

MIM 2016 DEPLOYMENT AND CONIGURATION GUIDE

1 ARCHITECTURE OVERVIEW	5
1.1 MIM 2016 / AZURE ACTIVE DIRECTORY COMPONENTS	5
1.2 MIM 2016 SERVERS	6
1.3 MIM 2016 LICENSING	7
1.4 SQL SERVER CONFIGURATION.....	8
1.5 SHAREPOINT ARCHITECTURE	8
1.6 MIM SYNCHRONIZATION SERVICE AND MIM SERVICE SCHEMA.....	9
1.7 MIM REPORT.....	9
1.8 SERVICE ACCOUNT	10
1.9 PASSWORD SELF-SERVICE FEATURES.....	10
1.10 MIM CERTIFICATE MANAGEMENT.....	10
1.11 BHOLD.....	10
1.12 LANGUAGE PACK	11
1.13 NETWORK FLOWS	11
2 INSTALLATION STEP BY STEP	12
2.1 DEPLOY THE ACTIVE DIRECTORY FOREST.....	12
2.2 CREATE A ROOT PUBLIC KEY AUTHORITY.....	13
2.3 CONFIGURE INTERNET EXPLORER BY GPO	14
2.4 INSTALL POCEXCH1	15
2.5 PREPARE THE ENVIRONMENT (DNS, SERVICE ACCOUNT AND PREPARE POCMIM)	18
2.6 INSTALL AND CONFIGURE AZURE ACTIVE DIRECTORY CONNECT ON POCDC1.....	23
2.7 CONFIGURE AZURE ACTIVE DIRECTORY PASSWORD SELF SERVICE FEATURES.....	28
2.8 INSTALL POCMIM	30
2.8.1 <i>Install SQL server on POCMIM.....</i>	30
2.8.2 <i>Install SharePoint 2013 Foundation on POCMIM.....</i>	32
2.8.3 <i>Deploy MIM Synchronization Service on POCMIM.....</i>	40
2.8.4 <i>Install MIM Service on POCMIM.....</i>	43
2.8.5 <i>Install Visual Studio 2015 on POCMIM</i>	48
2.8.6 <i>Install MIMWAL.....</i>	49
3 CONFIGURE MIM 2016 SOLUTION	52
3.1 MAIN USE CASES	52
3.1.1 <i>schema and synchronization rules</i>	52
3.1.2 <i>MIM 2016 Web interface customization.....</i>	55
3.1.3 <i>Other requirements</i>	55
3.2 CREATE HR DATABASE AND IMPORT YOUR HR DATA.....	55
3.3 CONFIGURE LOGO	59
3.4 CONFIGURE THE MIM SYNCHRONIZATION SERVICE SCHEMA AND THE MIM SERVICE SCHEMA	59
3.5 CREATE THE HR MANAGEMENT AGENT (SQL SERVER) IN MIM SYNCHRONIZATION SERVICE	62
3.6 CREATE THE ACTIVE DIRECTORY MANAGEMENT AGENT	64
3.7 CONFIGURATION DU MANAGEMENT AGENT FIM SERVICE	68
3.8 CONFIGURE THE RUN PROFILES FOR EACH MANAGEMENT AGENT	71
3.9 CREATE SYNCHRONIZATION RULES.....	73
3.9.1 <i>Create HR-IN synchronization rules</i>	73
3.9.2 <i>Create HR-OUT synchronization rule</i>	75
3.9.3 <i>Create the synchronization rule AD-USER-OUT</i>	76
3.9.4 <i>Create the synchronization rules AD-USERS-IN</i>	78
3.9.5 <i>Create the synchronization rules AD-DISABLE-USERS</i>	80
3.9.6 <i>Create the synchronization rule for distribution group</i>	81
3.9.7 <i>Create the synchronization rule for security group</i>	84
3.10 CONFIGURE ALL SETS.....	86
3.11 CONFIGURE ALL MIM WORKFLOWS	89
3.11.1 <i>Create workflow AD-USERS-OUT</i>	89
3.11.2 <i>Create the workflow HR-OUT</i>	90
3.11.3 <i>Create the workflow AD-DISABLE-USERS</i>	91

3.11.4	<i>Create and configure the Workflow _AD-REMOVE-USERS</i>	92
3.11.5	<i>Generate attributes from MIM portal.....</i>	94
3.11.6	<i>Create the workflow Manager_Approval_Classic.....</i>	96
3.11.7	<i>Create the workflow Notify Manager.....</i>	96
3.11.8	<i>Create the workflow _Distribution Group Provisioning to AD and _Security Group Provisioning to AD</i>	96
3.11.9	<i>Workflows Result</i>	97
3.12	MANAGEMENT POLICY RULES	98
3.12.1	<i>Configure Synchronization: Synchronization account controls users it synchronizes Management Policy rule</i> 98	
3.12.2	<i>Enable the rules to synchronize groups.....</i>	98
3.12.3	<i>Allow user to connect to the MIM 2016 portal</i>	98
3.12.4	<i>Create the management policy rule _AD-USERS-OUT</i>	100
3.12.5	<i>Create the management policy rule _HR-OUT.....</i>	101
3.12.6	<i>Create the management policy rule AD-DISABLE-USERS</i>	102
3.12.7	<i>Create the management Policy rule AD-REMOVE-USERS</i>	103
3.12.8	<i>Create the management rule policy _Distribution Group Creation and Provisioning to AD</i>	104
3.12.9	<i>Create the management rule policy _Security Group Creation and Provisioning to AD</i>	104
3.12.10	<i>Create the management policy rule which start the workflow _Generates values</i>	104
3.12.11	<i>Start the workflow which send an email to manager (Type not equal to Cadre dirigeant).....</i>	105
3.12.12	<i>Start the workflow which requires approval of manager (Type equal to Cadre dirigeant)</i>	107
3.12.13	<i>Allow a manager to read attributes of his reports.....</i>	108
3.12.14	<i>Allow a manager to change EmployeeType, Mobile Phone, Office Phone and Photo of his reports</i>	109
3.12.15	<i>Allow a user to read attributes of his own user account.....</i>	110
3.12.16	<i>Allow user to modify attributes of his own user account.....</i>	111
3.12.17	<i>Allow users to read attributes of other users.....</i>	112
3.12.18	<i>Allow a manager to create his reports.....</i>	113
3.13	CONFIGURE PROVISIONNING	114
3.14	CONFIGURE DEPROVISIONNING FOR USER	114
3.15	CONFIGURE RULES PRECEDENCE FOR USER CLASS (METAVERSE SCHEMA)	116
3.16	CONFIGURE RULES PRECEDENCE FOR GROUP CLASS (METAVERSE SCHEMA)	118
3.17	CONFIGURE RESOURCE CONTROL DISPLAY CONFIGURATION	119
3.18	BACKUP THE POC ENVIRONMENT	122
3.19	DATABASE SIZE.....	123
3.20	MIM PORTAL CUSTOMIZATION	124
3.20.1	<i>MIM Portal components</i>	124
3.20.2	<i>Navigation bar configuration.....</i>	125
3.20.3	<i>Home Page configuration</i>	127
3.20.4	<i>CSS customization</i>	128
4	USE CASES (STEP BY STEP).....	129
4.1	PROVISION NEW USERS	129
4.1.1	<i>Global overview</i>	129
4.1.2	<i>Step by step</i>	130
4.2	DEPROVISION	138
4.2.1	<i>Global overview</i>	138
4.2.2	<i>Step by step</i>	138
4.3	CHANGE USER FIRST NAME AND/OR LAST NAME.....	142
4.3.1	<i>Global overview</i>	142
4.3.2	<i>Step by step</i>	142
4.4	CHANGE HR INFORMATION	144
4.4.1	<i>Step by step</i>	144
4.5	EMPLOYEE TYPE CHANGED BY HR TEAM	146
4.5.1	<i>Global overview</i>	146
4.5.2	<i>Step by step</i>	146
4.6	MANAGER ATTRIBUTE.....	148

4.6.1	<i>Global overview</i>	148
4.6.2	<i>Step by step</i>	148
4.7	MOBILE, TELEPHONE NUMBER EMPLOYEE TYPE (BIDIRECTIONAL SYNCHRONIZATION).....	152
4.7.1	<i>Global overview</i>	152
4.7.2	<i>Step by step</i>	152
4.8	ADDRESS FIELDS	153
4.8.1	<i>Global overview</i>	153
4.8.2	<i>Step by Step</i>	153
4.9	USER SELF SERVICE	154
4.9.1	<i>Global overview</i>	154
4.9.2	<i>Step by step</i>	154

1 ARCHITECTURE OVERVIEW

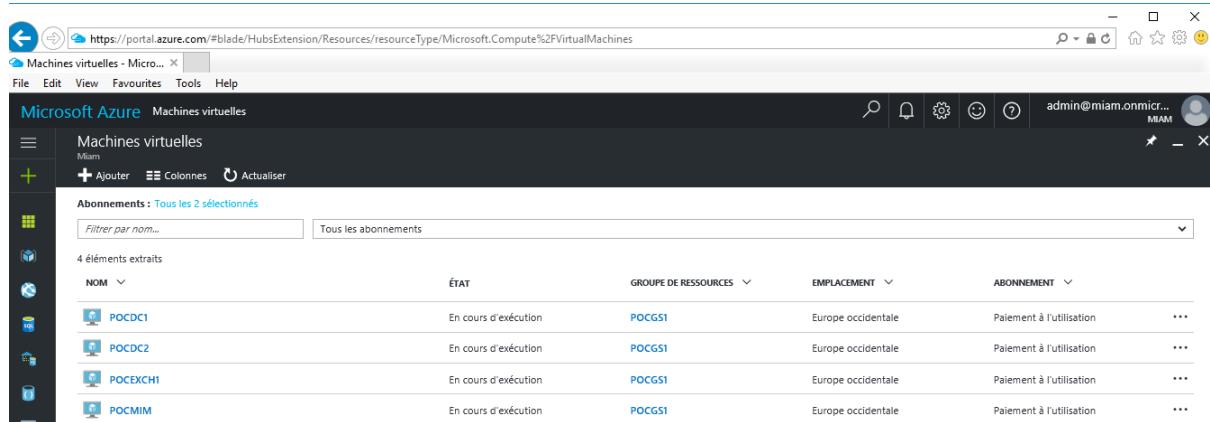
1.1 MIM 2016 / AZURE ACTIVE DIRECTORY COMPONENTS

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: <ul style="list-style-type: none">➤ 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 <i>Pass the hash</i> 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 <i>Azure Active Directory Premium</i> 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.



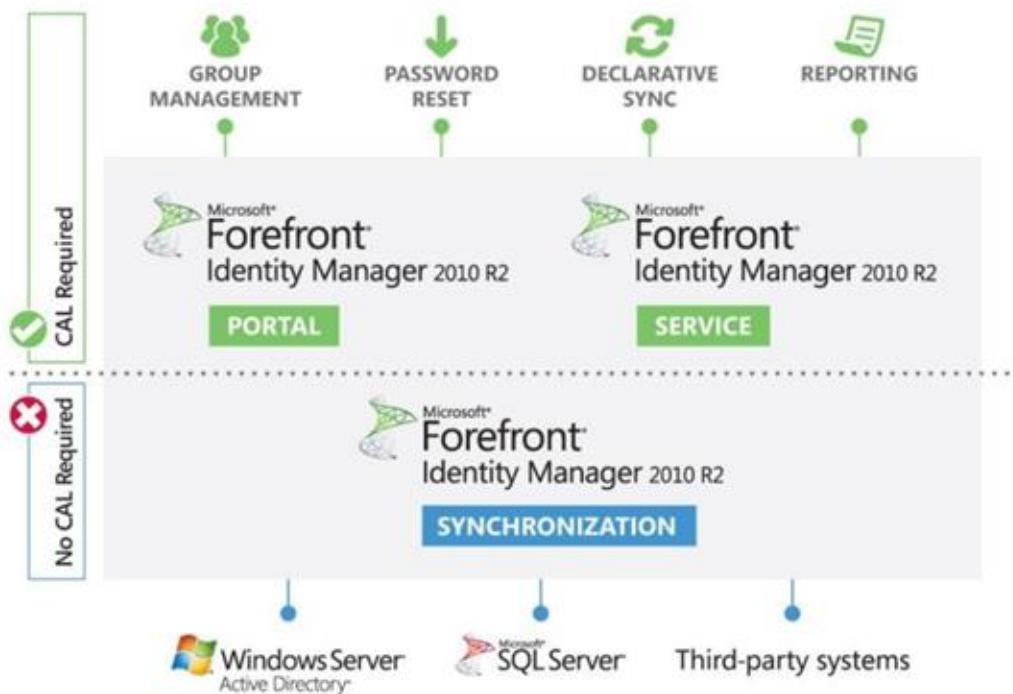
The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The top navigation bar includes links for Machines virtuelles - Micro... (with a count of 2), File, Edit, View, Favorites, Tools, Help, and a user account (admin@miam.onmicrosoft.com). The main content area is titled "Microsoft Azure Machines virtuelles" and shows a list of four virtual machines:

NOM	ÉTAT	GROUPES DE RESSOURCES	EMPLACEMENT	ABONNEMENT
POCDC1	En cours d'exécution	POCGS1	Europe occidentale	Paiement à l'utilisation
POCDC2	En cours d'exécution	POCGS1	Europe occidentale	Paiement à l'utilisation
POCEXCH1	En cours d'exécution	POCGS1	Europe occidentale	Paiement à l'utilisation
POCMIM	En cours d'exécution	POCGS1	Europe occidentale	Paiement à l'utilisation

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 (<i>POCMIAM.INTRA</i>) and Azure Active Directory Connect server. Remote access: RDP (<i>pocdc1.westeurope.cloudapp.azure.com</i>) 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 (<i>CHILD.POCMIAM.INTRA</i>) Remote access: RDP (<i>pocdc2.westeurope.cloudapp.azure.com</i>) 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 (<i>pocech1.westeurope.cloudapp.azure.com</i>) 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 (<i>pocmim.westeurope.cloudapp.azure.com</i>) Backup: every day at 3 AM.

1.3 MIM 2016 LICENSING



Microsoft has completely changed 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. (incl. smart card & digital certs)
- a CAL is required for an 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](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](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

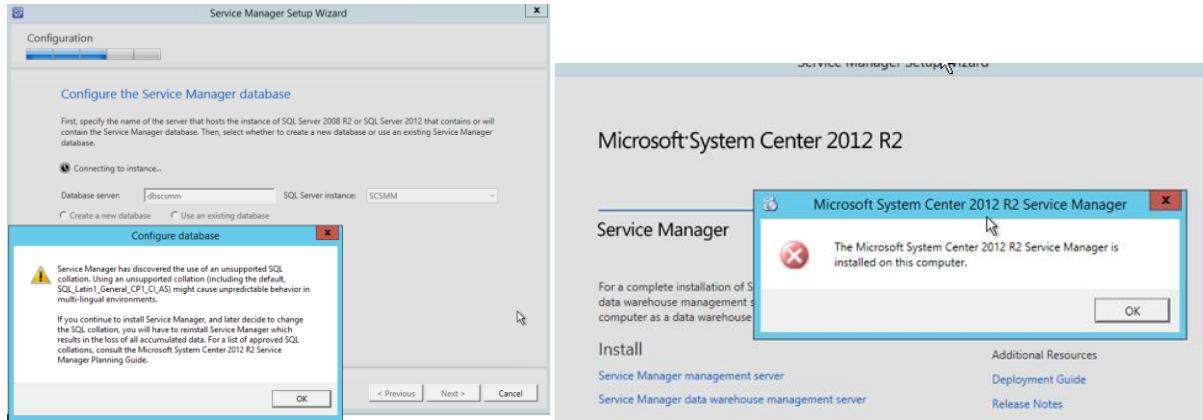
The schema of MIM Services and MIM Synchronization Services will be updated to add attributes like *Global_ID*, *Domain*, *HomeMdb*, *MsExchHomeServer* to the class *Person*.

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-mimsp	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

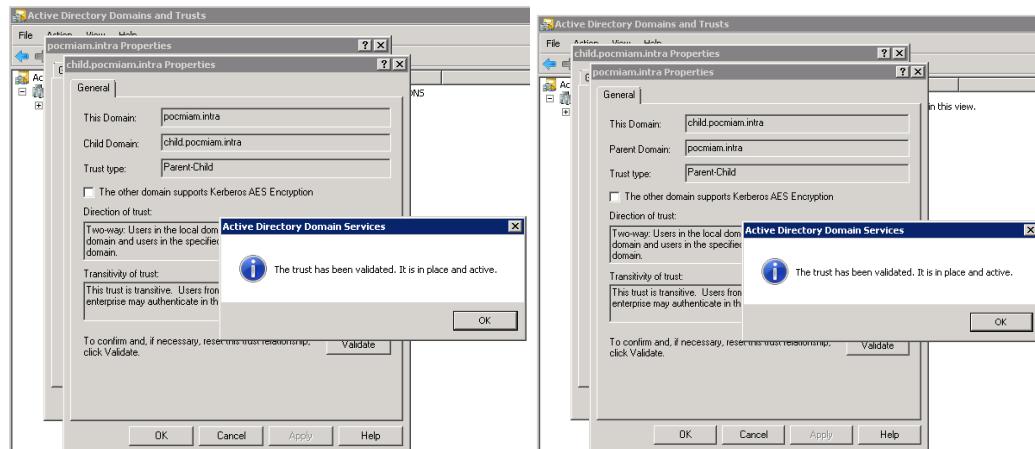
2.1 DEPLOY THE ACTIVE DIRECTORY FOREST

Apply this guide to create domain controller in Azure IaaS.

