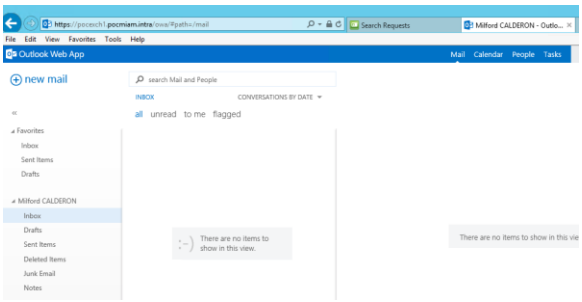


Go to the Metaverse Search.
The *accountName*, *HomeMdb* and *DisplayName* have values.



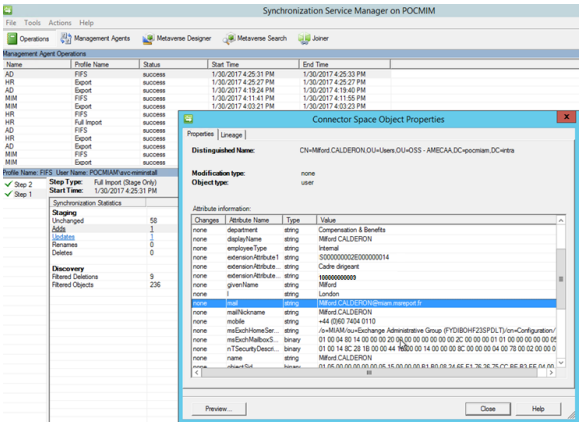
Press a key to continue synchronization script.
The new user will be created on Active Directory.

The user has been created in Active Directory and added automatically in dynamic group (*Internal-Users* or *External Users*)

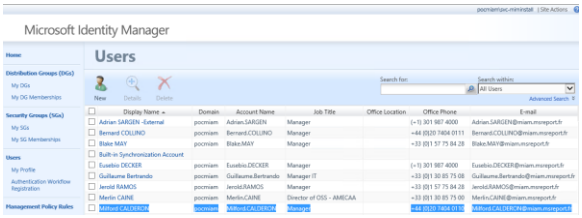


The user has been created properly in Active Directory and has an Exchange mailbox.

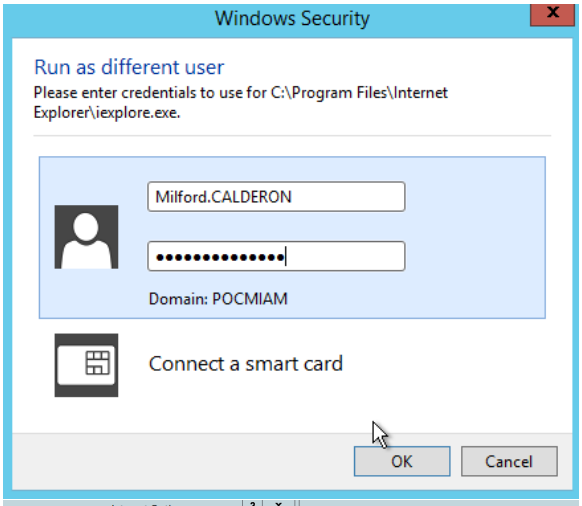
To connect to his Exchange mailbox:
https://pocexch1.pocmiam.intra/owa



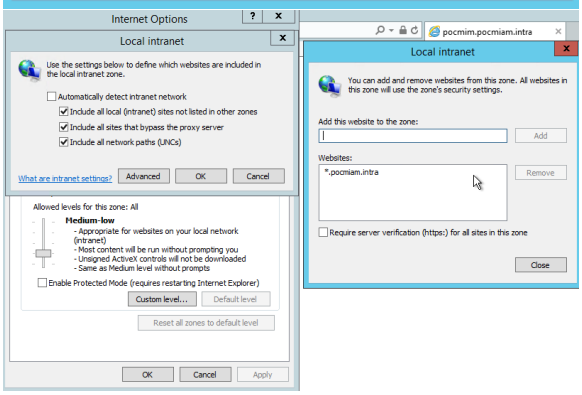
Press a key to resume the synchronization script.
This will export change in SQL Server (no change).
Press a key again. This will import the changes in the AD Connector space.
Exchange Recipient Address Policy has generated an email address to the new user.
MIM has imported it to the AD connector space.
The synchronization has updated the FIM Metaverse and the connector space of all others MIM 2016 Management Agent.
That's why an update must be exported to the MIM Management Agent.



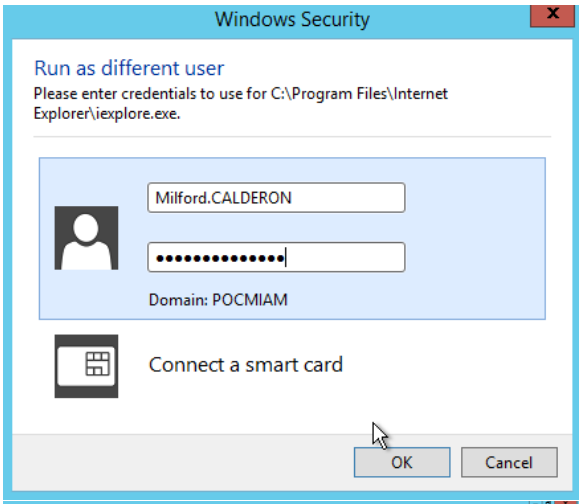
Press a key to continue the synchronization.
This will import all changes from the HR database (no change).
Start the script *C:_adm\Synchronization\StartFimSynchronization.bat.*
This will perform all the synchronization steps without manual action.
Go to the MIM portal again:
https://pocmim.pocmiam.intra/IdentityManagement
The user has now an email address.



Start Internet Explorer in the context of the new user account.

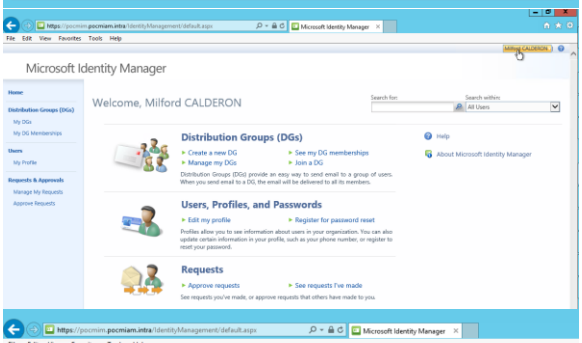


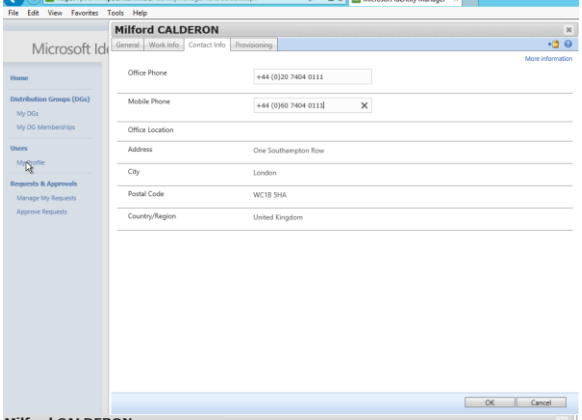
Add **.pocmiam* in the local Intranet.



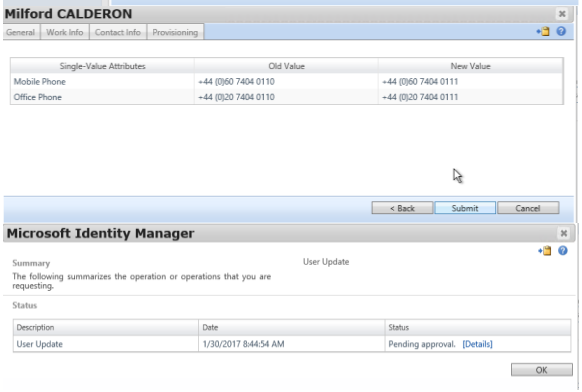
Start Internet Explorer in the context of the new user account.

Go to the MIM 2016 portal.
https://pocmim.pocmiam.intra/IdentityManagement

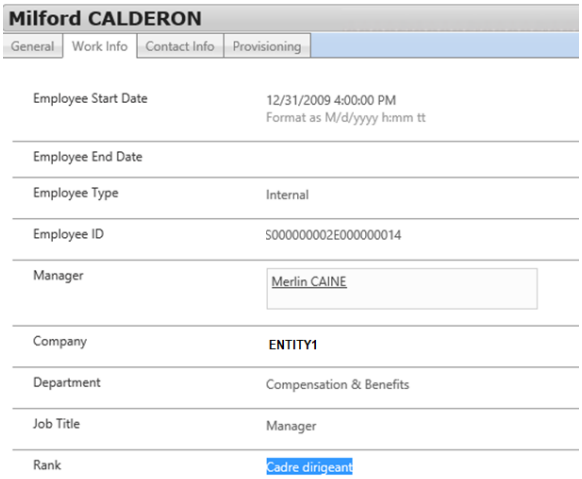




You can now use the MIM 2016 portal.
User can update his phone number (require Manager approval) if the Type of this user is equal to *Cadre dirigeant*.