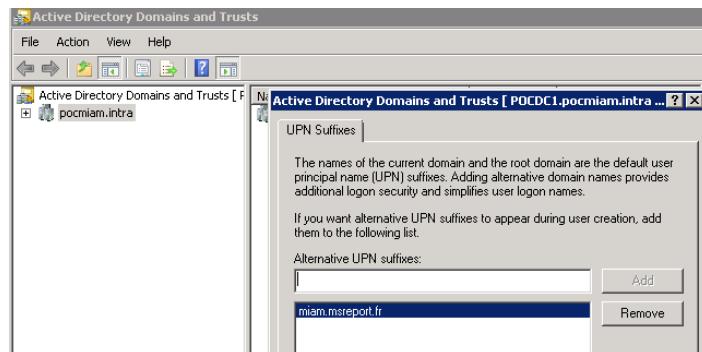
<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-new-forest-virtual-machine>

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:XXXXXX /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.

The screenshot shows the 'Add Roles Wizard' interface for creating a Root Public Key Authority (PKI). It consists of five sequential steps:

- Select Role Services:** Shows options for 'Role Services' including 'Certification Authority' and 'Certification Authority Web Enrollment'.
- Specify Setup Type:** Shows options for 'Setup Type' including 'Enterprise' (selected) and 'Standalone'.
- Specify CA Type:** Shows options for 'CA Type' including 'Root CA' (selected) and 'Subordinate CA'.
- Configure Cryptography for CA:** Shows settings for 'Cryptographic service provider (CSP)' set to 'RSA\Microsoft Software Key Storage Provider' and 'Key character length' set to '2048'. It also lists hash algorithms: SHA256, SHA384, SHA512, and SHA1.
- Set Validity Period:** Shows a note about certificate validity and a dropdown for 'Select validity period for the certificate generated for this CA' set to '10 Years'.

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

Select *Enterprise*.

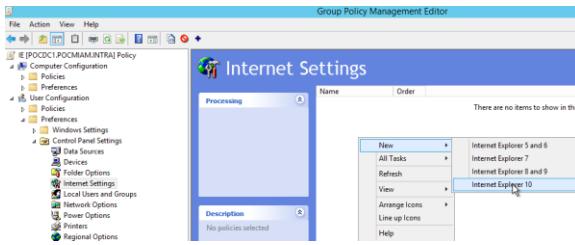
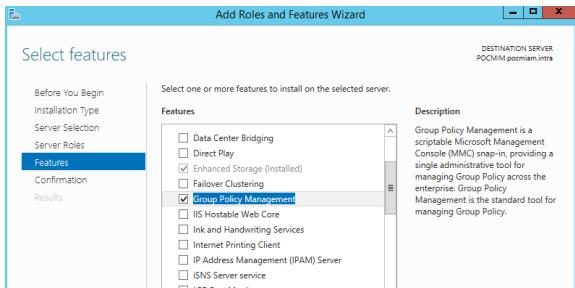
Select *Root CA*.

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

Enter *Pocmiam*.

Perform a default installation and click on *Finish*.

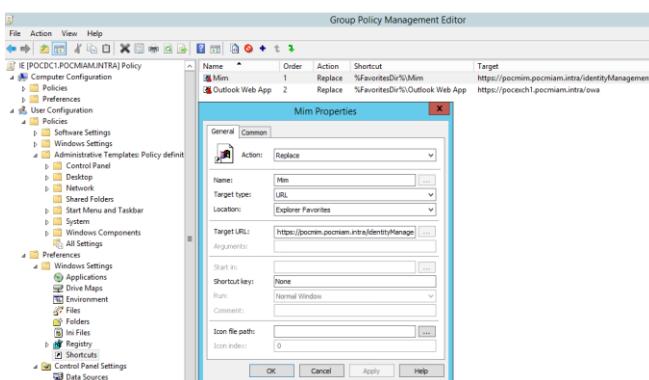
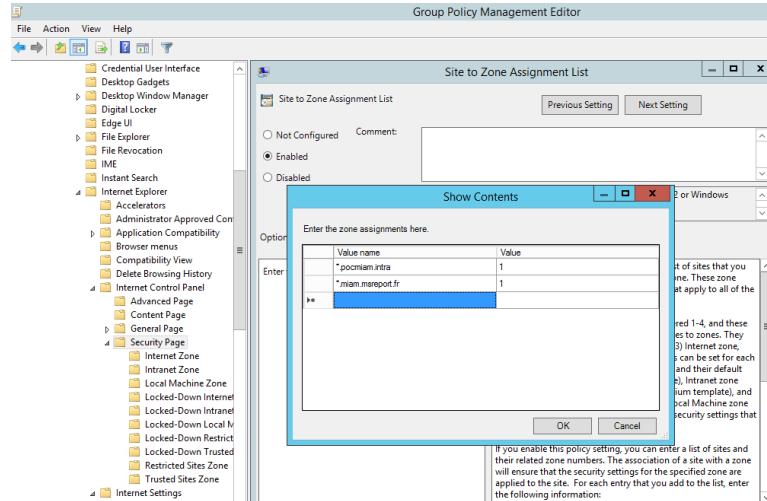
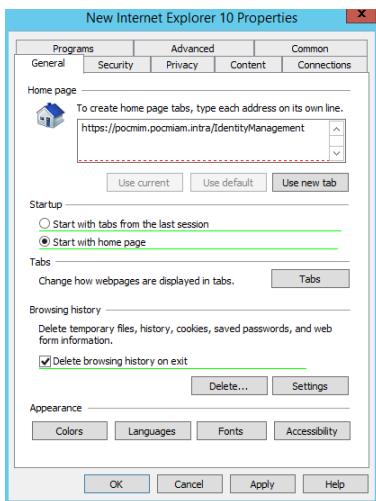
2.3 CONFIGURE INTERNET EXPLORER BY GPO



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`

The screenshot shows two windows from the Microsoft Azure portal:

- POCEXCH1-ip - Configuration**: Shows the VM details. Under "Affectation", "Statique" is selected, and the "Adresse IP" is set to 52.174.199.24. The "Étiquette de nom DNS (facultatif)" field contains "pocexch1".
- ipconfig1 - ipconfig1**: Shows the network interface configuration. Under "Paramètres d'adresse IP publique", "Adresse IP publique" is set to "POCEXCH1-ip (52.174.199.24)". Under "Paramètres d'adresse IP privée", "Adresse IP" is set to "10.0.0.7".

Prepare the server to deploy Exchange 2013

[https://technet.microsoft.com/en-us/library/bb691354\(v=exchg.150\).aspx](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

```
Administrator: Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\gmathieu> 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

Success Restart Needed Exit Code Feature Result
----- ----- -----
True Yes SuccessRest... [Application Server, HTTP Activation, .NET...
WARNING: You must restart this server to finish the installation process.

PS C:\Users\gmathieu>
```

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](https://technet.microsoft.com/en-us/library/bb691354(v=exchg.150).aspx)

NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	B...
BRS - Americas Area	POCEXCH1	POCEXCH1	Mounted	0
Mailbox Database ...	POCEXCH1	POCEXCH1	Mounted	0
DS - AMECAA	POCEXCH1	POCEXCH1	Mounted	0
DS - China	POCEXCH1	POCEXCH1	Mounted	0
DS - Continental ...	POCEXCH1	POCEXCH1	Mounted	0
DS - France	POCEXCH1	POCEXCH1	Mounted	0
DS - North Ameri...	POCEXCH1	POCEXCH1	Mounted	0
DS - South Ameri...	POCEXCH1	POCEXCH1	Mounted	0
PHS - International	POCEXCH1	POCEXCH1	Mounted	0

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

Install the Exchange 2013 Enterprise license.

Generate Exchange 2013 certificate.

*Friendly name for this certificate:

pocexch1.pocmiam.intra

Click on **Next**.

Click on **Next**.

Exchange Certificate - Internet Explorer

Use a local shared folder to store the request.

Microsoft Active Directory Certificate Services – Pocmiam

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #11 Web server) in the Saved Request box.

Saved Request:

```
81kPZ/6r3j1iX3htpx/HUyJidJgMuQ0fpwF498NV
YD1ND5kPoCx25OS6ronacNkw3euDakuzGLkeo^
YUDG+sVXBm62nTxSjgPNFIghhVIQ5nfWRas03MS
Oap0lnPA+E2oLsg05Hz0w271rhFzz1Mit73DJ5wn
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server	<input checked="" type="checkbox"/>
------------	-------------------------------------

Additional Attributes:

Attributes:	^
-------------	---

Click on *Submit* button.

Enterprise Office 365

Exchange admin center

recipients servers databases database availability groups virtual directories certificates

permissions compliance management organization protection mail flow mobile public folders unified messaging

servers

hybrid tools

Select server: **POC0011.pocmim.intra**

+ ⌂ ⌂ ⌂ ⌂

NAME	STATUS	EXPIRE ON
TenantSyncMasterCert	Valid	1/22/2018
poocmim.pocmim.intra	Finding request	1/22/2018
Microsoft Exchange Server Auth Certificate	Valid	12/27/2001
Microsoft Exchange	Valid	1/22/2022
WMSVC	Valid	1/26/2027

poocmim.pocmim.intra

Certification authority-signed certificate
Issuer: C=PR, S=DF, L=Paris, O=MAMM-DU-IT,
OU=process/pocmimcerts

Status

Complete **Test** 1/22/2018

Cancel

Assigned to services

NONE

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

complete pending request

This will import the certificate file that you received from the certification authority. After it's imported, you can assign this certificate to various Exchange services. [Learn more](#)

*File to import from (example: \\server\folder\MyCertificate.CER):
\\pocexch1.pocmiam.intra\c\$\adm\Exchange.cer

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

DNS Manager				
File Action View Help				
DNS	Name	Type	Data	Timestamp
POCDC1	_msdcsv			
	_sites			
	_tcp			
	_msdcsv.pocmiam.intra			
	child.pocmiam.intra			
	pocmiam.intra			
Forward Lookup Zones	(same as parent folder)	Start of Authority (SOA)	[34], pocdc1.pocmiam.intra....	static
	(same as parent folder)	Name Server (NS)	pocdc2.child.pocmiam.intra.	static
	(same as parent folder)	Name Server (NS)	pocdc1.pocmiam.intra.	static
	(same as parent folder)	Host (A)	10.0.0.5	1/22/2017 1:00:00 AM
	pocdc1	Host (A)	10.0.0.5	static
	POCEXCH1	Host (A)	10.0.0.7	1/22/2017 10:00:00 AM
	POCMIM	Host (A)	10.0.0.4	1/22/2017 11:00:00 AM
	mimportal	Host (A)	10.0.0.4	
	mimservice	Host (A)	10.0.0.4	
	register	Host (A)	10.0.0.4	

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-mimspool -name svc-mimspool
Set-ADAccountPassword -identity svc-mimspool -NewPassword $sp
Set-ADUser -identity svc-mimspool -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-mimspool
setspn -S http/mimportal.pocmiam.intra pocmiam\svc-mimspool

```

Create the groups below (global groups).

```

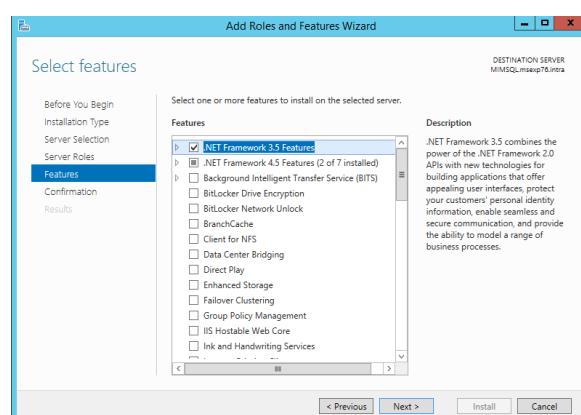
FIMSyncAdmins
FIMSyncBrowse
FIMSyncJoiners
FimSyncOperators
FIMSyncPasswordSet
SCSM-Admins

```

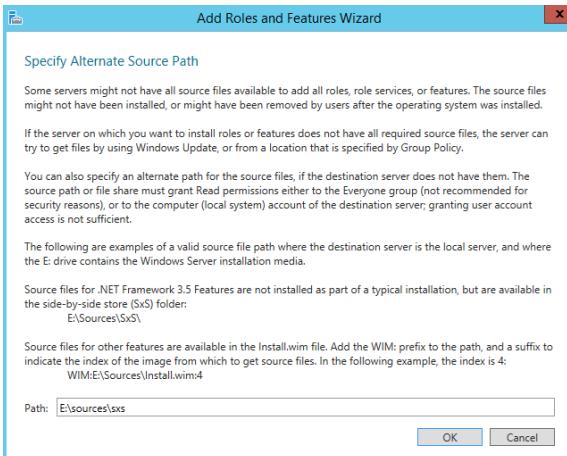
Add *svc-mimservice* as member of the group *FIMSyncPassword* (to enable *Password reset portal*).

Add *gmathieu, sa-mathieu, svc-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).

Permissions	Allow	Deny
Read only replication secret synchronization	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Reanimate tombstones	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Replicating Directory Changes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes All	<input type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes In Filtered Set	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

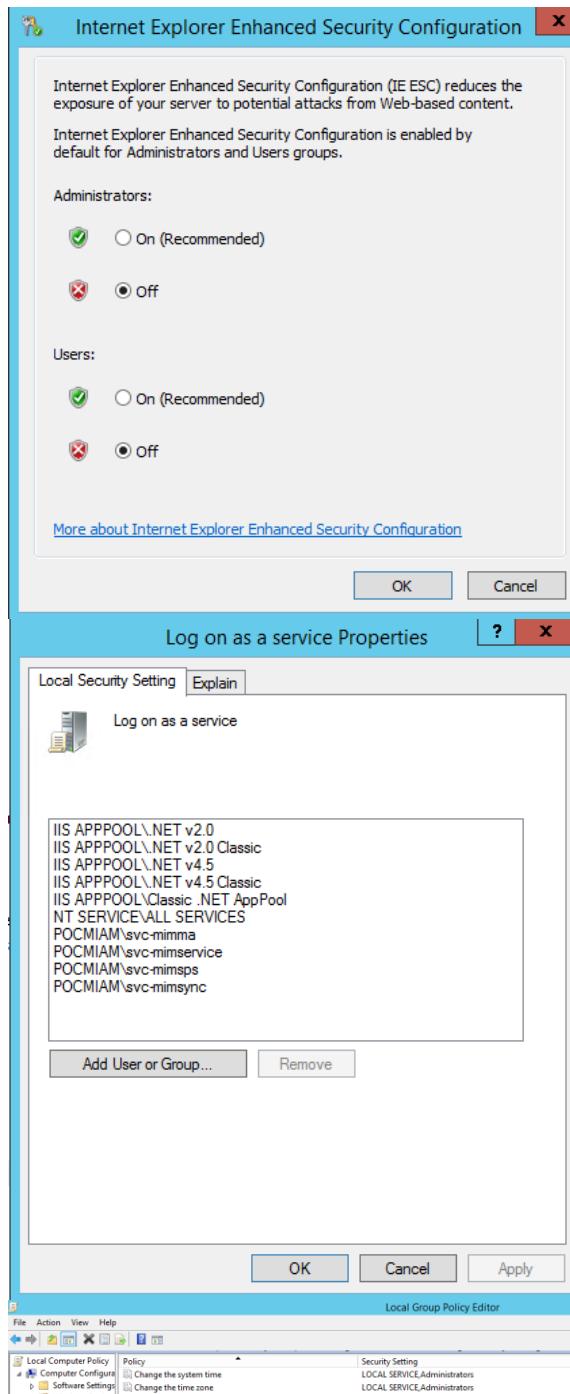
Delegate also to **pocmiam\svc-adma** the right **Replicate Directory Changes** at the domain level for **POCMIAM.INTRA** and **CHILD.POCMIAM.INTRA**. This is required to allow the MIM 2016 AD connector to perform delta sync:
<https://support.microsoft.com/en-us/kb/303972>

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-mimsp`s 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-mimsp`

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>

svc-mimservice Properties

Organization	Published Certificates	Member Of	Password Replication	
Dial-in	Object	Security	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
Delegation				

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

Do not trust this user for delegation
 Trust this user for delegation to any service (Kerberos only)
 Trust this user for delegation to specified services only
 Use Kerberos only
 Use any authentication protocol

svc-mimspool Properties

Organization	Published Certificates	Member Of	Password Replication	
Dial-in	Object	Security	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
Delegation				

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

Do not trust this user for delegation
 Trust this user for delegation to any service (Kerberos only)
 Trust this user for delegation to specified services only
 Use Kerberos only
 Use any authentication protocol

Configure *svc-mimservice* for Kerberos delegation.

```
Windows PowerShell
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator.<REDACTED> iisreset /STOP
Attempting stop...
Internet services successfully stopped
PS C:\Users\Administrator.<REDACTED> C:\Windows\System32\inetsrv\appcmd.exe unlock config /section:windowsAuthentication -commit:apphost
Configuration "system.applicationHost/system/security/authentication/windowsAuthentication" at configuration path "MACHINE/WEBROOTS/<REDACTED>" has been updated.
PS C:\Users\Administrator.<REDACTED> iisreset /START
Attempting start...
Internet services successfully started
PS C:\Users\Administrator.<REDACTED> ..
```

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advanced Security

Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Configure IIS on the server POCMIM.

iisreset /STOP
C:\Windows\System32\inetsrv\appcmd.exe unlock config /section:windowsAuthentication -commit:apphost
iisreset /START

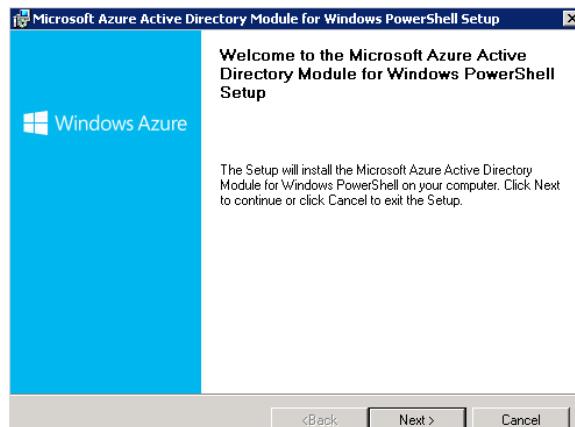
Disable Windows Firewall for the private, public and domain profils on all severs of the lab.