Click on *Submit* button.



This change requires an approval because this user has a *Type* equal to *Cadre Dirigeant*.

4.2 DEPROVISION

4.2.1 Global overview

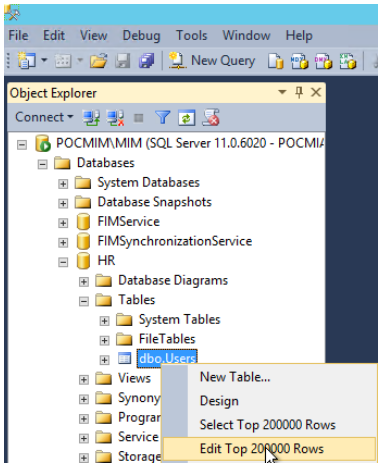
Test 1: user account (based on *EmployeeEndDate* attribute) are disabled automatically 30 days after departure and move into a *DisabledUsers* OU.
Test 2: user account (based on *EmployeeEndDate* attribute) are removed automatically 365 days after departure. Exchange mailbox become a disconnected mailbox and will be remove after 30 days.
Test 3: remove user in Active Directory.
Test 4: remove user in HR database.
Test 5: remove user in Active Directory.

Take care of the format of date in HR database (US format - MM/dd/yyyy).

Success criteria:
Test 1: user is disabled and moved in the *DisabledUsers* OU.
Test 2: user is removed in Active Directory, MIM portal and SQL server portal.
Test 3: user is recreated in Active Directory (new user account)
Test 4: user is removed in MIM portal and Active Directory.
Test 5: objects is disconnector in RH and AD then the object is deleted in Metaverse and remove also from MIM portal.

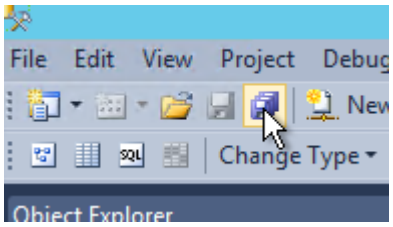
4.2.2 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.
Start SQL Server Management Studio. Click on *Connect*.

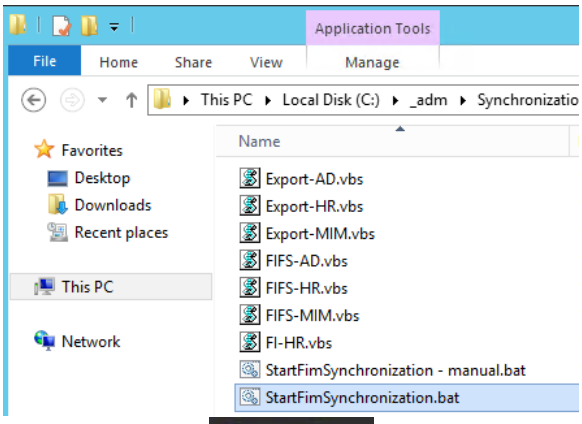


Edit the Users SQL Server table.

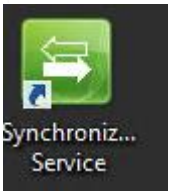
Use the user you provision previously. In this example: *S000000002E000000014.*
Set the *Employee End Date* to the value 03/03/2016 (**US format**).



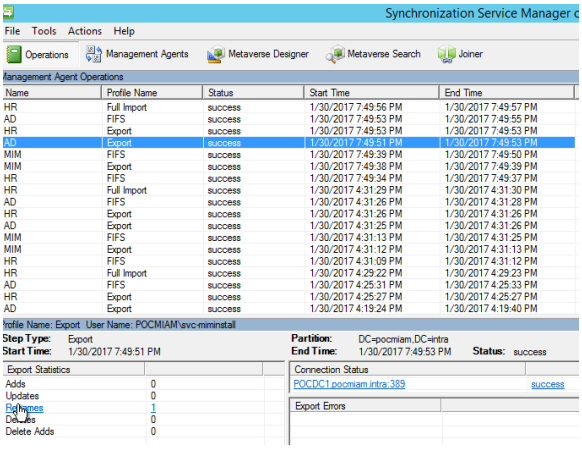
Go the next line and save the change.



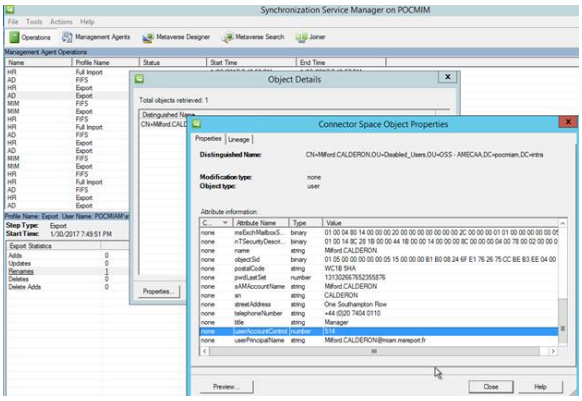
Start the synchronization cycle:
C:_adm\Synchronization\StartFimSynchronization.bat



Start the Synchronization Service console and review the change.



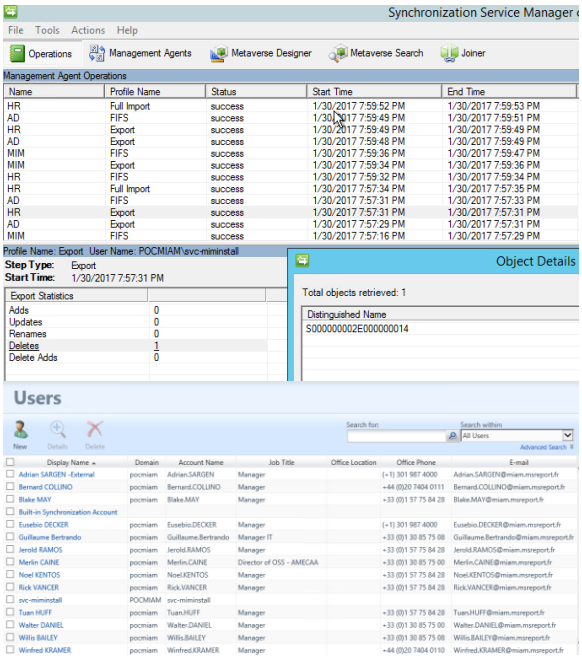
Go to the tab *Operations*.



Review the result of the AD Export operation.
The user account has been moved and disabled.
(End of test 1)

Go again in the SQL Server table *Users*.
Use the user you modify previously. In this example: *S000000002E000000014.*
Set the *Employee End Date* to the value 11/01/2015 (US date).

Start all synchronization cycle <u>2 times</u> because MIM service requires time to generate the list of ERE to delete a user account in the target system.
C:_adm\Synchronization\StartFimSynchronization.bat

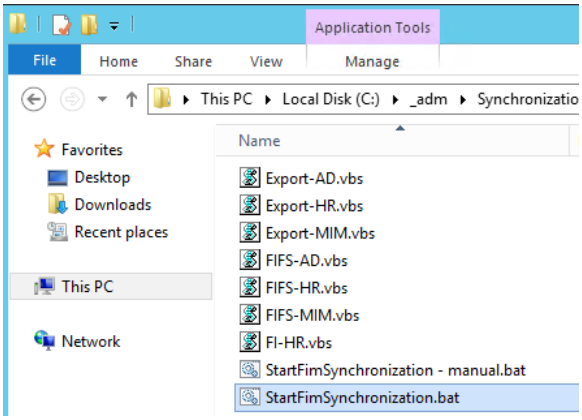


The Active Directory user account is removed.
The entry is the *Users* SQL server table is also removed.

Start again the synchronization script.

The user is also removed in the MIM service and in the Metaverse.

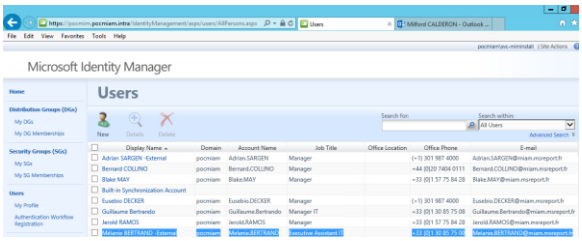
Recreate a new user in the HR database with the same Global_ID of the user you removed previously.



Start all synchronization cycle.
C:_adm\Synchronization\StartFimSynchronization.bat

Wait 30 seconds and start again the synchronization steps.
A new user account is recreated in AD and the MIM 2016 portal.

Start again the synchronization.

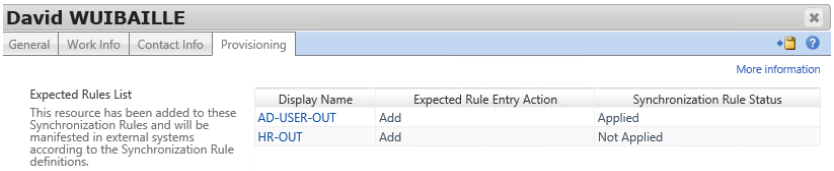


The user is recreated in Active Directory and in the MIM 2016 portal.