2.6 INSTALL AND CONFIGURE AZURE ACTIVE DIRECTORY CONNECT ON POCDC1

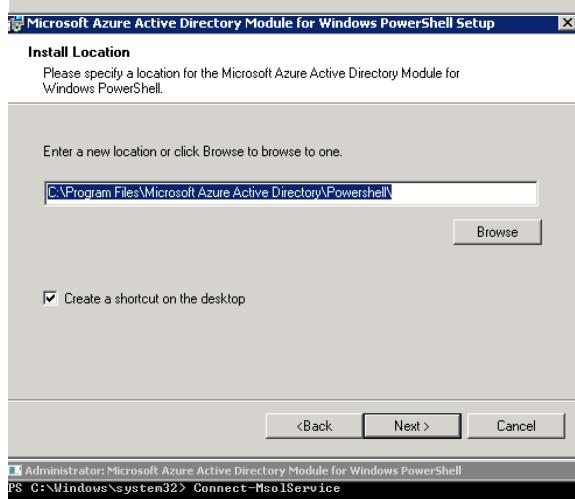
We will configure *Azure Active Directory Connect* tool to allow synchronization between Azure Active Directory and the Active Directory forest *POCMIAM.INTRA*.

This tool will also be used to replicate password from Azure Active Directory to Active Directory (Azure Active Directory Premium feature).

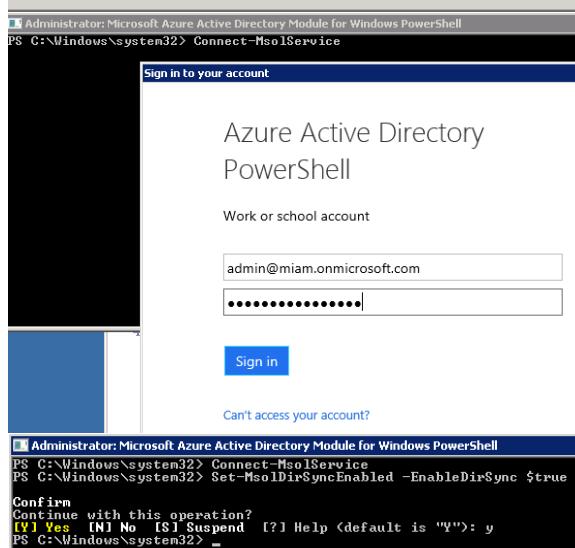
Install PowerShell V3 (Windows6.1-KB2506143-x64.msu).



Install Azure Active PowerShell module.



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



Start Azure Active Directory PowerShell module.

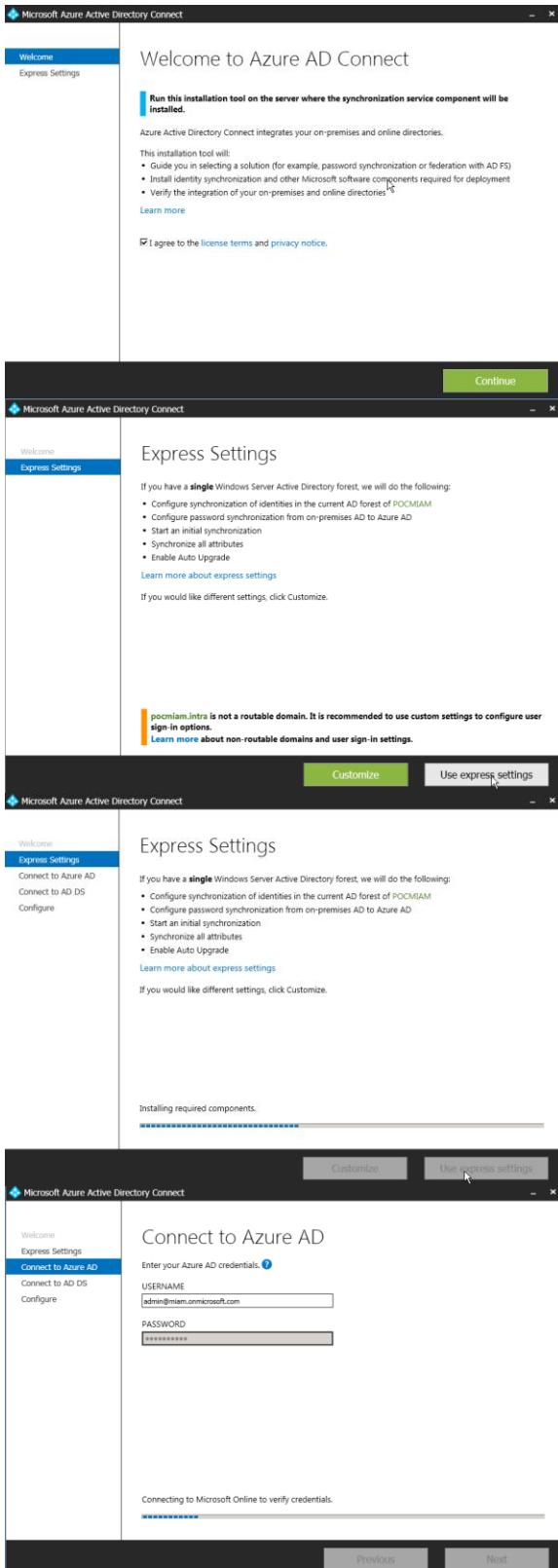
Enter the command:

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



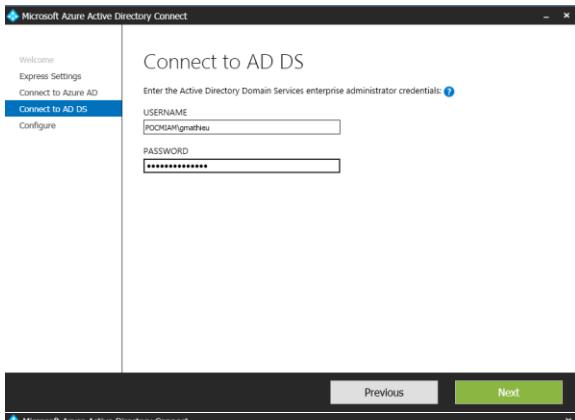
Download and start the installation of Azure Active Directory Connect:

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

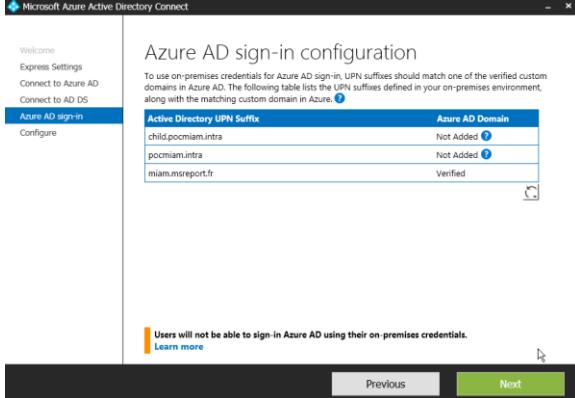
Use *Express Settings*.

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

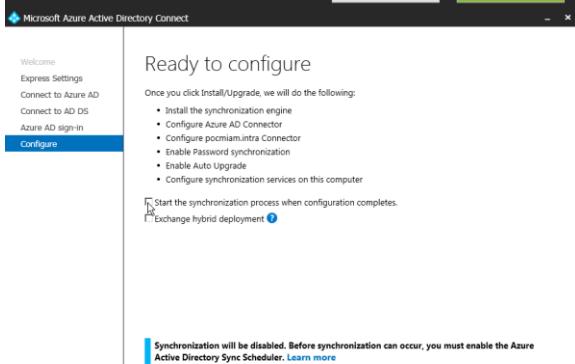
Username: *admin@miam.onmicrosoft.com*
 Click on *Next*.



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

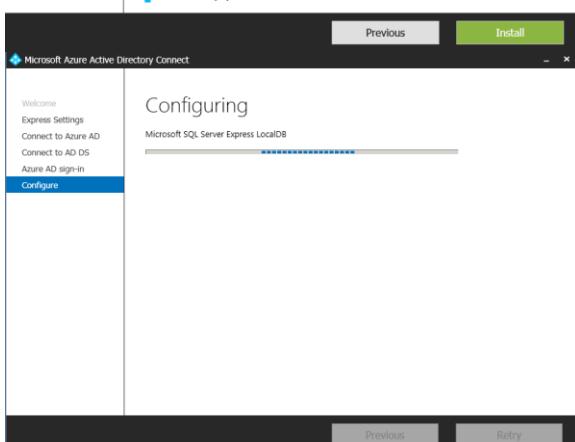


Click on *Next*.

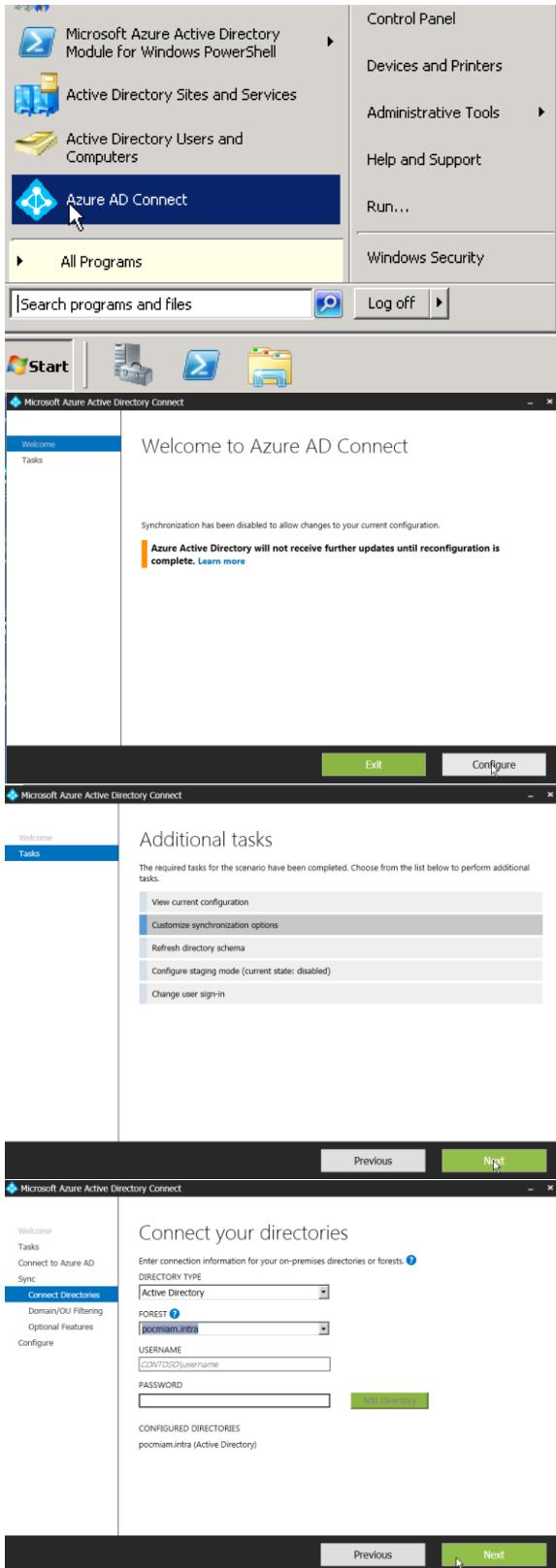


Uncheck the box [Start the synchronization process when configuration completes.](#)

Click on *Install*.



Click on *Close*.



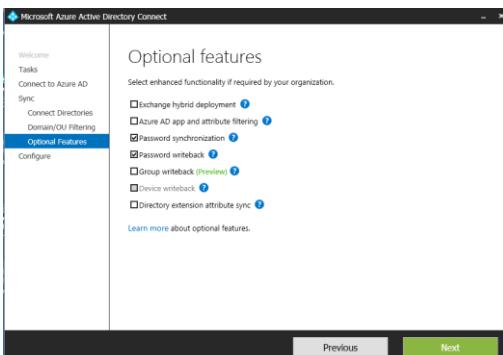
Start *Azure AD Connect* console.

Click on *Configure*.

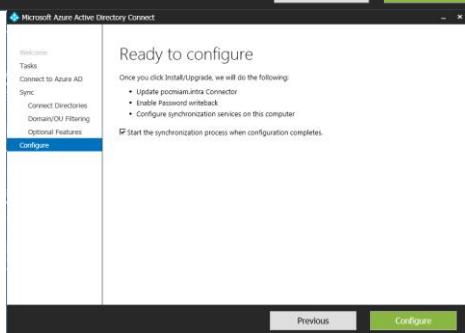
Click on *Customize synchronization options*.

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

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various services like Automation, Machine Learning, Stream Analytics, Operational Insights, and Traffic Manager. The main area is titled 'active directory' under 'miam'. It displays basic information such as 'ANNALES', 'ESPACES DE NOMS/ACCÈS CONFIÉ', 'FOURNISSEURS D'AUTHENTIFICATION MULTIFACTEUR', and 'RIGHTS MANAGEMENT'. A table lists 'NOM' (Name), 'ÉTAT' (Status), 'RÔLE' (Role), 'ABONNEMENT' (Subscription), 'RÉGION DE CENTRE DE DONNÉES' (Data Center Region), and 'PAYS OU RÉGION' (Country or Region). One row for 'miam' is selected.

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

This screenshot shows the 'Configure' tab for the 'miam' Active Directory service. It includes sections for 'UTILISATEURS', 'GROUPES', 'APPLICATIONS', 'DOMAINES', 'INTÉGRATION D'ANNEXE', 'CONFIGURER', 'RAPPORTS', and 'LICENCES'. A central message says 'Votre répertoire est prêt à être utilisé. Voici quelques options de démarrage.' Below it are buttons for 'J'E VEUX', 'Configurer l'annexe', 'Gérer les apps', and 'Développer des applications'.

Click on *Configure*.

This screenshot shows the 'Restrict access to password reset' configuration page. It has a 'RESTRICT ACCESS TO PASSWORD RESET' section with 'YES' and 'NO' buttons. Below it, 'AUTHENTICATION METHODS AVAILABLE TO USERS' lists 'Office Phone', 'Mobile Phone', 'Alternate Email Address', and 'Security Questions', with 'Office Phone' and 'Mobile Phone' checked. A 'NUMBER OF AUTHENTICATION METHODS REQUIRED' dropdown is set to '1'. Other sections include 'REQUIRE USERS TO REGISTER WHEN SIGNING IN' (set to 'YES'), 'NUMBER OF DAYS BEFORE USERS ARE ASKED TO CONFIRM THEIR AUTHENTICATION INFORMATION' (set to '360'), and 'CUSTOMIZE CONTACT YOUR ADMINISTRATOR' (set to 'NO'). Buttons at the bottom are 'SAVE' and 'DISCARD'.

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

This screenshot shows the 'Write back passwords to on-premises active directory' configuration page. It includes sections for 'REQUIRE USERS TO REGISTER WHEN SIGNING IN' (set to 'YES'), 'NUMBER OF DAYS BEFORE USERS ARE ASKED TO CONFIRM THEIR AUTHENTICATION INFORMATION' (set to '360'), 'CUSTOMIZE CONTACT YOUR ADMINISTRATOR' (set to 'NO'), 'WRITE BACK PASSWORDS TO ON-PREMISES ACTIVE DIRECTORY' (set to 'YES'), 'PASSWORD WRITE BACK SERVICE STATUS' (set to 'Configured'), and 'ALLOW USERS TO UNLOCK ACCOUNTS WITHOUT RESETTING THEIR PASSWORD' (set to 'NO'). Buttons at the bottom are 'SAVE' and 'DISCARD'.

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

This screenshot shows the 'notifications' configuration page. It includes sections for 'EMAIL LANGUAGE PREFERENCE' (set to 'English'), 'NOTIFY ADMINS WHEN OTHER ADMINS RESET THEIR OWN PASSWORD' (set to 'YES'), 'NOTIFY USERS AND ADMIN WHEN THEIR OWN PASSWORD HAS BEEN RESET' (set to 'YES'), 'multi-factor authentication' (with a 'Manage service settings' link), and 'devices' (with a 'USERS MAY JOIN DEVICES TO AZURE AD' dropdown set to 'ALL SELECTED NONE'). Buttons at the bottom are 'SAVE' and 'DISCARD'.