(End of test 2)

Delete a standard user (not a manager or a top level user) in Active Directory
Start the synchronisation <u>script 2 times</u> and check result.
The user is recreated in Active Directory (new SID).
(End of test 3)

Delete s standard user (not a manager or a top level user) in HR database.
Start the synchronisation <u>script 3 times</u> and check result.
The user is not deleted in Active Directory and MIM 2016 portal but is disonnect from HR management agent.



(End of test 4)
Remove again the user in Active Directory.
Start the synchronization script.
The user is disconnector in AD and HR. That's why the user is deleted in the Metaverse. Then the user is deleted to MIM 2016 portal because the Metaverse object id deleted.
(End of test 5)

4.3 CHANGE USER FIRST NAME AND/OR LAST NAME

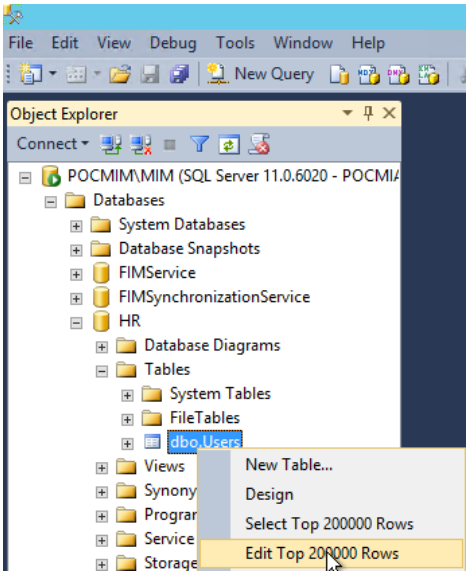
4.3.1 Global overview

HR team changes the *FIRST_NAME* or *LAST_NAME*.

Success criteria
The user account is renamed in Active Directory.
The *SamAccountName, mailNickName* and *UserPrincipalName* attributes are changed automatically.
Exchange 2013 will update email address based on *Exchange Recipient Address Policies*.

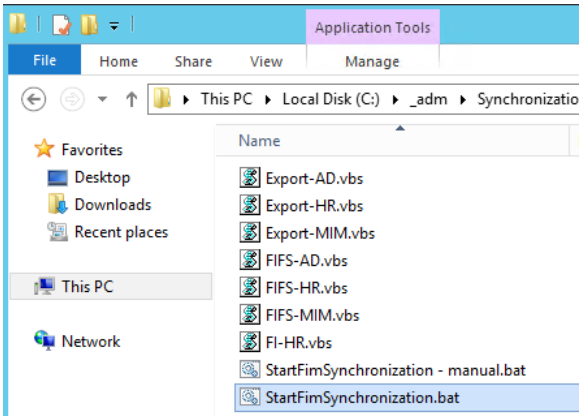
4.3.2 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.
Start SQL Server Management Studio.
Click on *Connect*.



Edit the *Users* SQL Server table.

Change the *LAST_NAME* for a user who exists in the Metaverse (in this example *S000000002E000000014*).

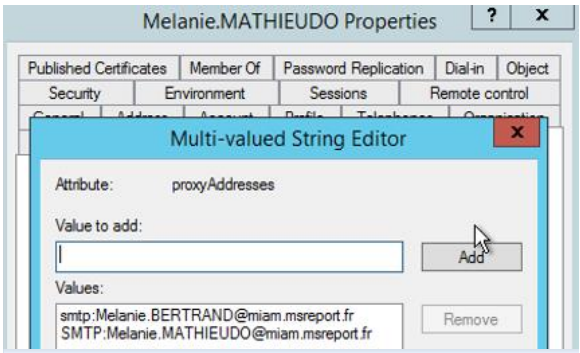


Start the synchronization script.
C:_adm\Synchronization\StartFimSynchronization.bat

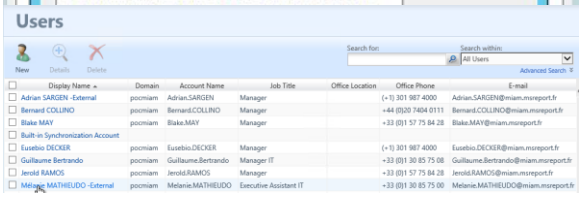
Wait 30 seconds and start again the synchronization script.

Wait 30 seconds and start again the synchronization script.

The Active Directory user account is renamed.
The *SamAccountName* and *UserPrincipalName* are changed.



The primary email address changes. The old email address is kept as secondary email address (email alias).



The user account is updated on the MIM 2016 portal.

4.4

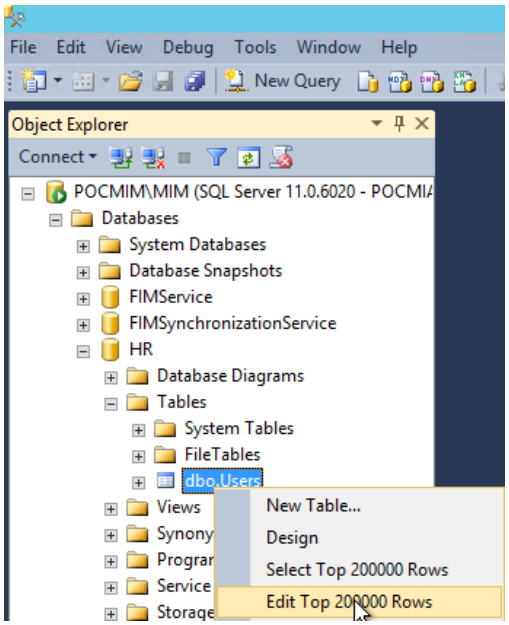
4.5 CHANGE HR INFORMATION

The user is moved to a new entity. The change is performed from HR system and consolidates in the HR database (the attributes *DIVISION*, *DEPARTMENT*, *JOB_TITLE*, *MANAGER*, *EmployeeEndDate*, *EmployeeStartdate*, *EMPLOYEE_ID* and *EMPLOYEE_TYPE* have been updated). Global_ID is not changed.
If *DIVISION* changes, the Exchange mailbox is moved on the proper mailbox database (require an additional script to move Exchange data).

Success criteria:
The user account is updated in MIM 2016 portal and Active Directory.
The user is moved automatically in the OU corresponding to his new HR entity.

4.5.1 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.
Start SQL Server Management Studio.
Click on *Connect*.

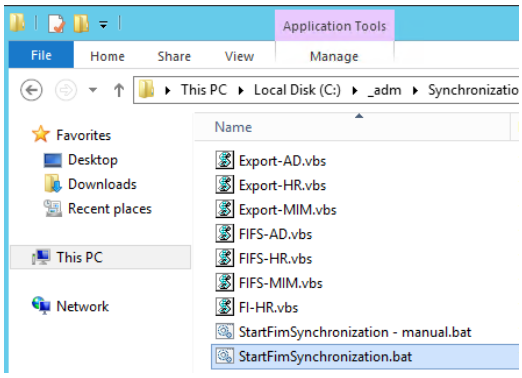


Edit the *Users* SQL Server table.

Change the attributes *DIVISION*, *DEPARTMENT*, *JOB_TITLE*, *MANAGER*, *EmployeeEndDate*, *EmployeeStartdate*, *EMPLOYEE_ID* and *EMPLOYEE_TYPE*. Use the user account created previously.

<u>Notes:</u> you must use a valid company name (company which has an Exchange database and root OU created in Active Directory).

Take care of the format of EMPLOYEE_ID
Exemple of valid value S000000008E100000121.



Start all synchronization steps:
C:_adm\Synchronization\StartFimSynchronization.bat

The Active Directory AD account is moved in the OU corresponding to the company.
The Exchange mailbox is also moved in the target Exchange 2013 mailbox database.

Notes: the mailbox content is not moved. It's not supported to change *HomeMdb* to move Exchange mailbox to a new database. The workaround is to start a PowerShell script via a MIMWALL workflow to start the Exchange PowerShell command named *New-MoveRequest*.
http://practical365.com/exchange-server/moving-exchange-server-2013-mailboxes/

4.6 EMPLOYEETYPE CHANGED BY HR TEAM

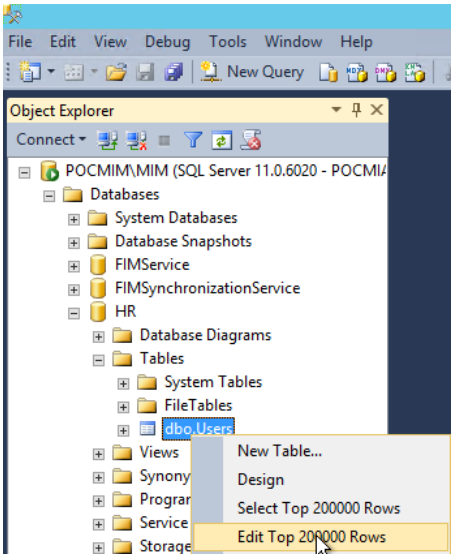
4.6.1 Global overview

HR team changes EmployeeType in HR system.

Success criteria:
Change is applied on MIM 2016 portal and Active Directory.
If EmployeeType is equal to *External*, *DisplayName* is updated based on this rule:
Last name + space + first name + -external
Else
Last name + space + first name
The user is added to the group *External-Users* and is removed from the group *Internal-Users*.

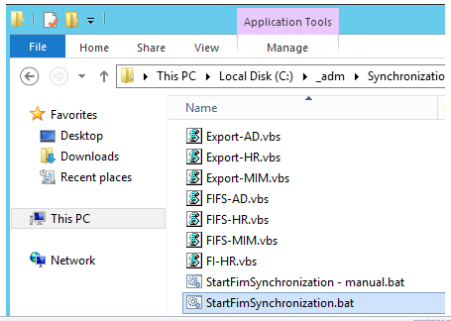
4.6.2 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.
Start SQL Server Management Studio.
Click on *Connect*.

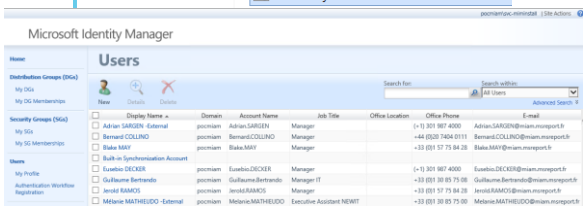


Edit the Users SQL Server table.

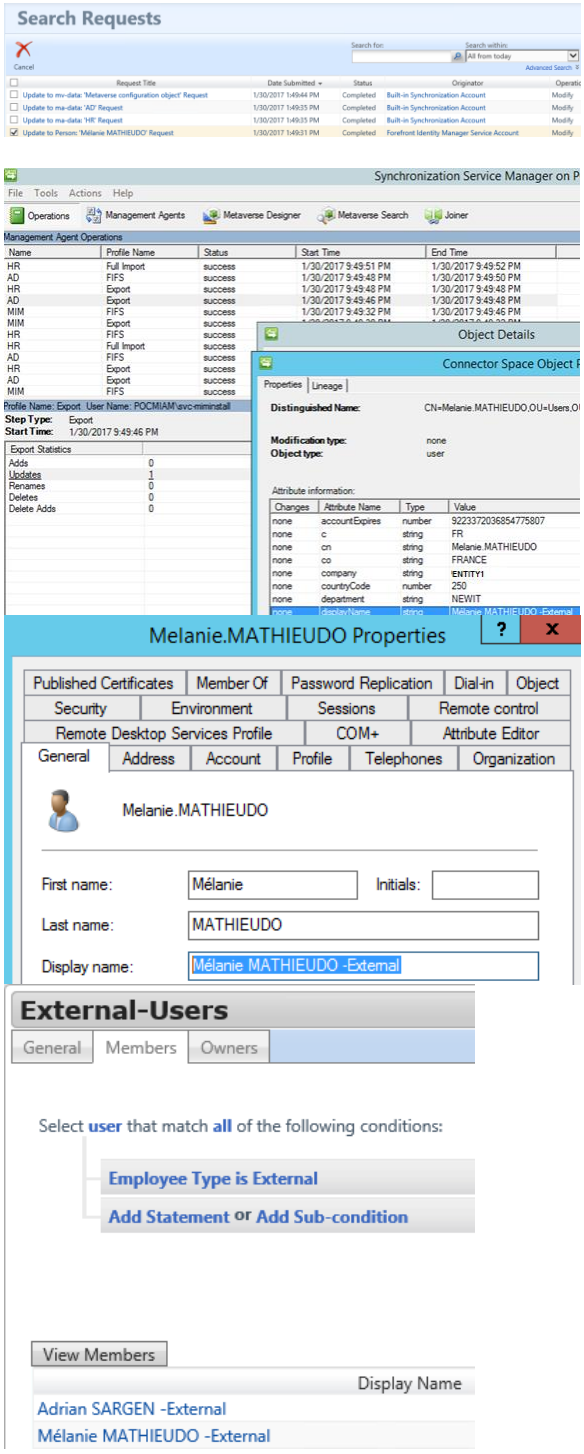
Change the Employee Type from *Internal* to *External* in the *Users* SQL Server table for a user (in this example *S000000002E000000014*).



Start all synchronization steps:
C:_adm\Synchronization\StartFimSynchronization.bat
Wait 30 seconds and start again all synchronization steps.



This start a MIM 2016 workflow which generate a new value for DisplayName based on *Employee Type*, *First Name* and *Last Name*.



The *DisplayName* attribute is updated to Active Directory.

The User is added automatically to the group *External-Users* and is removed from the group *Internal-Users*.

4.7 MANAGER ATTRIBUTE

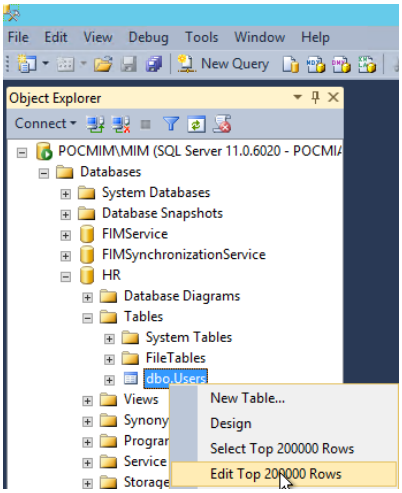
4.7.1 Global overview

Test 1: change the manager from HR database with a valid value.
Test 2: change the manager from HR database with an invalid value.
Test 3: change the manager (with a FIM administrator) from the MIM portal.
Test 4: change the manager (with AD administrator) from the Active Directory.

Success criteria:
Test 1: change is applied on MIM 2016 portal and Active Directory.
Test 2: no change is done. The previous value is keep.
Test 3: the change performed from the MIM 2016 is replaced by the value defined in HR database.
Test 4: the change performed from the Active Directory is replaced by the value defined in HR database.

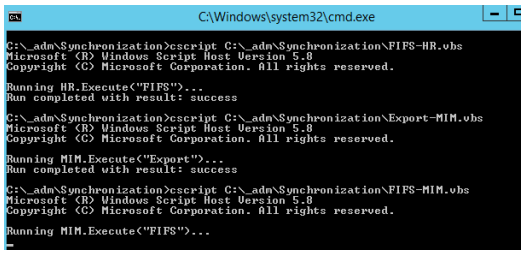
4.7.2 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.
Start SQL Server Management Studio.
Click on *Connect*.

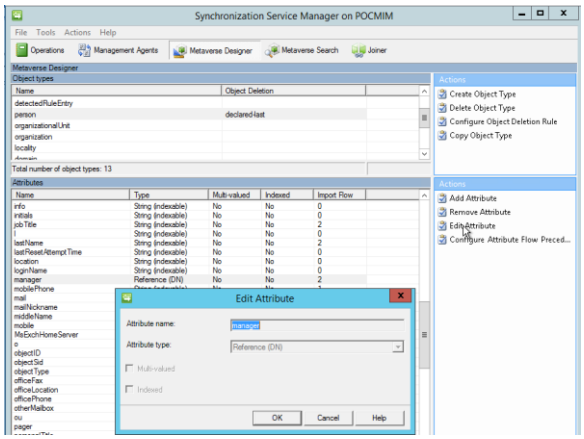


Edit the Users SQL Server table.

The Manager is a reference to another user based on the value of the *Employee_ID* attribute. Change the value of the column / attribute *MANAGER.* Click on the line below and save the changes.



Start all synchronization steps:
C:_adm\Synchronization\StartFimSynchronization.bat



Start the MIM Synchronization console.
Go to the tab *Metaverse Designer*.

Select the class *Person* then the attribute *Manager*.
Click on the link Edit attribute.

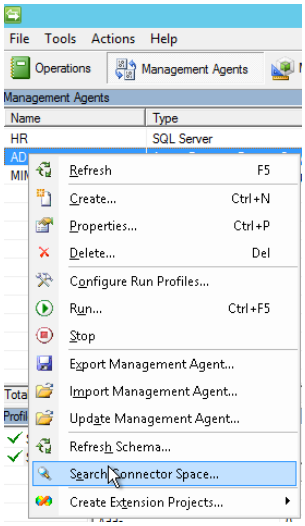
Manager is a *Reference (DN)* attribute.

A new manager is assigned on MIM 2016 portal and in Active Directory to the test user (*S000000002E000000014*).

The manager attribute changes. The FIM Synchronization Services display *none* on the Changes column because the tool compares the value between the AD connector space and the Metaverse.

We have performed a *Full synchronization*. That's why the console displays a change but not the value which has changed.