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](#).

Check out

confirm your order

Enterprise Mobility + Security E5 | 90 day subscription
250 users

Click on [Try now](#).

order receipt

Your confirmation number is: 1ecfe7c2-7613-46a6-8552-6c609e46b9a9
Important: To use your new licenses, make sure to assign them by editing users on the [Users](#) page.

Click on [Continue](#).

Order details

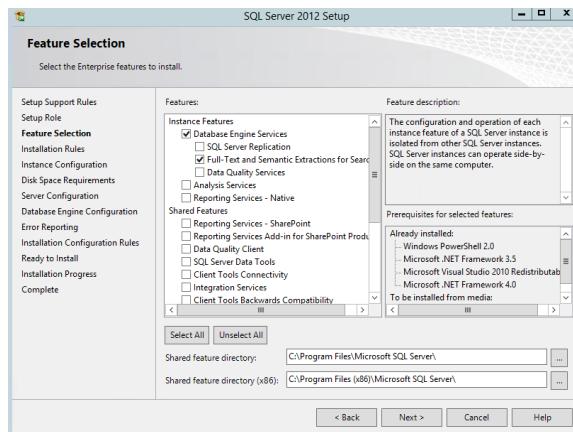
Enterprise Mobility + Security E5 | 90 day subscription
250 users

2.8 INSTALL POCMIM

2.8.1 Install SQL server on POCMIM

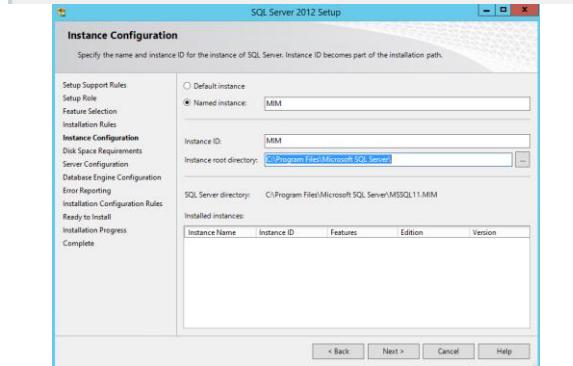
Download Windows 2012 R2 installation file to install .Net Framework 3.5.

This is a prerequisite for SQL server 2012 SP3. Check that `pocmiam\svc-sql` is member of the local administrators group on POCMIM.

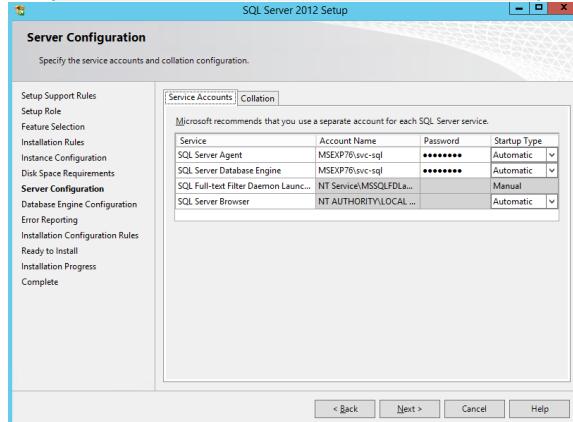


Select the following components:

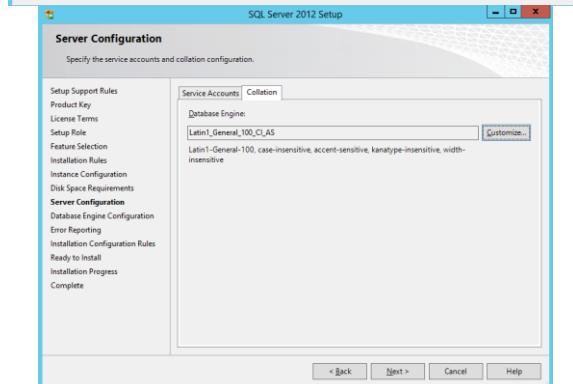
- *Database engine*
- *Full-text search*
- *Management Tools - Basic*
- *Management Tools - Complete*



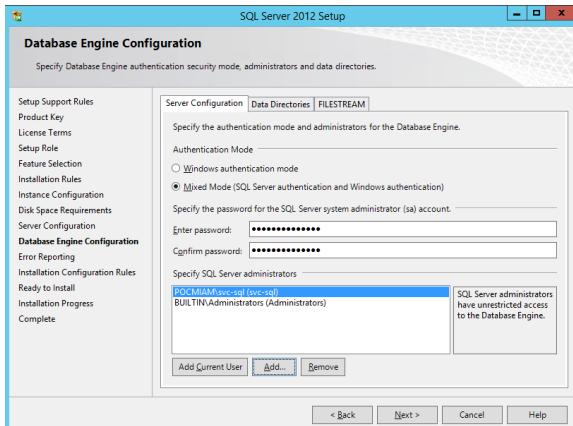
Enter *MIM* as Instance name.



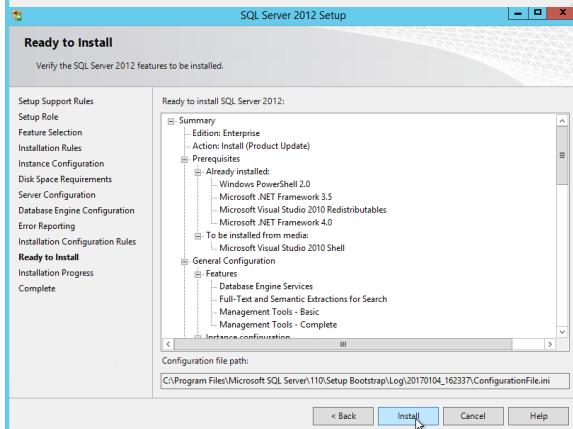
Click on *Next*.



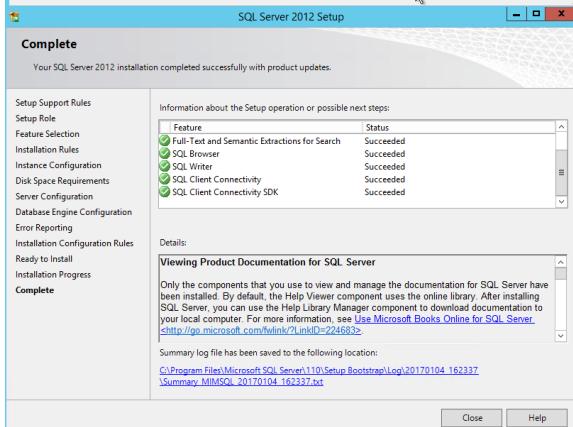
Collation: *Latin1_General_100_CI_AS*



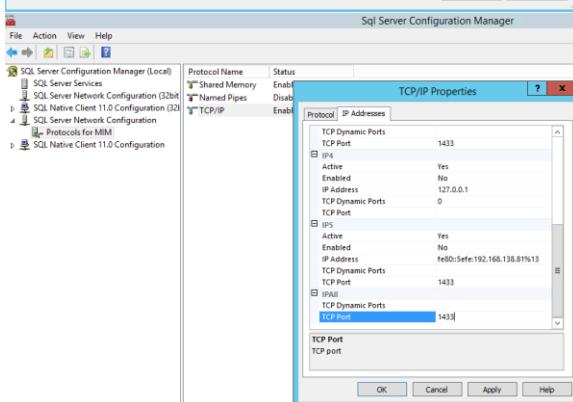
Add `pocmiam\svc-sql` and local administrators group as SYSADMIN.



Click on *Install* button.



Click on *Close* button.



Start SQL Server Configuration Manager.
Go to *Protocols for MIM* properties in the tab *IP Adresses*.

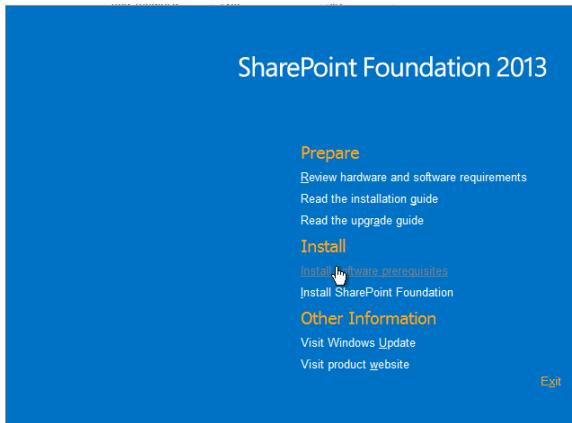
Configure SQL Server database to listen on port *TCP 1433*.

2.8.2 Install SharePoint 2013 Foundation on POCMIM

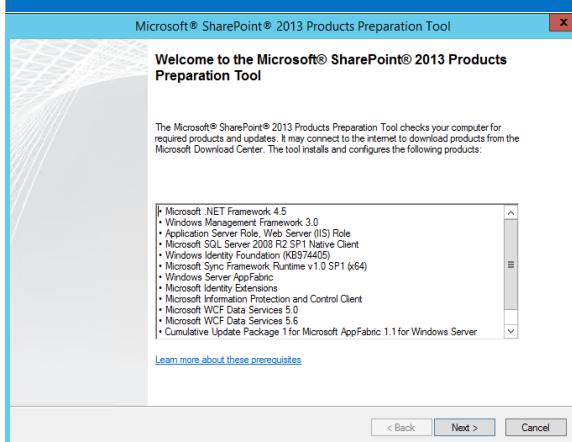
This documentation is based on <https://docs.microsoft.com/fr-fr/microsoft-identity-manager/deploy-use/prepare-server-sharepoint>

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

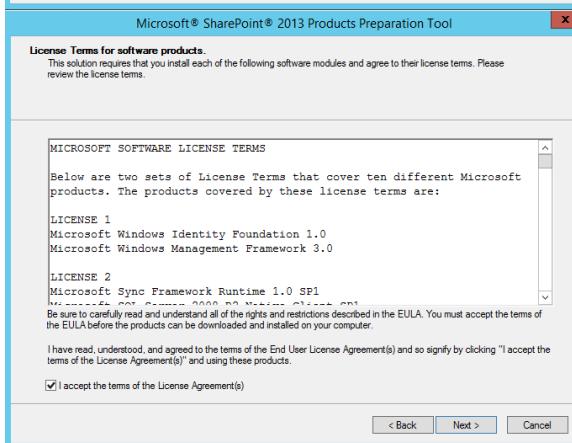
Check that the user account `pocmiam\svc-mimsp` is a local administrator of the server POCOIM.



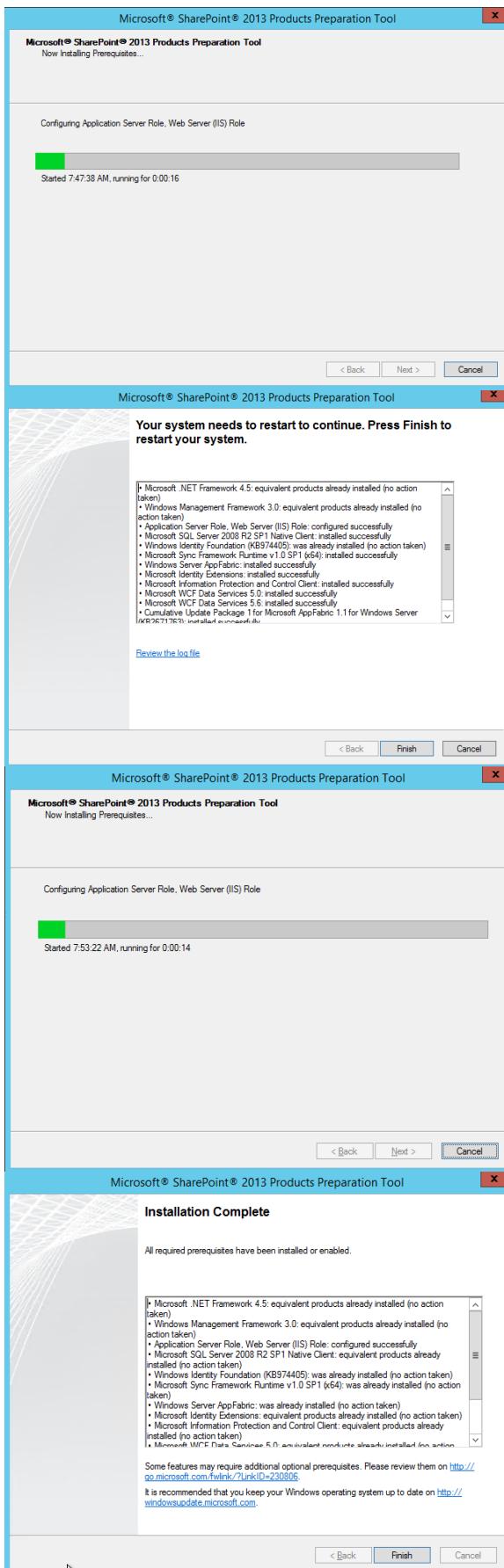
Click on *Install Software prerequisites*.



Click *Next*.



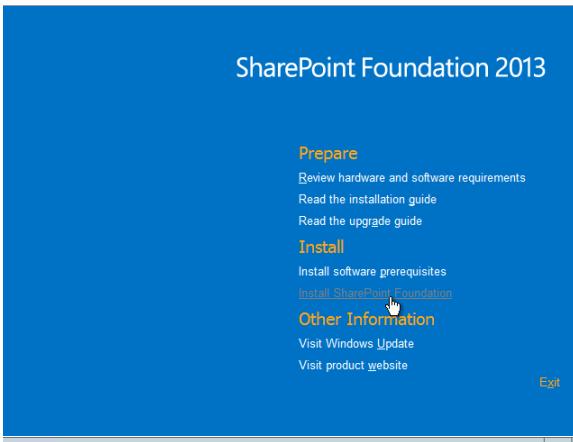
Click *Next*.



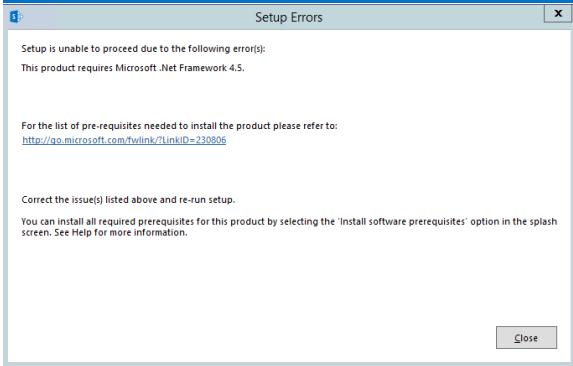
Click on *Finish* and then restart the server.

After Restart, the installation continues.

Click on *Finish* button.



Start the installation of SharePoint 2013 Foundation.

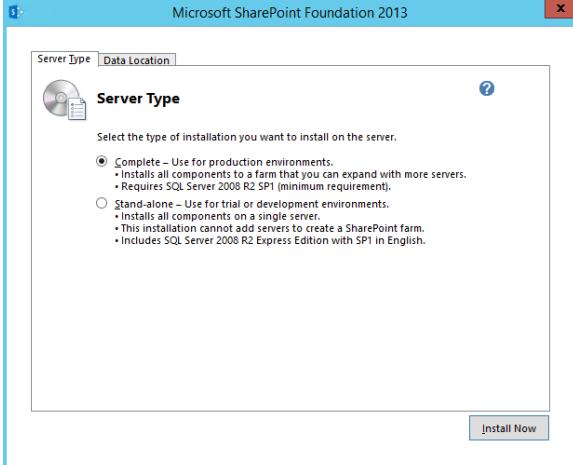


If the following message appears, apply this procedure:

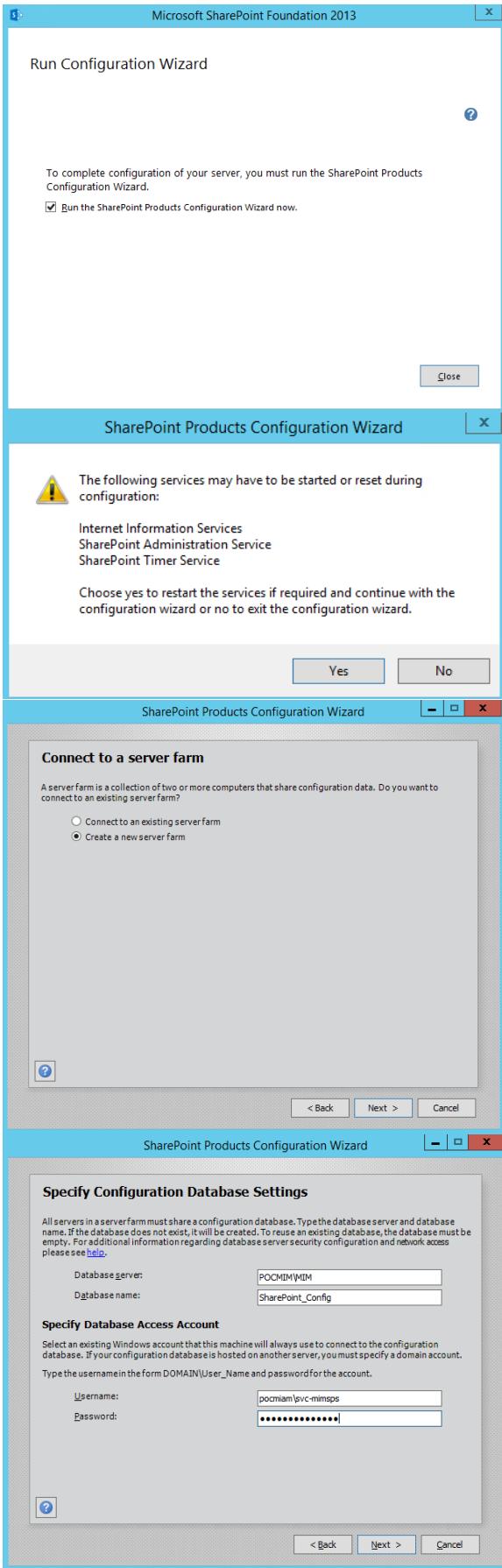
<https://support.microsoft.com/fr-fr/help/3087184/sharepoint-2013-or-project-server-2013-setup-error-if-the-.net-framework-4.6-is-installed>



Click on *Continue*.



Click on *Install Now*.

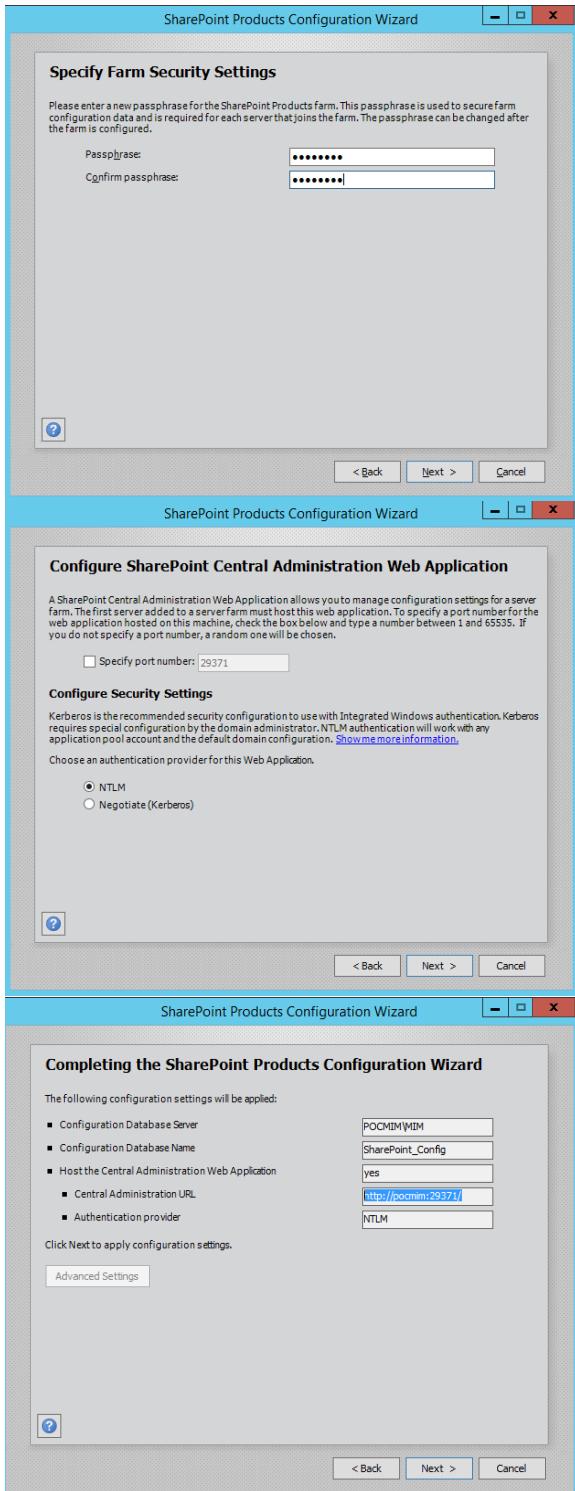


Click on *Close*.

Click *Yes*.

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

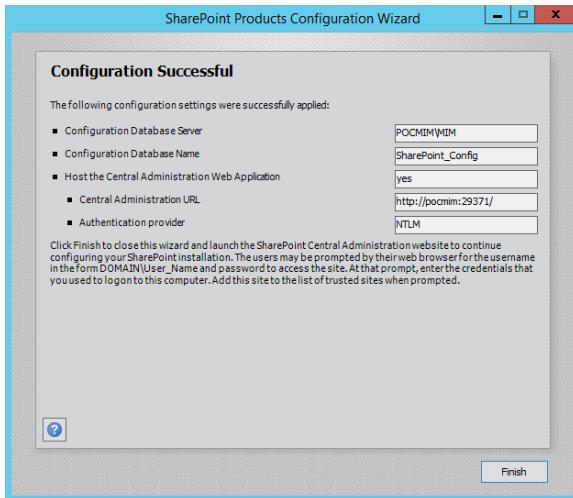
Enter the following information:
Database Server: *POCMIM\MIM*
Database name: *SharePoint_Config*
User: *pocmiam\svc-mimsp*



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

The screenshot shows the 'Administrator: SharePoint 2013 Management Shell' window. The command executed was:

```
PS C:\Users\gmathieu.POCMIM> $adminCredentials = get-credential pocmiam\svc-mimspool
PS C:\Users\gmathieu.POCMIM> $dbManagedAccount = New-SPManagedAccount -Credential $adminCredentials
PS C:\Users\gmathieu.POCMIM> New-SpWebApplication -Name "MIM Portal" -ApplicationPool "MIMAppPool" -ApplicationPoolAccount $dbManagedAccount -AuthenticationMethod "Kerberos" -Port 80 -URL http://mimportal.pocmiam.intra
```

A warning message is displayed:

WARNING: The Windows Classic authentication method is deprecated in this release and the default behavior of this cmdlet, which creates Windows Classic based web applications, is obsolete. It is recommended to use the Claims authentication methods. You can create a web application that uses Claims authentication method by specifying the AuthenticationProvider parameter set in this cmdlet. Refer to the <http://go.microsoft.com/fwlink/?LinkId=234549> site for more information. Please note that the default behavior of this cmdlet is expected to change in the future release to create a Claims authentication based web application instead of a Windows Classic based web application.

Display Name	Url
MIM Portal	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-mimspool -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.POCTIAM>
PS C:\Users\gmathieu.POCTIAM>
PS C:\Users\gmathieu.POCTIAM> $t = Get-SPWebTemplate -compatibilityLevel 14 -Identity "STS#1"
PS C:\Users\gmathieu.POCTIAM> $w = Get-SPWebApplication "MIM Portal"
PS C:\Users\gmathieu.POCTIAM> New-SPSite -Url $w.Url -Template $t -OwnerAlias pocmiam\svc-mininstall -CompatibilityLevel 14 -Name "MIM Portal" -SecondaryOwnerAlias pocmiam\svc-mininstall
Url                                         CompatibilityLevel
http://mimportal.pocmiam.intra                                14

PS C:\Users\gmathieu.POCTIAM> $s = SpSite($w.Url)
PS C:\Users\gmathieu.POCTIAM> $s.AllowSelfServiceUpgrade = $false
PS C:\Users\gmathieu.POCTIAM> $s.CompatibilityLevel = 14
PS C:\Users\gmathieu.POCTIAM> $contentService = [Microsoft.SharePoint.Administration.SPWebService]::ContentService;
PS C:\Users\gmathieu.POCTIAM> $contentService.ViewStateOnServer = $false;
PS C:\Users\gmathieu.POCTIAM> $contentService.Update();
PS C:\Users\gmathieu.POCTIAM> $imPortalUrl = "http://mimportal.pocmiam.intra"
PS C:\Users\gmathieu.POCTIAM> Set-SPWebApplication -Identity $imPortalUrl -AuthenticationMethod Kerberos -Zone Default
PS C:\Users\gmathieu.POCTIAM> cd c:\windows\system32\inetsrv
PS C:\windows\system32\inetsrv> .\config\applicationHost.config .\config\applicationHost.config.bak
PS C:\windows\system32\inetsrv> .\appcmd.exe set config "MIM Portal" /section:windowsAuthentication
Applied configuration changes to section "system.webServer/security/authentication/windowsAuthentication" for "MACHINE/WEBROOT/APPHOST/MIM Portal" at configuration commit path "MACHINE/WEBROOT/APPHOST/MIM Portal"
PS C:\windows\system32\inetsrv> =

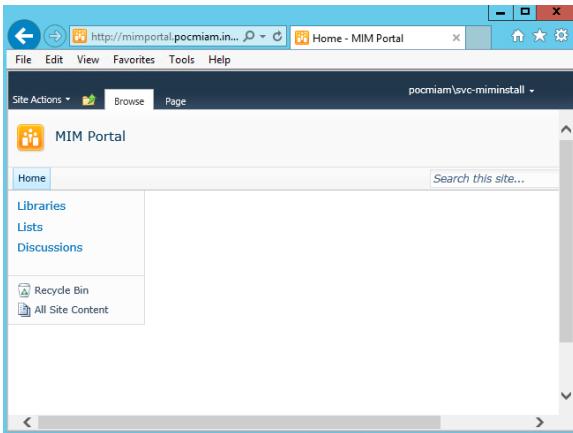
```

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

Type	Host Name	Port	IP Address	Binding Information
net.m...			localhost	
msm...			localhost	
net.tcp		8080*	*	
http		8080	*	



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



Disable indexing. Start SharePoint 2013 Management Shell:

Get-SPTimerJob hourly-all-sptimerservice-health-analysis-job | disable-SPTimerJob