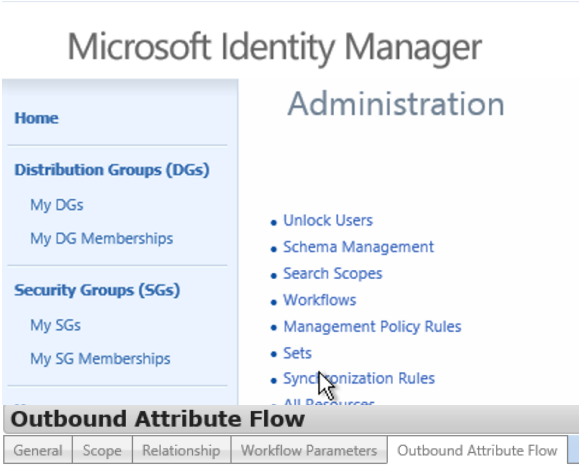
Change the manager of another user in the HR database. Perform manually the following synchronization sequence:
HR Full Import: review change of the HR connector space.
HR Full Synchronization. Check the value in the Metaverse.
MIM Export: check that the change has been done in the MIM portal.
MIM Full Import: check that the change has been applied in the MIM Connector space.
AD Export: check that the change has been applied in Active Directory.
HR Export: no change
AD Full Import: check that the change has been applied in the AD Connector space.
MIM Full Synchronization
AD Full Synchronization
HR Full import



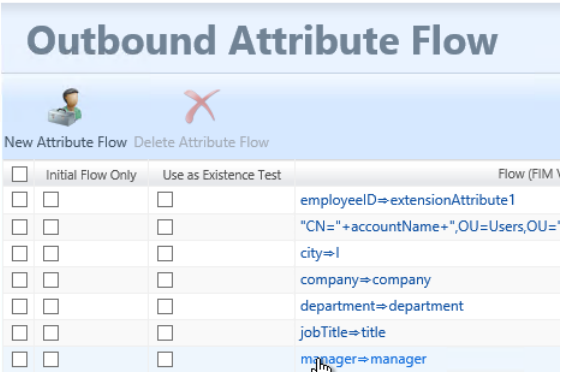
To retrieve the Connector space data, go to the tab *Management Agent* then right click on the Management Agent.
Click on *Search Connector Space*.
A new window appears.
Click on *Search.* You could display the pending actions like *Export*, *Import*.
You can only display *Connector* (object synchronized Metaverse / others Management Agent) or *Disconnector* (object synchronized with Metaverse / others Management Agent).
Try to change the value of a Manager with an incorrect value (bad Global_ID value).

The HR-IN synchronization rule (import data from HR database to the Metaverse) has not changed the previous value in the Metaverse because the *Manager* attribute is a reference attribute and the *Employee_ID* entered in the Manager field is not defined on any object.

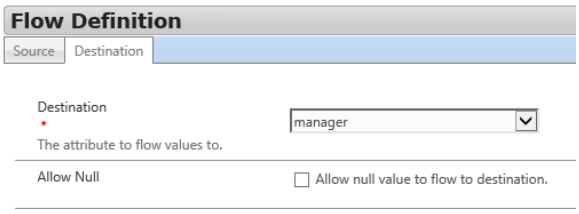
The current Manager value in Active Directory is not changed because no change has been performed in the Metaverse.



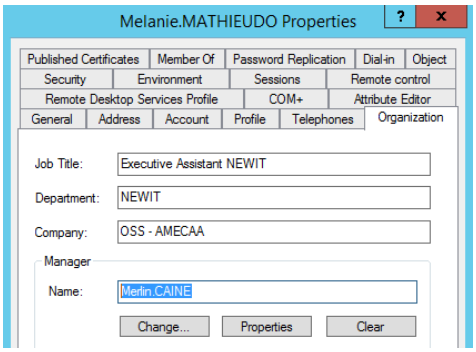
Go to MIM web portal.
Go to *Administration | Synchronization rule*.

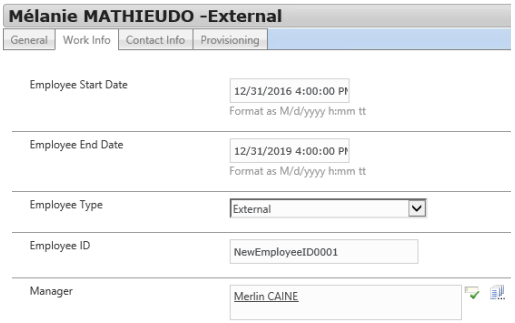


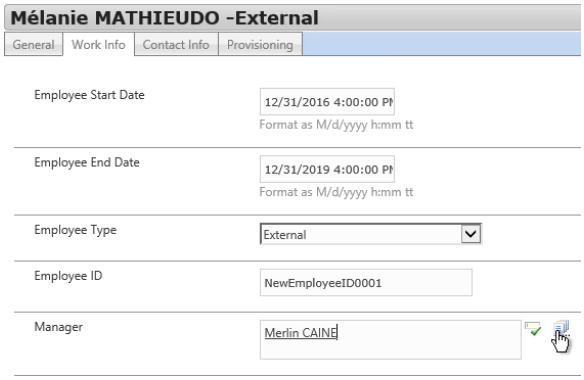
If you edit the *AD-OUT* synchronization rule, you could see that the synchronization engine is configured for the attribute *Manager* to not replace an existing value by an empty value.



Enter the previous value (*S000000002E000000001*) in the Manager field and start again the synchronization script.

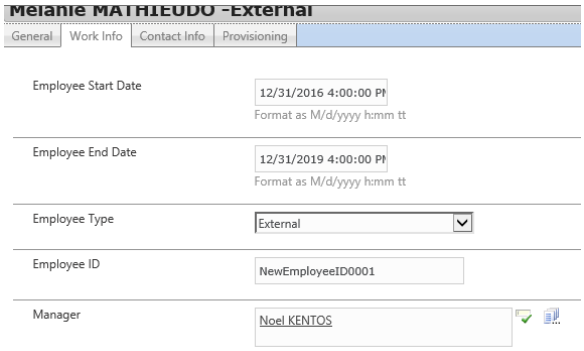




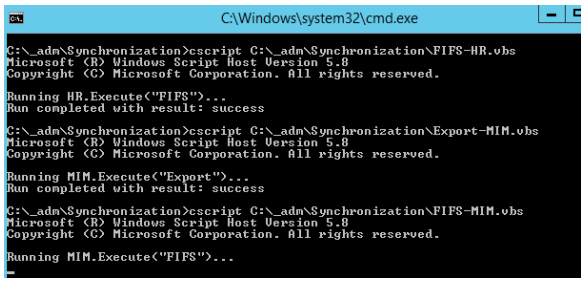


Change the value from the MIM portal. You must use a MIM 2016 administrator account like *pocmiam\svc-miminstall*.

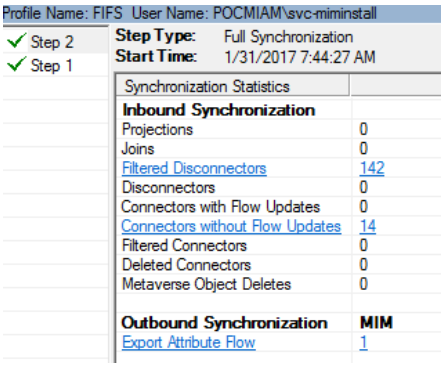
Change the Manager value.



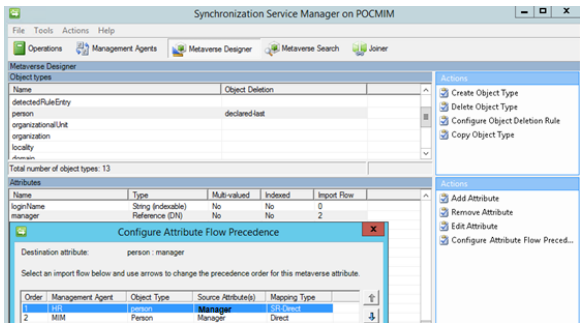
Define another user and then click on submit.



Start twice the synchronization script: *C:_adm\Synchronization\StartFimSynchronization.bat*



The value defined on the MIM portal is replaced by the value in the HR database.



Start the FIM Synchronization console.
Go to the tab *Metaverse Designer*.

Select the class *Person* then the attribute *Manager*.
Click on the link *Configure Attribute Flow precedence* attribute.

The change has been removed because we have defined that the *HR* Management Agent is authoritative for the attribute Manager.

Change the Manager attribute from Active Directory and check that you obtain the same result.

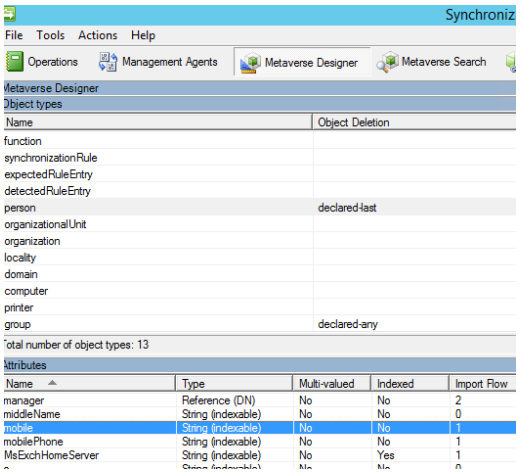
4.8 MOBILE, TELEPHONENUMBER EMPLOYEETYPE (BIDIRECTIONAL SYNCHRONIZATION)

4.8.1 Global overview

Test 1: HR team changes Mobile, TelephoneNumber and EmployeeType attributes in HR database.
Test 2: manager changes Mobile, Office Phone and EmployeeType fields in MIM 2016 portal.
Test 3: AD administrator changes *Mobile*, *TelephoneNumbe*r and *EmployeeType* attributes in Active Directory

Success criteria:
Test 1: the change is applied in all systems (HR, MIM 2016 portal, Active Directory).
Test 2: the change is applied in all systems (HR, MIM 2016 portal, Active Directory).
Test 3: the change is replaced by the value in HR system.

4.8.2 Step by step



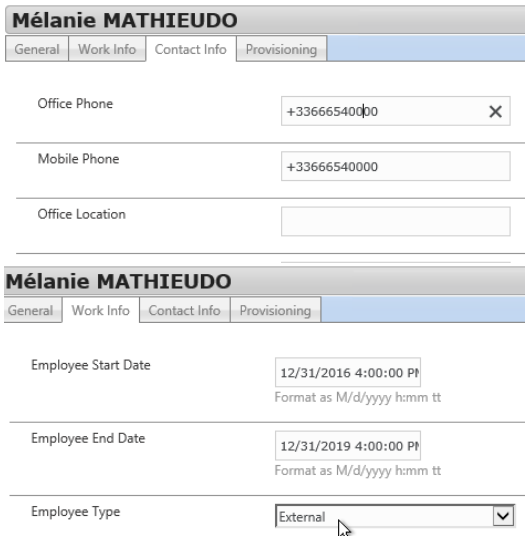
Start MIM Synchronization console.
Go to the tab *Metaverse Designer*.

Select the class *Person* then the attribute *Mobile, MobilePhone, EmployeeType, EmployeeTypeFIM, TelephoneNumber* and *OfficePhone*.

Click on the link *Configure Attribute Flow precedence*.

The Import Flow is set to 1 because only one management agent update values of the Metaverse.

Edit the Users SQL Server table.
Change the Mobile and TelephoneNumber and EmployeeType attributes of a test user from HR database.
Start the synchronization script twice.
The change is applied on all systems. *DisplayName* is updated based on EmployeeType value.



Change the Mobile and TelephoneNumber and EmployeeType attributes of a test user from MIM 2016 portal.
Start the synchronization script twice (sometimes 3 times).
The change is applied on all systems. *DisplayName* is updated based on EmployeeType value.
All the attributes are updated in the HR system.

If you change the value from Active Directory, the change is replaced by the value of MIM portal / HR database.

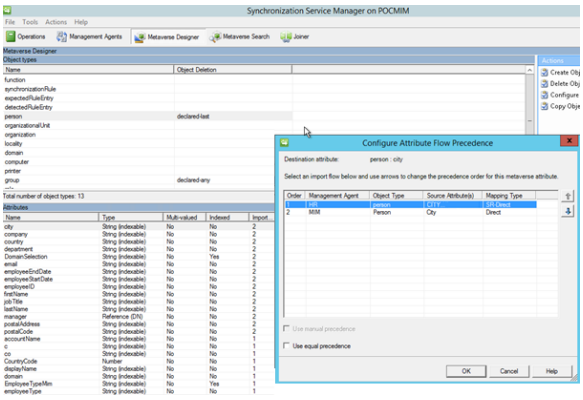
4.9 ADDRESS FIELDS

4.9.1 Global overview

Test 1: HR teams change address fields in HR databases (*STATE*, *ZIP_CD*, *CITY* and *C*)
Test 2: MIM administrators change address fields via MIM portal databases (*Postal code*, *Address*, *City* and *Country*).
Test 3: AD administrators change address fields in Active Directory portal databases (*PostalCode*, *StressAddress*, *l* and *C,Co, CountryCode* attributes).

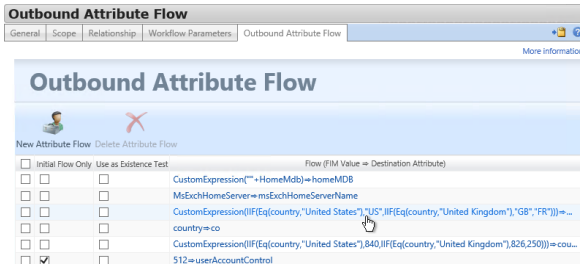
Success criteria:
Test 1: the change is applied in all systems (HR, MIM 2016 portal, Active Directory).
Test 2: the HR configuration replaces the value defined in MIM 2016 portal.
Test 3: the HR configuration replaces the value defined in Active Directory.

4.9.2 Step by Step

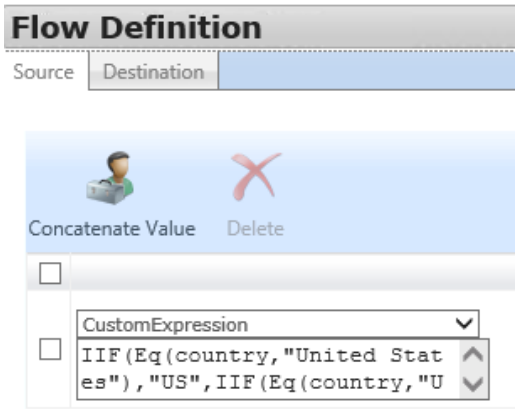


Start MIM Synchronization console.
Go to the tab *Metaverse Designer*.
Select the class *Person* then the attribute *City*.
Click on the link *Configure Attribute Flow precedence* attribute.
The Import Flow is set to 2 because this information is synchronized from MIM portal and from HR database. The order must be HR and then MIM to define that HR is the source of authority for the City attribute.
The same configuration must be defined for country, *postalAddress* and *postalCode*.
The attribute C, Co, CountryCode of the Metaverse are not used in this configuration.

Perform the 3 tests and validate the result. <u>Start synchronization twice for each test.</u>



Go to *Administration | Synchronization rules*.
Edit the synchronization rule *AD-OUT*.
Go to the tab *Outbound Attribute Flow* and edit the synchronization rule which are used to generate *C* and *Co* attribute based on the Metaverse Attributed *Country*.
Active Directory requires that 3 attributes are populated to define the country of an Active Directory user (address fields).



We use a Custom Expression to generate this.
To generate C attribute:
IIF(Eq(country,"United States"),"US",IIF(Eq(country,"United Kingdom"),"GB","FR"))

To generate CountryCode attribute:
IIF(Eq(country,"United States"),840,IIF(Eq(country,"United Kingdom"),826,250))

4.10 USER SELF SERVICE

4.10.1 Global overview

Test1: users can update his office phone or mobile phone (with or without *HR approval based* on Type) from the MIM portal. If Type is "*Cadre dirigeant*", an approval is required else no approval is required.
Test2: users can register his mobile and email from the web site http://aka.ms/ssprsetup.
Test 3: users can reset his password from the website http://aka.ms/ssprs by enter a passcode received on his mobile phone.

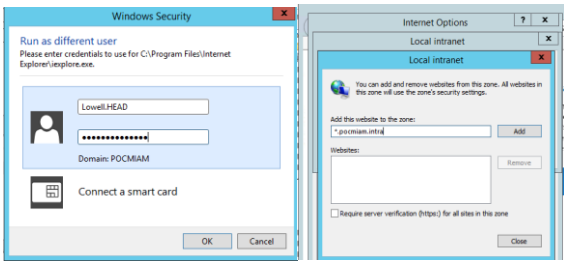
Success criteria
Test1: users can change his office phone or his mobile phone with or without approval based on Type.
Test2: users can register his mobile phone to reset his passcode.
Test3: users can reset his passcode with his mobile phone.

4.10.2 Step by step

Select 4 users in HR database:

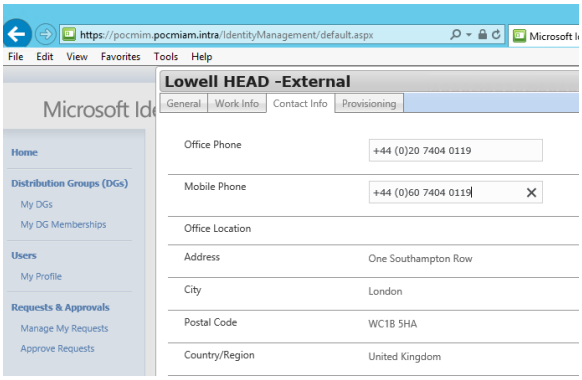
- One standard user (*Type* is equal to *Cadre*) and his manager.
- One standard user (*Type* is equal to *Cadre Dirigeant*) and his manager.

The Manager attributes in HR database is a reference to the *Global_ID* of a user (the manager).
Lowell HEAD has the Employee Id *S000000002E000000103*.
His manager is Bernard COLLINO has the Employee Id S000000002E000000005.
Type of Lowell HEAD is "*Agent de maitrise*".