```
'$ C:\> Get-SPTimerJob hourly-all-sptimerservice-health-analysis-job | disable-SPTimerJob
'$ C:\> _
```

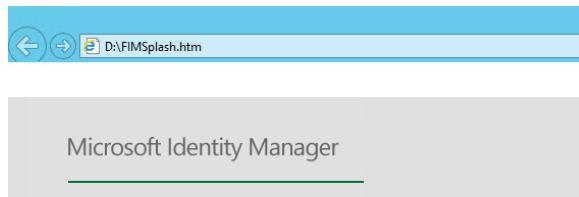
Restart the server.

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.

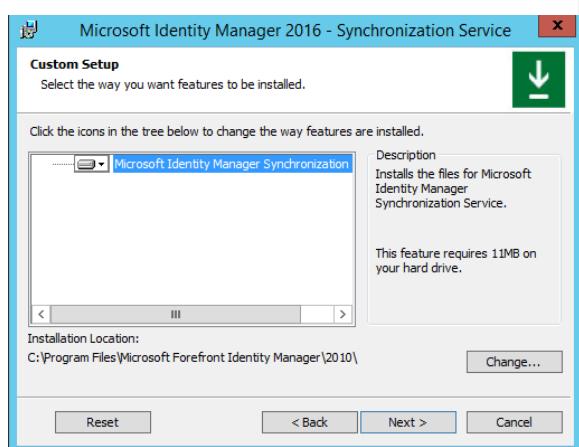
Check if SQL Server 2012 native client is installed on POCMIM.



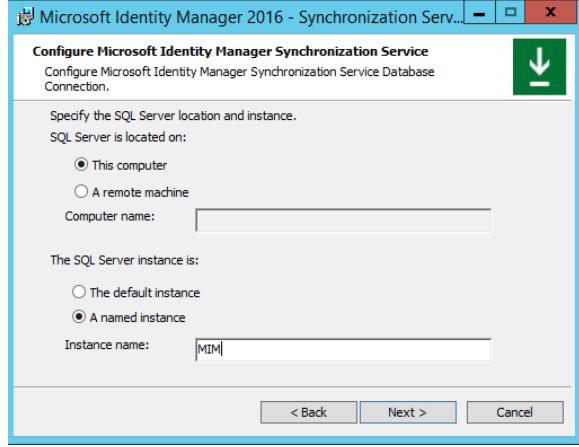
The screenshot shows a browser window with the address bar containing `D:\FIMSplash.htm`. The main content area displays the Microsoft Identity Manager logo and navigation links for "Identity Manager Service and Portal" and "Identity Manager Synchronization Service".

Open a session with a domain user which have local administrator right.

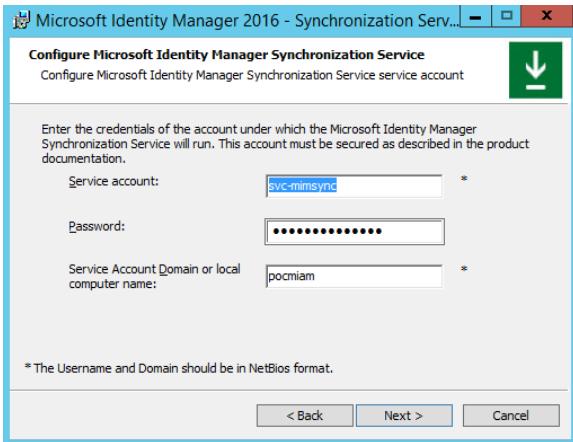
Check if you have created the 5 MIM Synchronization Service groups created previously. Click on *Install Synchronization Service* link.



Click on *Next >*.



Select a named instance and enter `MIM`.



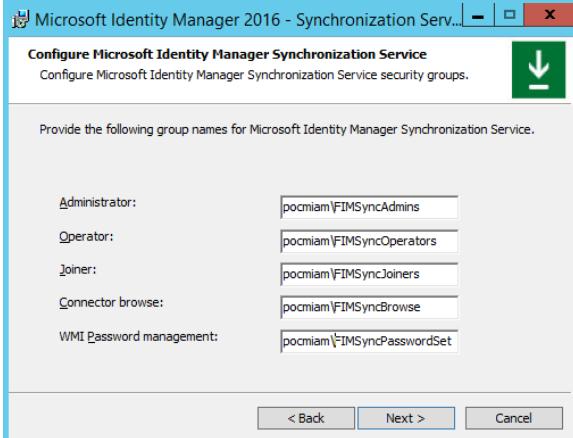
Enter the following information:

Service account: *svc-mimsync*

Password: *enter the password*

Service Account Domain or local computer name:
pocmiam

The domain name must be entered in NETBIOS format.



Administrator: *pocmiam\FIMSyncAdmins*

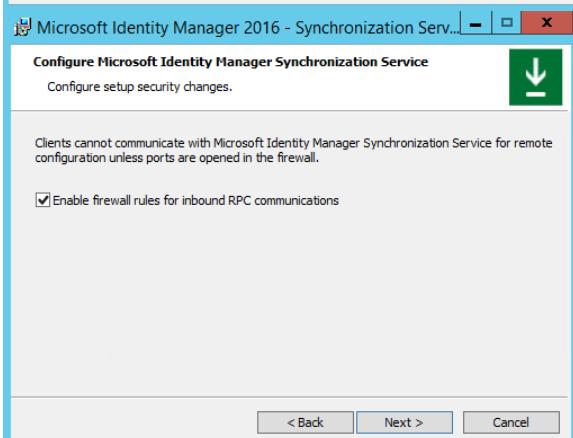
Operator: *pocmiam\FimSyncOperators*

Joiner: *pocmiam\FIMSyncJoiners*

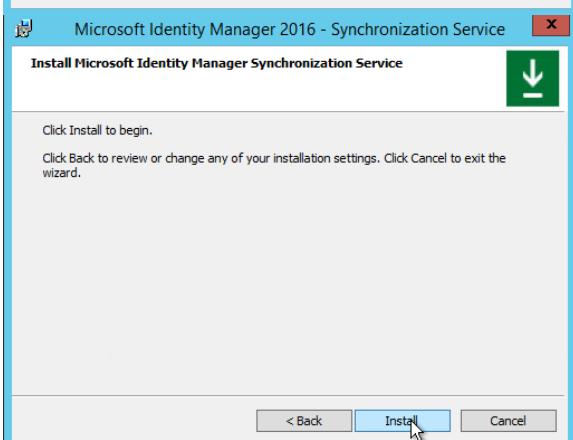
Connector browse: *pocmiam\FIMSyncBrowse*

WMI Password Management:

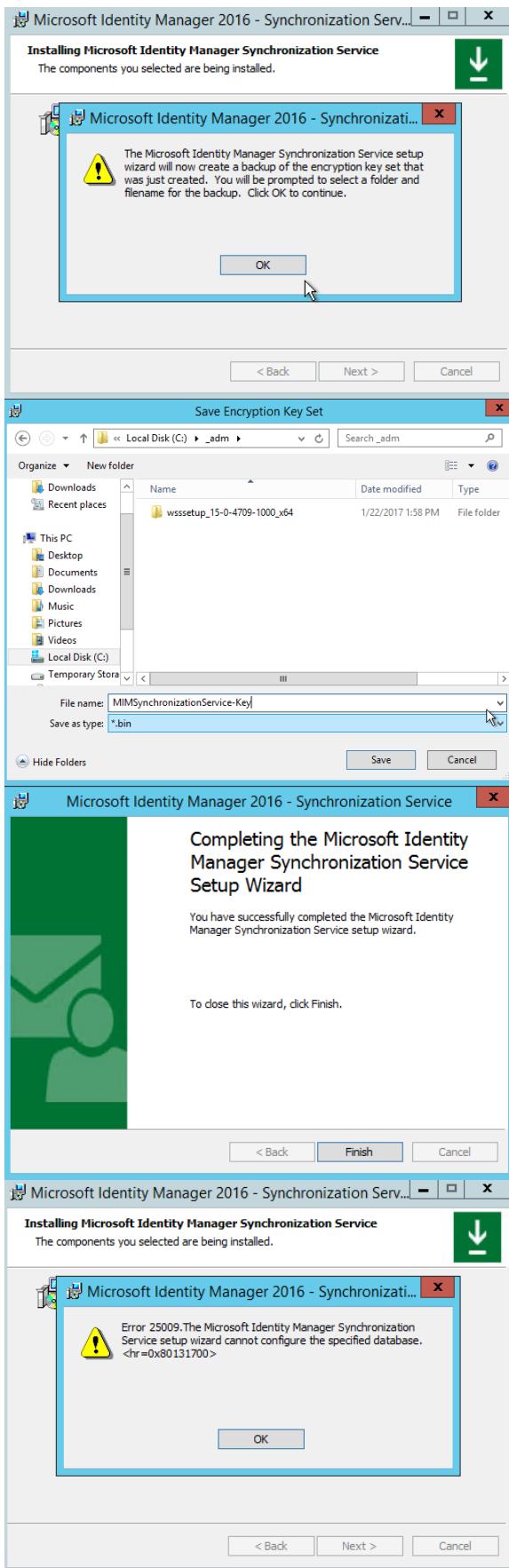
pocmiam\FIMSyncPasswordSet



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:

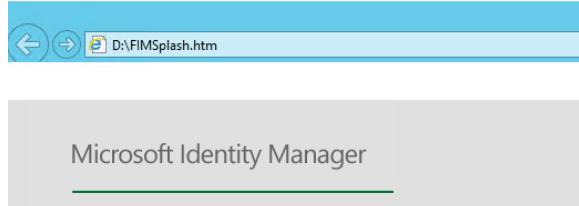
```
msiexec /i "D:\Synchronization
Service\Synchronization Service.msi" /L*v
c:\Log\LOG.txt
```

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`.

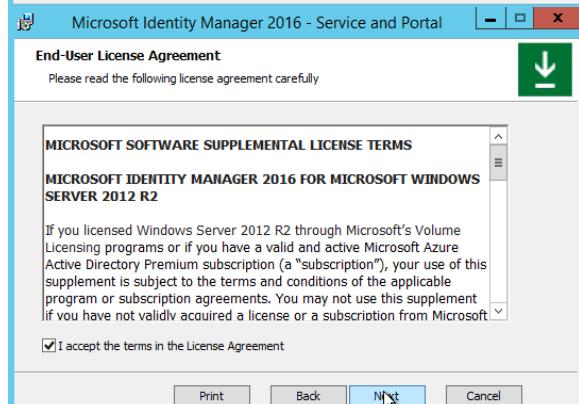
This user has local administrative right on POCMIM server, on the SharePoint Server and on SQL server instance. Provide SYSADMIN right to this account: `Pocmiam\svc-mimma`.



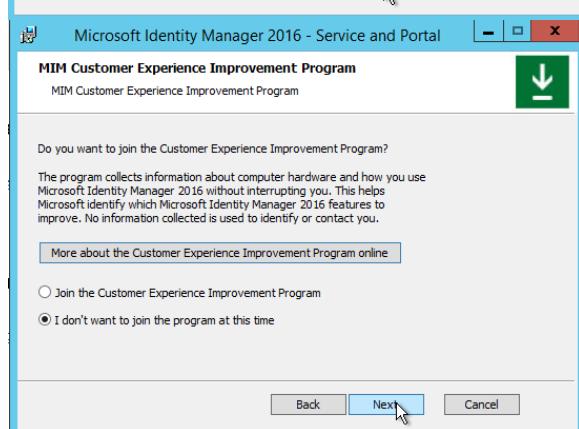
Click on *Install Service and Portal*.



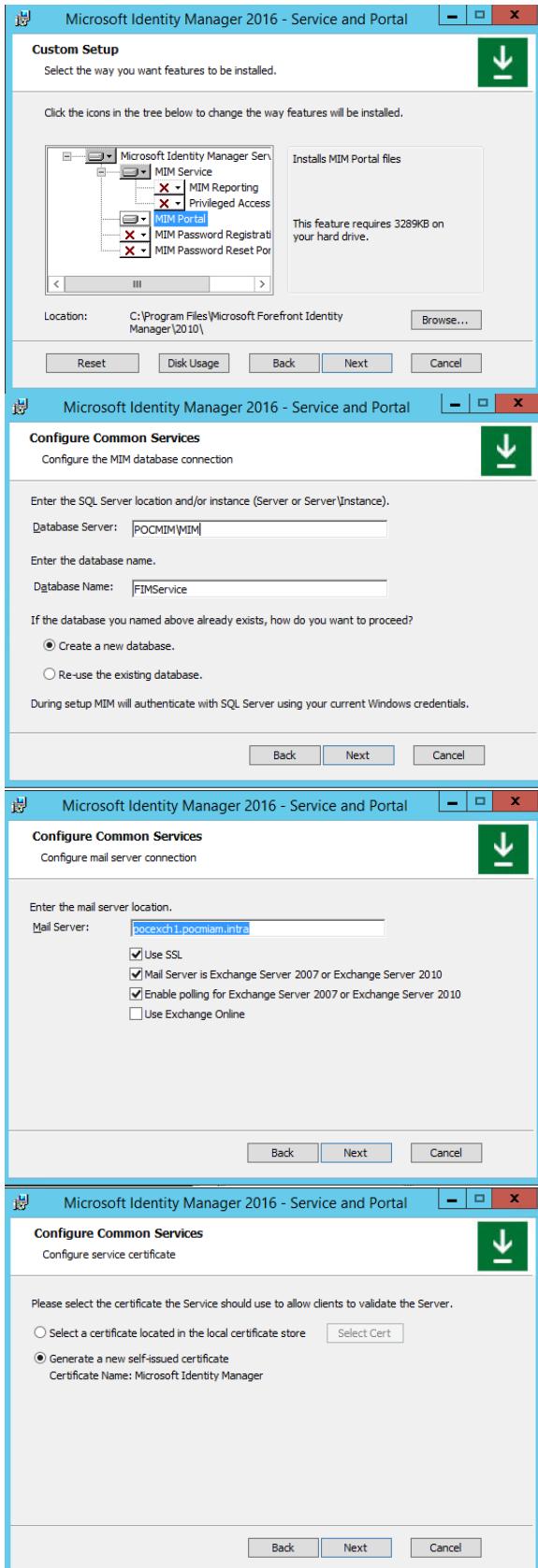
Click on *Next*.



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*.

Microsoft Identity Manager 2016 - Service and Portal

Configure Common Services

Configure the MIM service account

Enter the credentials of the account under which the MIM service will run. This account must be locked down as described in the product documentation.

Service Account Name:

Service Account Password:

Service Account Domain:

Service Email Account:

Service Email Account Password:

IMPORTANT: The service email account is used to process requests and approvals. This email account should be created for the exclusive use of the Identity Management service. Please see the Before You Begin section of the Setup Guide for more information.

Back Next Cancel

Microsoft Identity Manager 2016 - Service and Portal

Configure Common Services

Configure the Microsoft Identity Manager Service and Portal synchronization...

Enter information about the MIM synchronization server.

Synchronization Server:

MIM Management Agent Account: *

Domain\Account

* Enter the domain and user name of the Microsoft Identity Manager Service and Portal Management Agent account. This is the account entered on the "Connect to Database" page in the Management Agent creation wizard.

Back Next Cancel

Microsoft Identity Manager 2016 - Service and Portal

Configure MIM Service and Portal

Configure connection to the MIM Service

Enter the server address the MIM Portal and other clients should use to contact the MIM Service. Do not use localhost or prefix http:// or https:// to the server address.

MIM Service Server address: *

* If this is a stand alone installation, this should be the name of the server itself. If this is a scaled out installation, this should be the name the clients should use to contact the cluster.

Back Next Cancel

Microsoft Identity Manager 2016 - Service and Portal

Configure MIM Service and Portal

Configure connection to the MIM Service

Enter the URL to the SharePoint site collection where the MIM Portal should be hosted.

Sharepoint site collection URL:

Back Next Cancel

Enter the following information:

Service Account Name: *svc-mimservice*

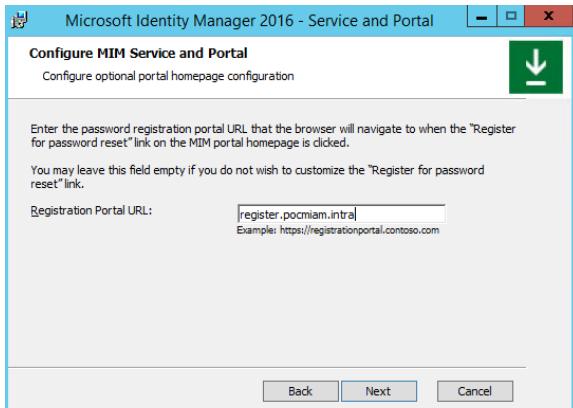
Service Account Domain: *pocmiam.intra*

Service Email Account: *gmathieu@pocmiam.intra*

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

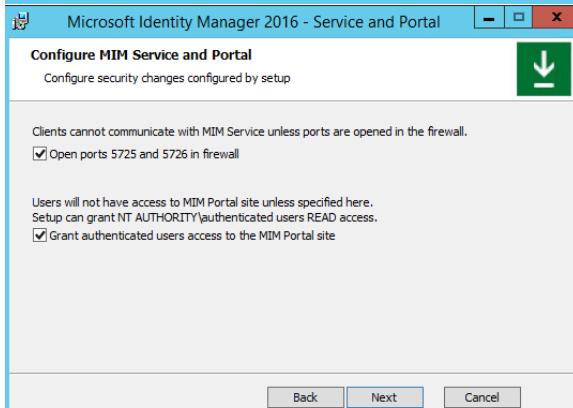
MIM Service Server address:
Mimservice.pocmiam.intra

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

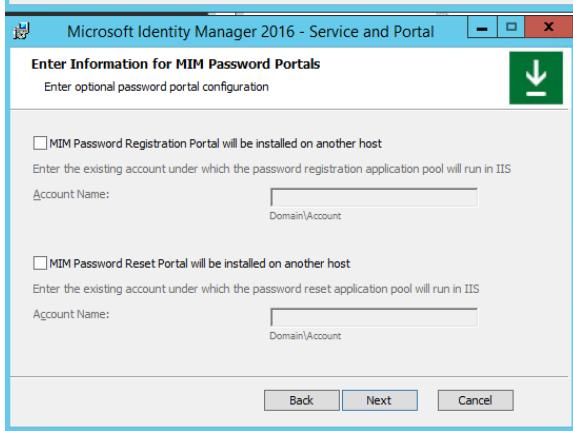


Registration Portal URL:

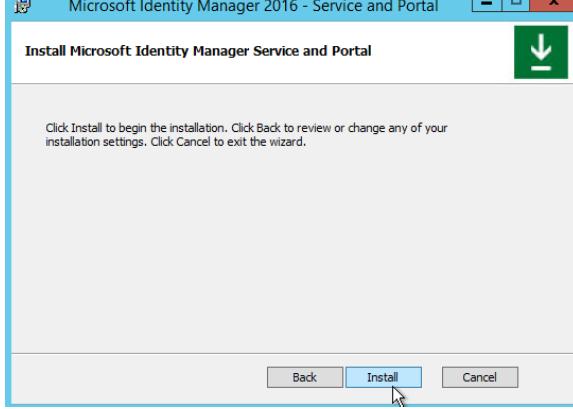
https://register.pocmiam.intra



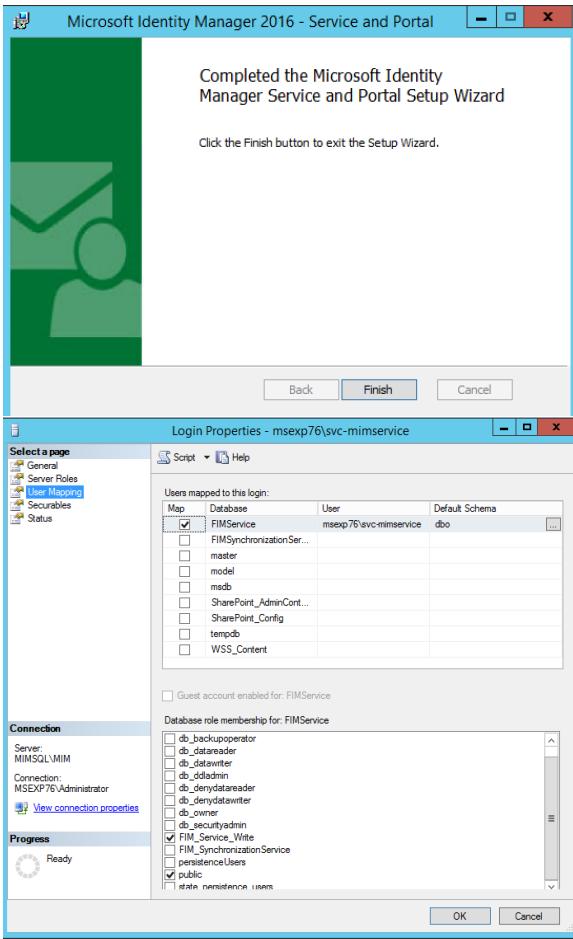
Check the boxes *Open ports 5725 and 5726 in firewall* and *Grant authenticated users access to MIM Portal site*.



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.

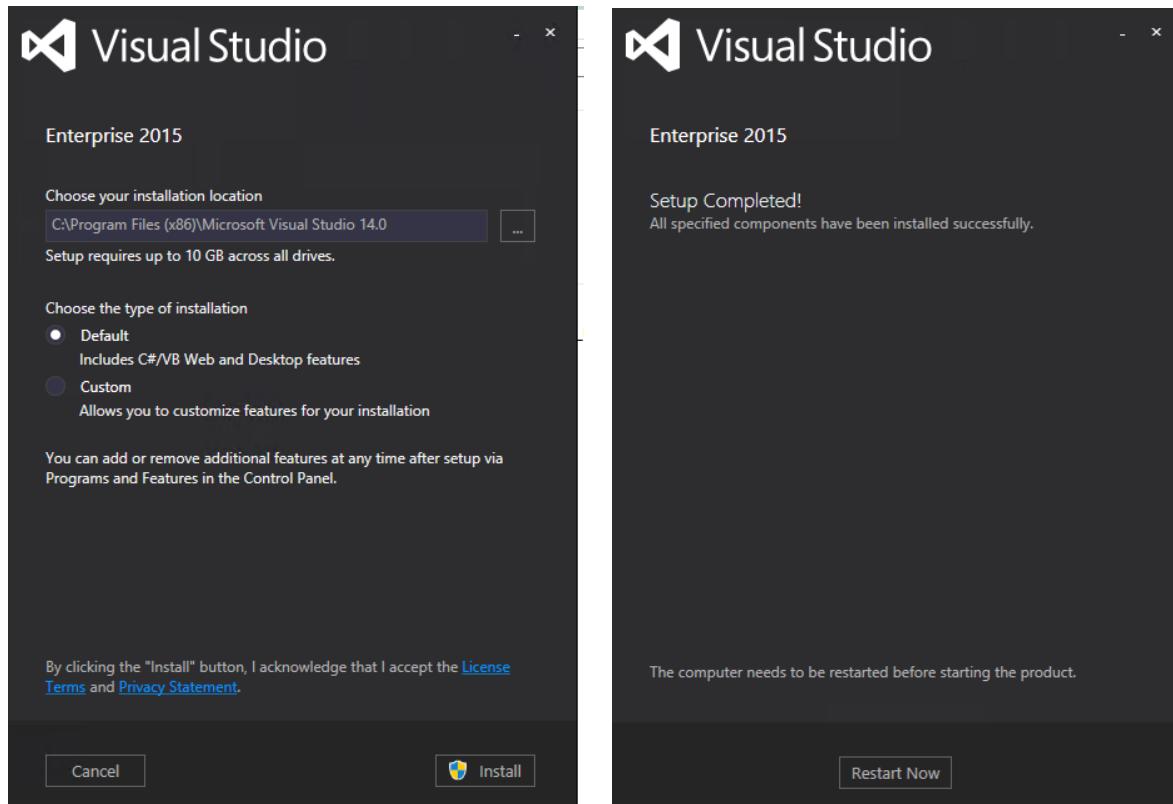
Connect to: <http://mimservice.pocmiam.intra/IdentityManagement>

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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\svc-mimininstall> cd C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\
PS C:\Users\svc-mimininstall>
PS C:\Users\svc-mimininstall> C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\Scripts\sn.exe -K C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\WAL.snk

Microsoft (R) .NET Framework Strong Name Utility Version 3.5.30729.1
Copyright (c) Microsoft Corporation. All rights reserved.

Invalid option K
PS C:\Users\svc-mimininstall> C:\_adm\MIMWAL-2.16.1028.0\MIMWAL-2.16.1028.0\src\Scripts\sn.exe -k ..\WAL.snk

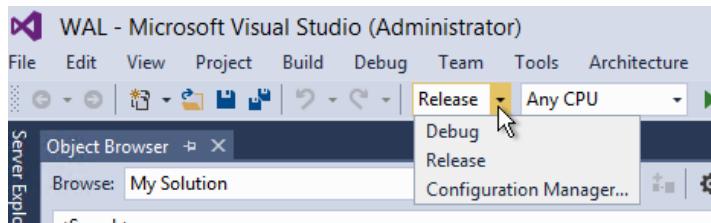
Microsoft (R) .NET Framework Strong Name Utility Version 3.5.30729.1
Copyright (c) Microsoft Corporation. All rights reserved.

Key pair written to ..\WAL.snk
PS C:\Users\svc-mimininstall>
```

Copy the pair key to the proper emplacement.