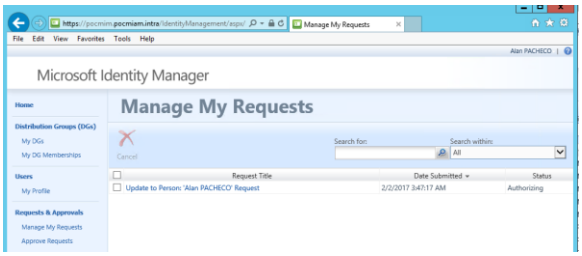
Start Internet Explorer in the context of the user account *Lowell.HEAD*.

Add **.pocmiam.intra* in Local Intranet (required).
Connect to https://pocmim.pocmiam.intra/IdentityManagement

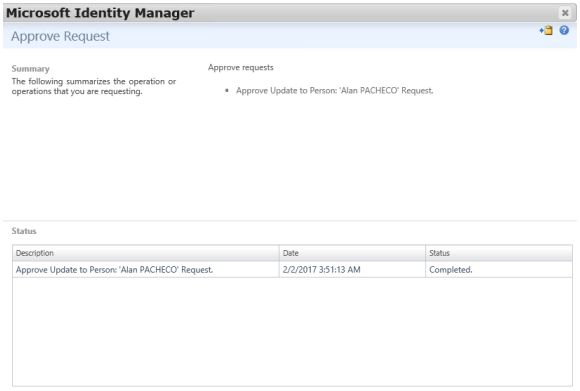


Edit the *Office Phone* and *Mobile Phone*.
Click on *Submit*.

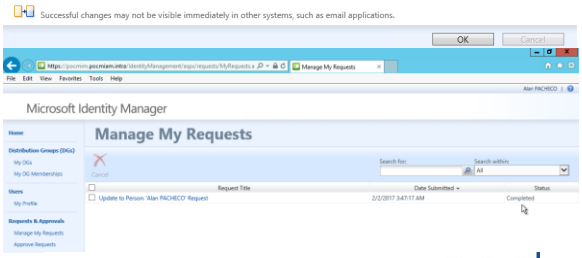
The change is applied without approval because the *Type* of the user is "*Cadre*".
Perform the same action with the user with a Type as *Cadre dirigeant*. An approval of the manager will be required.
Alan PACHECO (*Alan.PACHECO*, *S000000002E000000106*) has a Type with the value *Cadre dirigeant*.
His Manager is Jerold RAMOS (S000000002E000000006).
Change his Office Phone and Mobile Phone.



When you click on Submit, an approval is required.

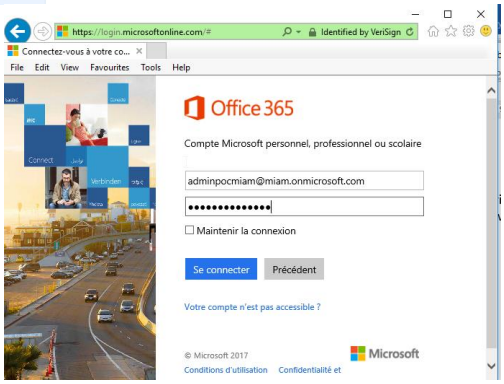


Log with the Manager user account on the MIM 2016 web portal and approve the request.

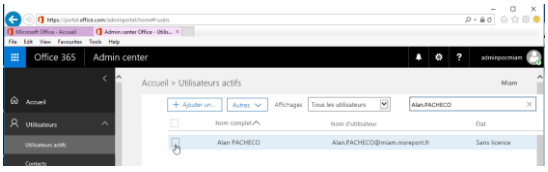


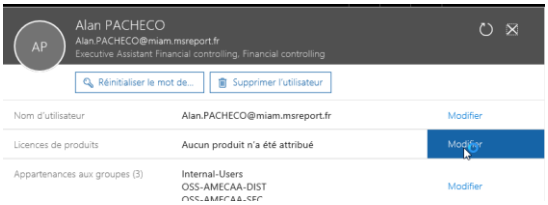
The change is applied on the MIM portal.

(End of test 1)

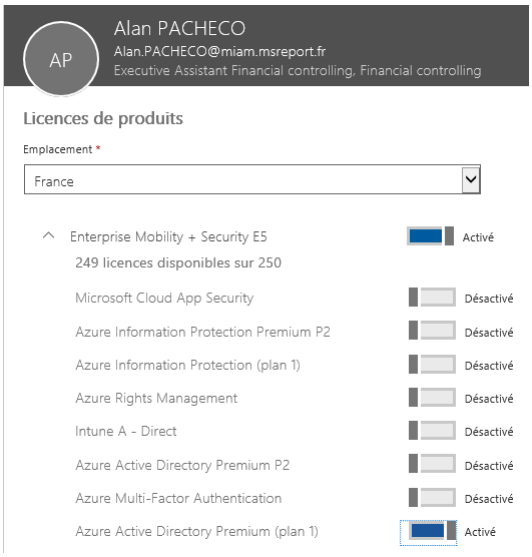


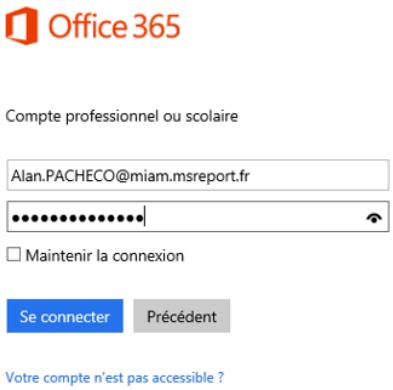
Connect to Office 365 portal (https://login.microsoftonline.com) with the user account adminpocmiam@miam.onmicrosoft.com.



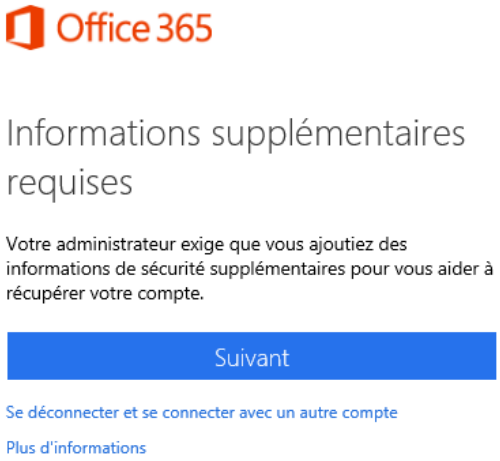


Assign Azure Active Premium P1 license from the Office 365 portal to an existing user (*Alan.PACHECO* in this example).



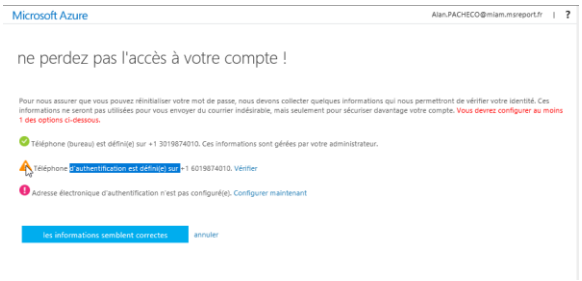


Connect to *Alan.PACHECO*



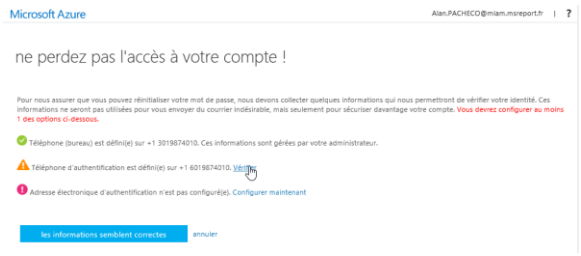
Each user must register the first time to SSPR website (https://account.activedirectory.windowsazure.com/passwordreset/register.aspx?client-request-id=27b726b9-d7f0-4551-bddc-f2b6eae10b4d&sspr=1)

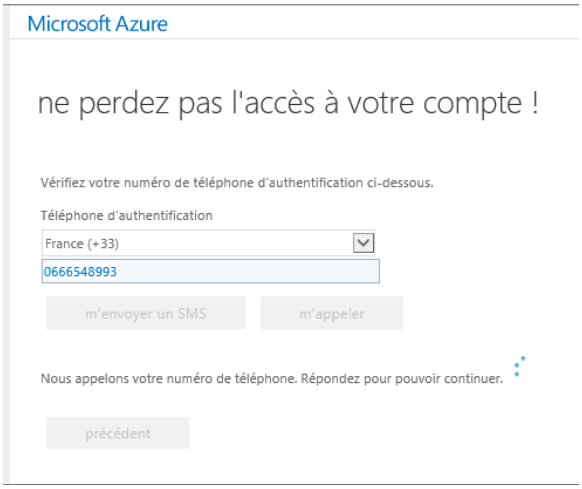
You could access to this site by using also this short link http://aka.ms/ssprsetup.



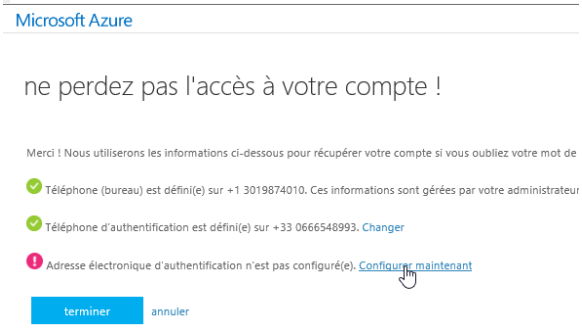
Office phone and Mobile phone are replicated by default by Azure Active Directory Connect.

Click on the link *Verify*. You can change the default mobile phone used.

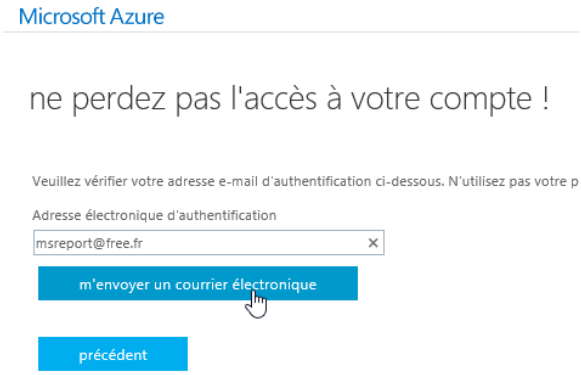


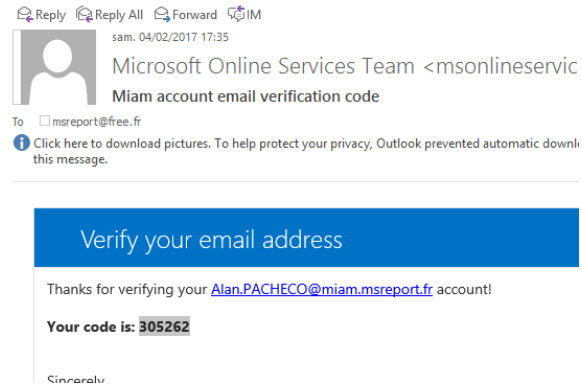


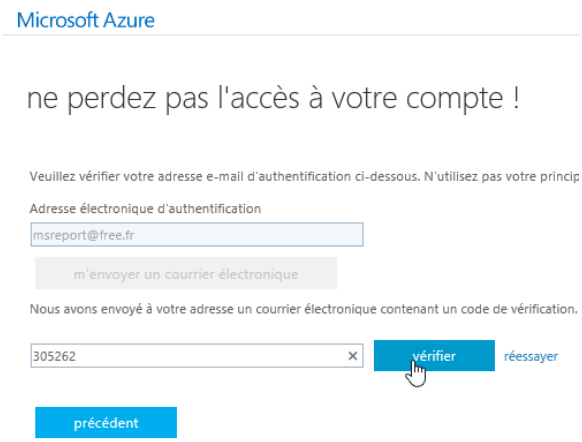
Click on *Call me*. Respond to the call and press on the key *#*.

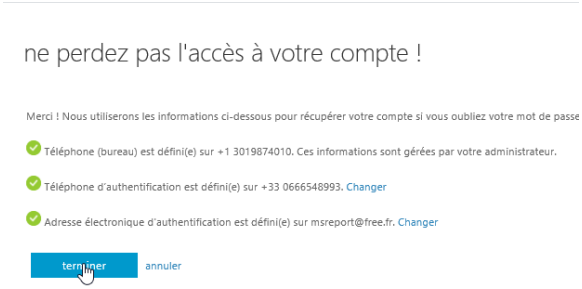


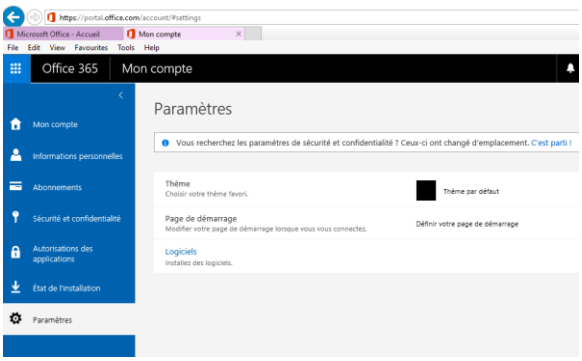
You could also enter a personal email address (avoid using your primary email address).





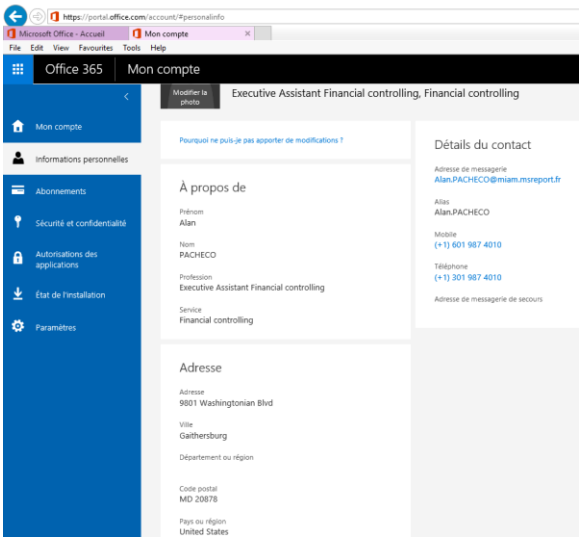


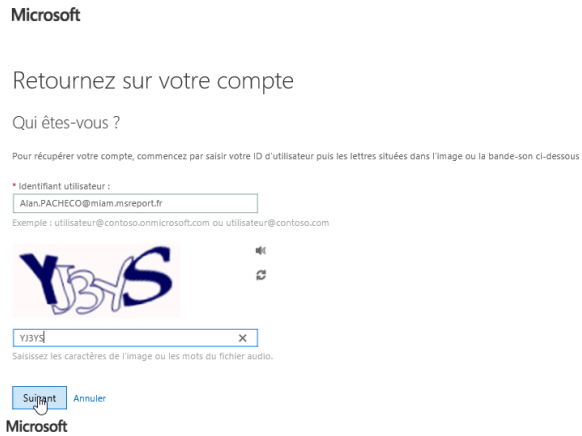




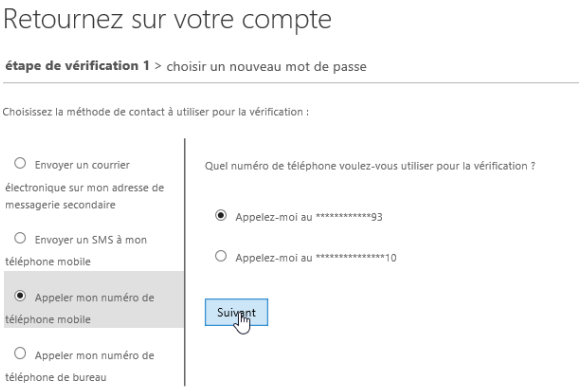
User can view his setting from Azure Active Directory portal, review is applications, download his software and manage his settings.
https://portal.office.com/account/#settings

(End of test 3)



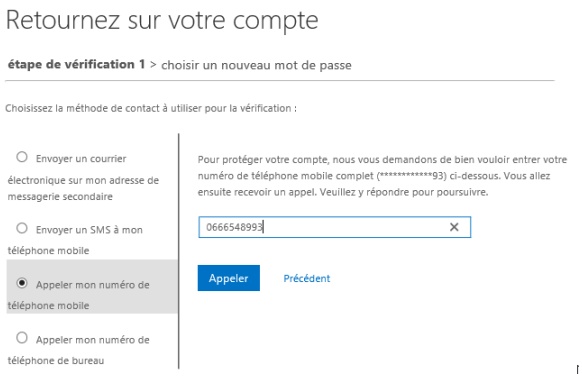


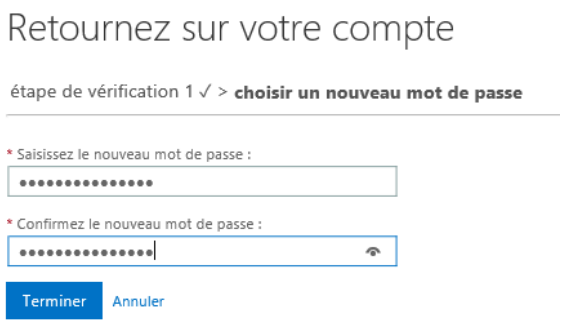
Go to the website http://aka.ms/sspr and reset the password of the user account Alan.PACHECO@miam.msreport.fr



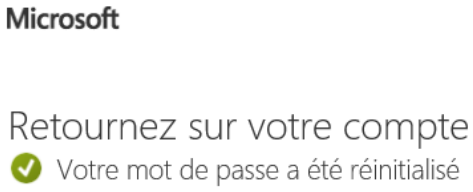
Select the proper phone number and enter it manually as requested.

Press the key # of the phone to verify the connection. You can now reset your password





Enter your new password.



Try connect to https://pocmim.pocmiam.intra/identitymanagement from the computer POCMIM to check that the Active Directory user account password has also changed.