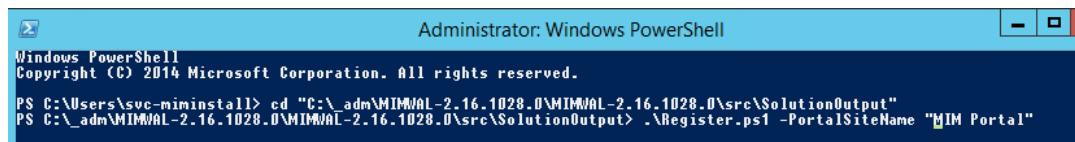
Edit the file *WAL.sln* with Visual Studio.

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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\svc-mimininstall> 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"
```

```

PS C:\Users\suc-mimininstall> cd "C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput"
PS C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput> .\Register.ps1 -PortalSiteName "MIM Portal"
DEBUG: Registering assembly in GAC:
'C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivityLibrary.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\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivityLibrary.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\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivityLibrary.dll'
DEBUG: Loading Assembly:
'C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivityLibrary.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\Microsoft.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 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 MIMMAL XOMLs by executing UpdateWorkflowXoml.ps1 script.
PS C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput> .

```

Start also the command: *UpdateWorkflowXoml.ps1*

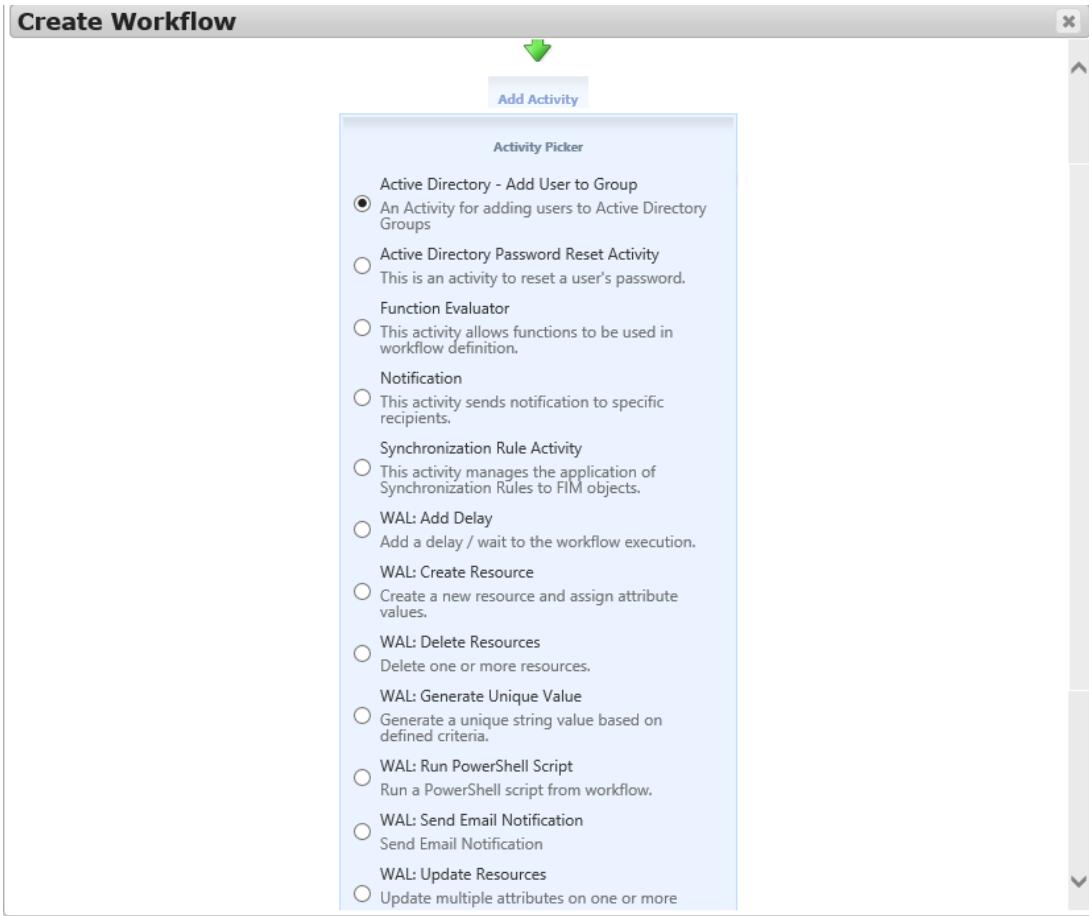
```

PS C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput> .\UpdateWorkflowXoml.ps1
DEBUG: Loading Assembly:
'C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput\MicrosoftServices.IdentityManagement.WorkflowActivityLibrary.dll'

Skipping Workflow : '_AD User Deletion Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : '_AD User Deprovision Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : '_Add-To-Group'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : '_AD-Out-Test1'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : '_Security Group Provisioning to AD'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Expiration Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Filter Validation Workflow for Administrators'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Filter Validation Workflow for Non-Administrators'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Group Expiration Notification Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Owner Approval Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'PAM: Handle PAM Request'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'PAM: Request Authorization'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Password Reset Action Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Password Reset AuthN Workflow'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Requestor Validation With Owner Authorization'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'Requestor Validation Without Owner Authorization'. No updates necessary. It does not use any MIMMAL activities.
Skipping Workflow : 'System Workflow Required for Registration'. No updates necessary. It does not use any MIMMAL activities.
PS C:\_adm\MIMMAL-2.16.1028.0\MIMMAL-2.16.1028.0\src\SolutionOutput> .

```

Check that all news workflow activities are available.



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 automatically: 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 : <i>Internal</i> and <i>External</i> 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 : <i>givenname + . + Sn.</i> <i>In case of conflict, add a digit</i> 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	I	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 maîtrise": 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>

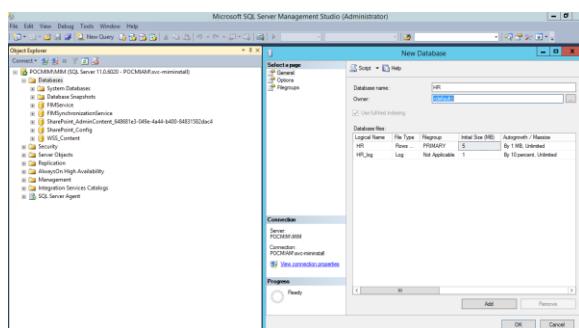
The script *CreateCSV-V6.ps1* generates the HR CSV file with a specified number of random users.

You can also define the number of entity.

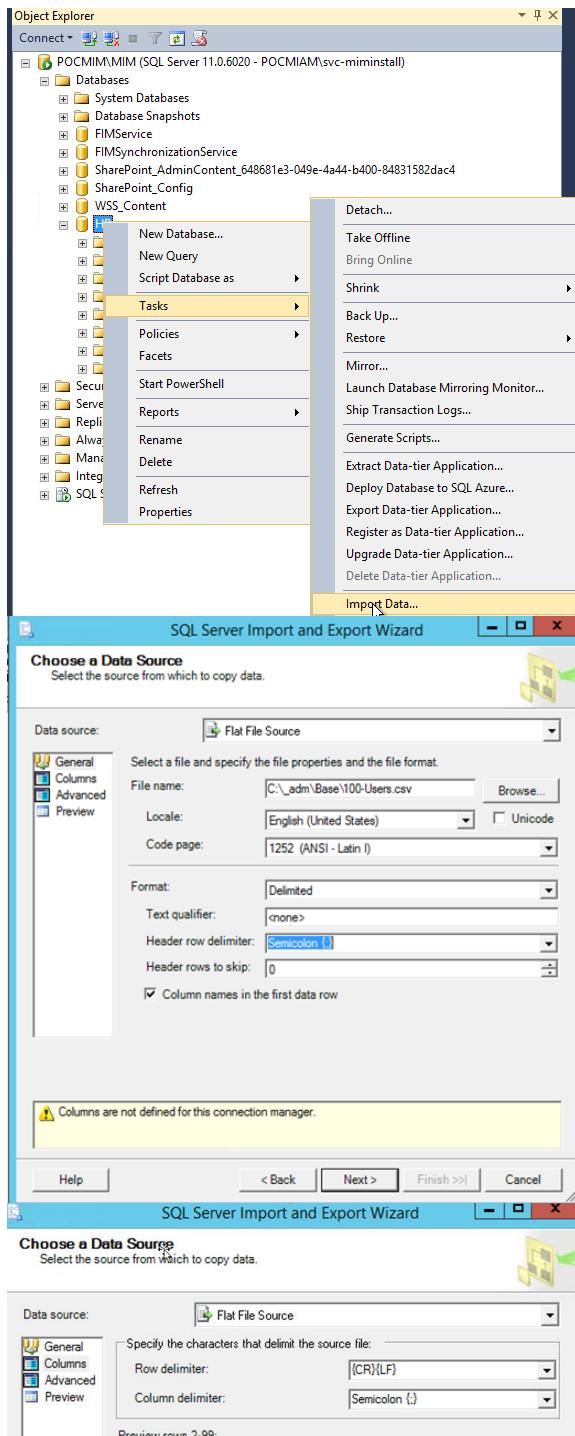
Each entity has a level 1 manager, a few level 2 managers and standards internal or external users.

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.



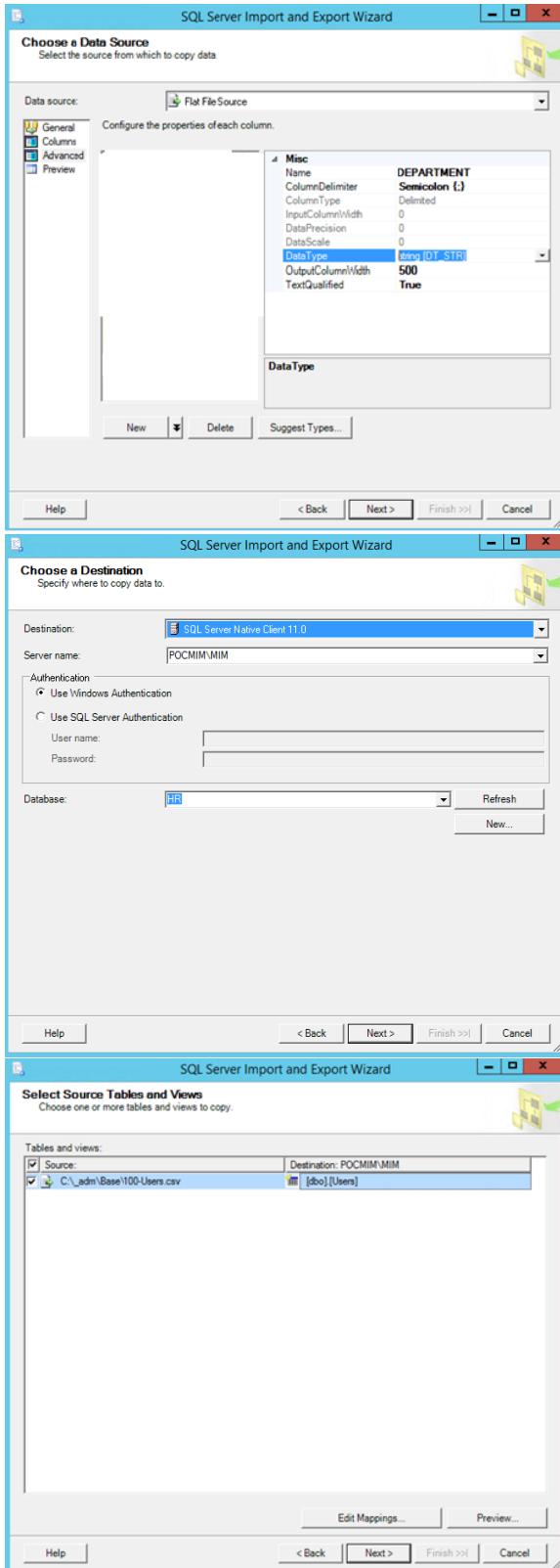
Create the HR SQL Server database.



Import the CSV as a new table.

Text qualifier: *semicolon*

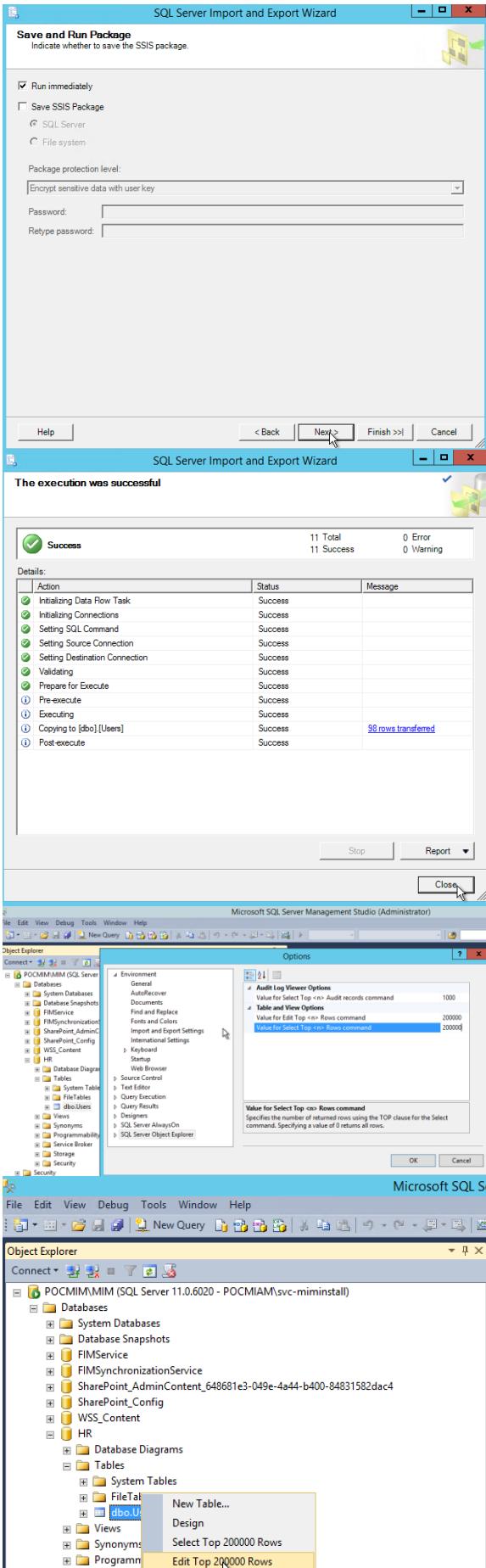
Click on *Advanced* Tab.



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

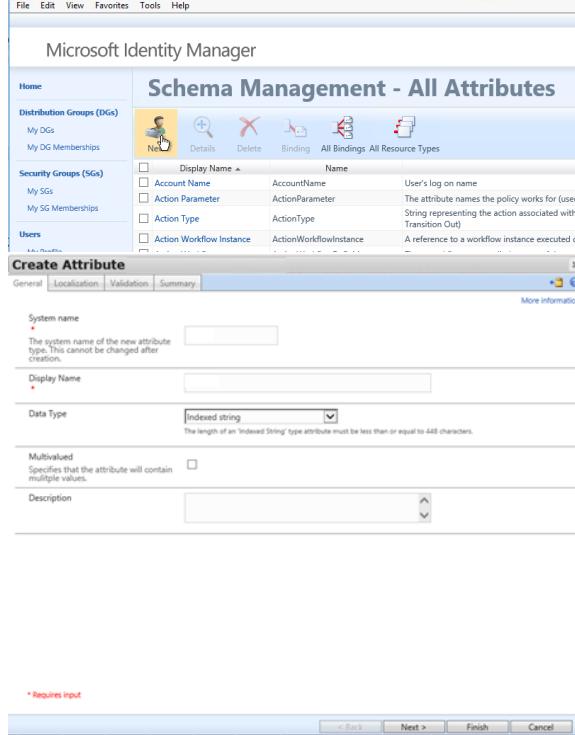
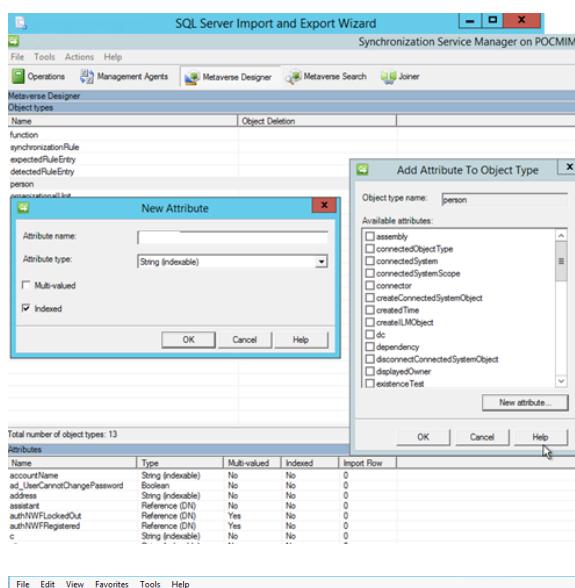
`C:\Program Files\Common Files\microsoft shared\Web Server Extensions\14\TEMPLATE\IMAGES\MSILM2`

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/IdentityManager/aspx/schema/AllAttributeDescriptions.aspx).
<https://mimportal.pocmiam.intra/IdentityManager/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 Binding

General | Attribute Override | Localization | Validation | Summary | More information

Resource Type: User

Attribute Type: Rank

Required:

* Requires input

< Back Next > Finish Cancel

Create all bindings.

Assign each new attribute to the class *Person*.

<https://mimportal.pocmiam.intra/IdentityManager/aspx/schema/AllBindingDescriptions.aspx>

Microsoft Identity Manager

Administration

- My DGs
- My DG Memberships
- My SGs
- My SG Memberships
- My Profile
- Authentication Workflow Registration
- Workflows
- Sets

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

Microsoft Identity Manager

Filter Permission

Administrator Filter Permission
<input checked="" type="checkbox"/> Administrator Filter Permission
<input type="checkbox"/> Non-Administrator Filter Permission

Selected Items:

Filter Permission Administrator Filter Permission

General | Permitted Filter Attributes

Allowed Attributes
Select the attributes permitted in the filter definition.

Data Warehouse Mapping: HomeMdb, MsExchHomeServer

Allowed Membership References
Select a collection of groups or sets for which a filter may reference the members.

All Groups and Sets

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

File Edit View Favorites Tools Help

pocmiam\svc-miminstall | Site Actions ?

Microsoft Identity Manager

Schema Management - All Attributes

Employee Type

Name	Description
EmployeeType	

Search for: Employee Type Search within: Attributes Advanced Search

Employee Type

String pattern: ^(Internal|External)?\$

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.

Schema Management - All Bindings

EmployeeType

Company

Attribute Is Required:

Attribute Type: Company

Integer Maximum:

Integer Minimum:

Locatable:

Resource Type: User

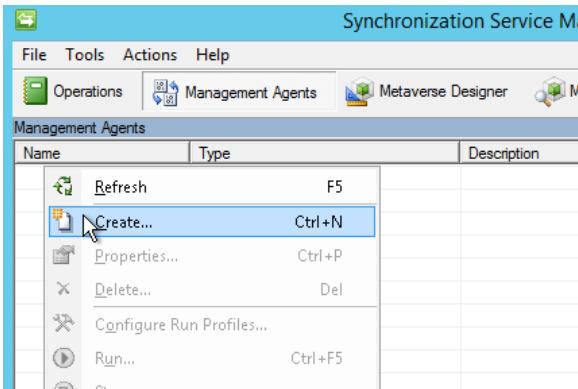
String Regular Expression: ^(ENTITY1|ENTITY2|ENTITY3)?\$

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

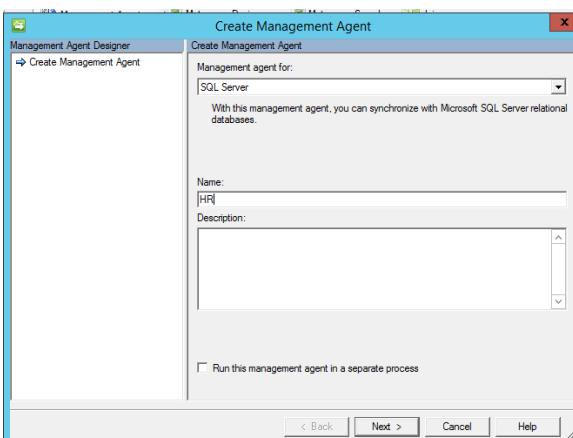
Go to advanced view and enter the following value in String regular Expression.

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

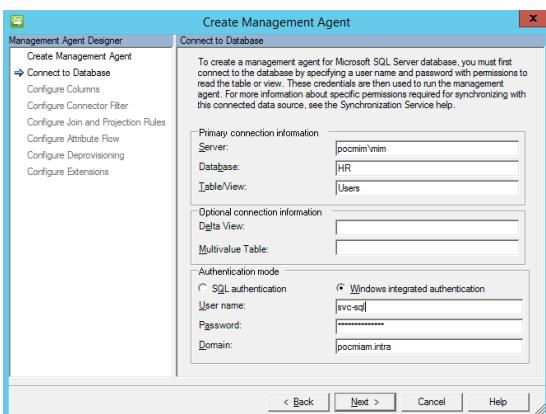
3.5 CREATE THE HR MANAGEMENT AGENT (SQL SERVER) IN MIM SYNCHRONIZATION SERVICE



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



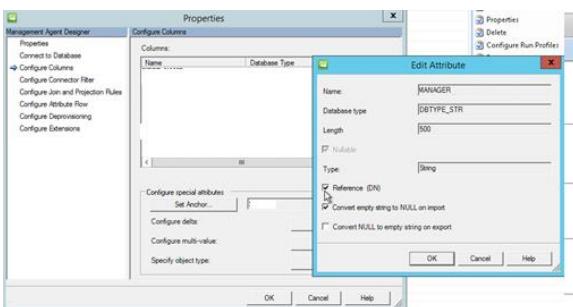
Create a SQL Server Management Agent named *HR*.



Enter the information to connect to the SQL Server database / table.

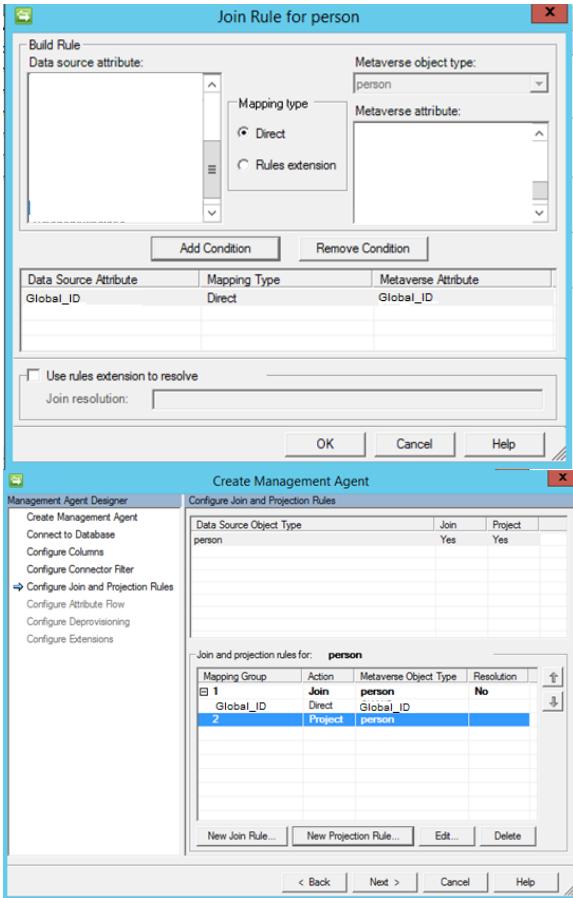
Click Next.

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.

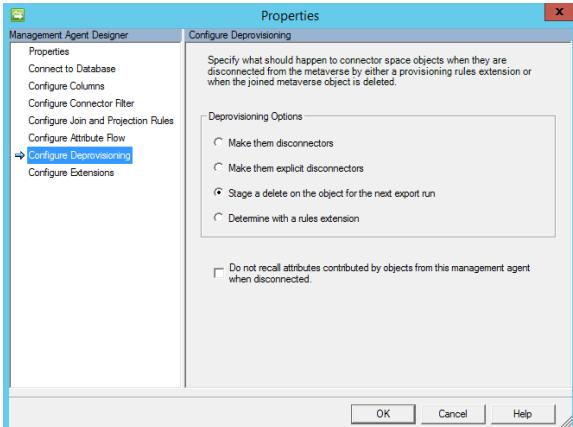


All user without a valid *Global_ID* will become disconnector.

Use the *Global_ID* as join rule.

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

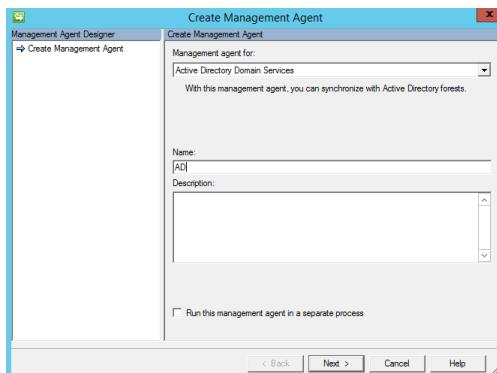
In the tab “Configure Attribute flow”, configure no attribute flow. We will use a MIM service synchronization rule to replicates HR data to the Metaverse.



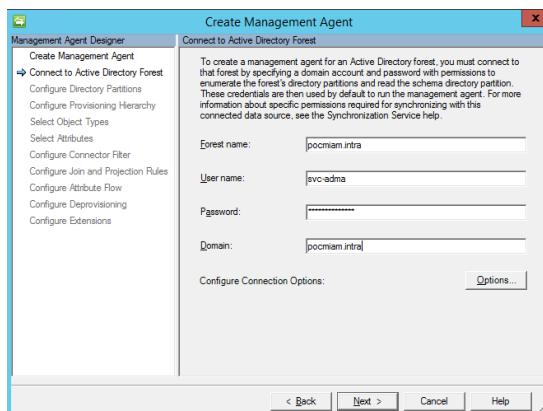
Select *Stage a delete on the object* for the next export run.

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

3.6 CREATE THE ACTIVE DIRECTORY MANAGEMENT AGENT

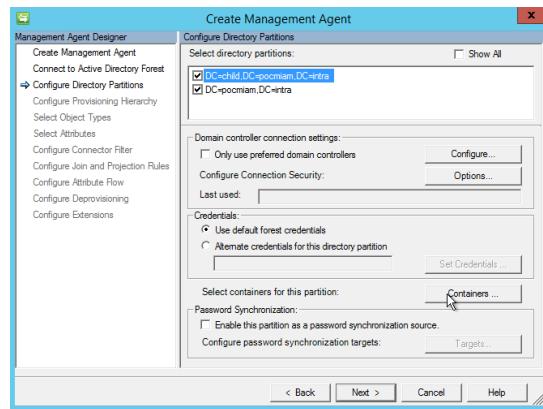


Create a new Active Directory Management Agent named **AD**.



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

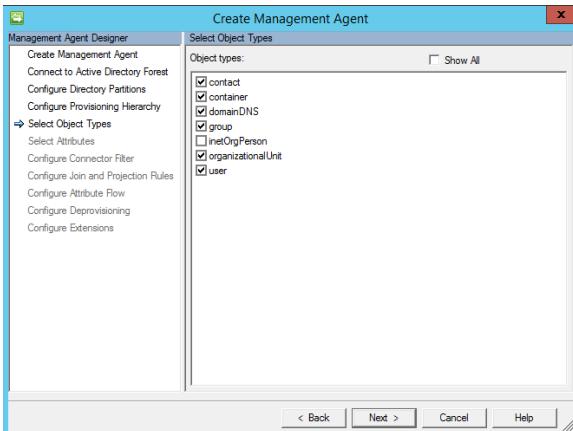
We have defined previously Active Directory permissions in the 2 domains for this service account.



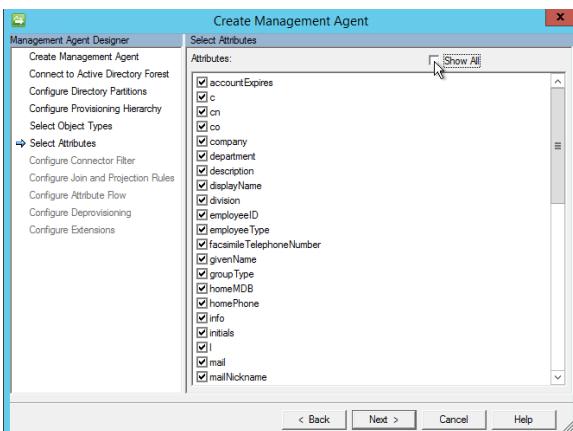
Click on **Containers** button.
Select only OU corresponding to each HR entities.

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.



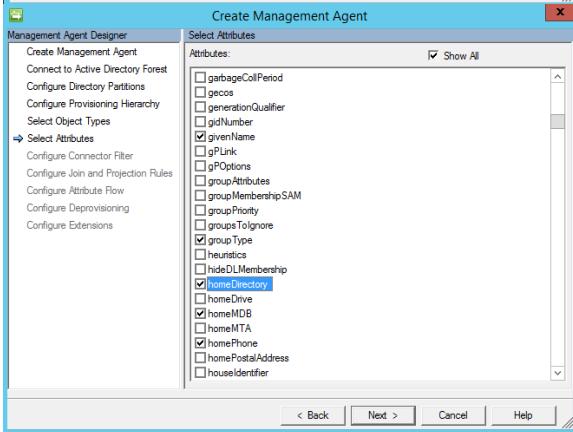
Keep existing object classes.
Select *contact*, *user* and *group* object.



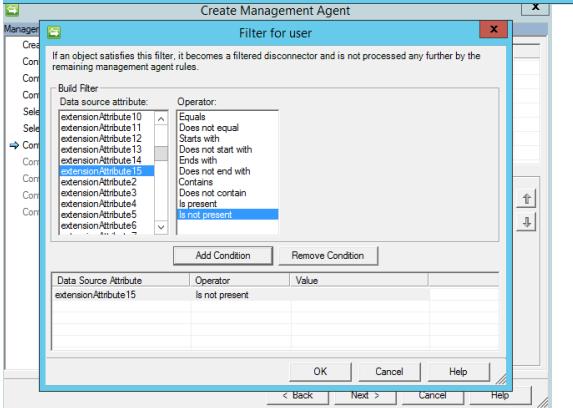
You must have prepare your schema for Exchange.

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

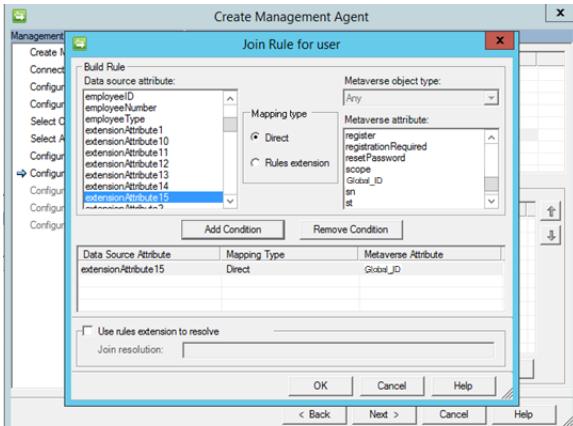
Select also all attributes used in this lab and add also attributes required for Exchange 2013 like
HomeMdb, *MsExchHomeServer*



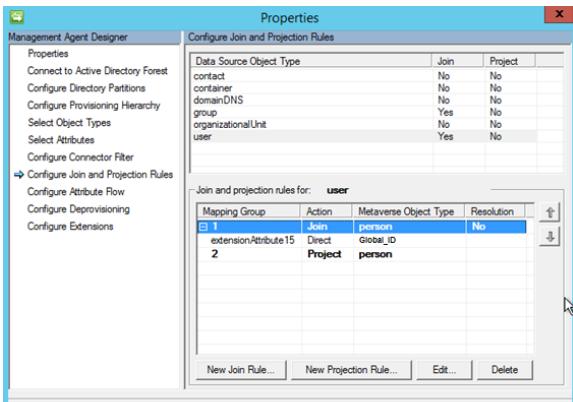
Add also attributes related to password and group management:
Unicodepwd
Pwdlastset
GroupType



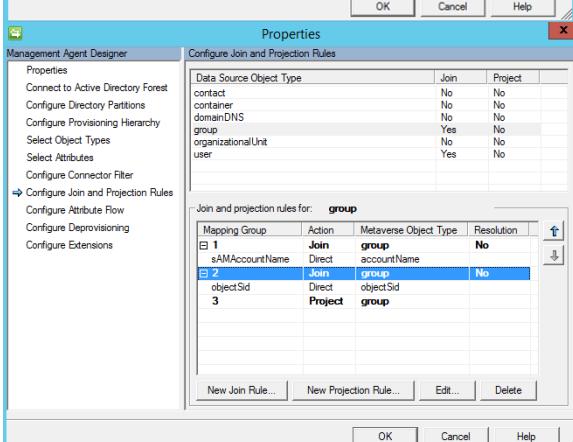
Configure as disconnector each user without *ExtensionAttribute15*. This attribute will store the Global_Id.



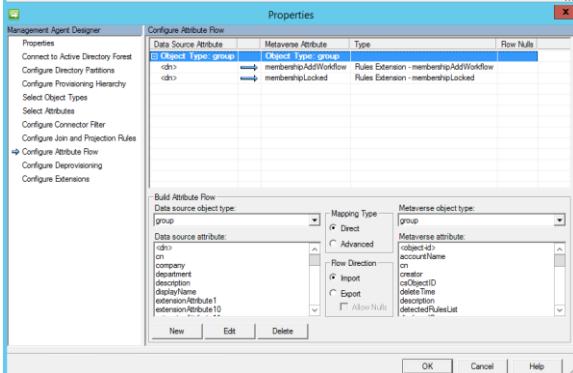
Configure ExtensionAttribute15 and Global_ID as join rule.



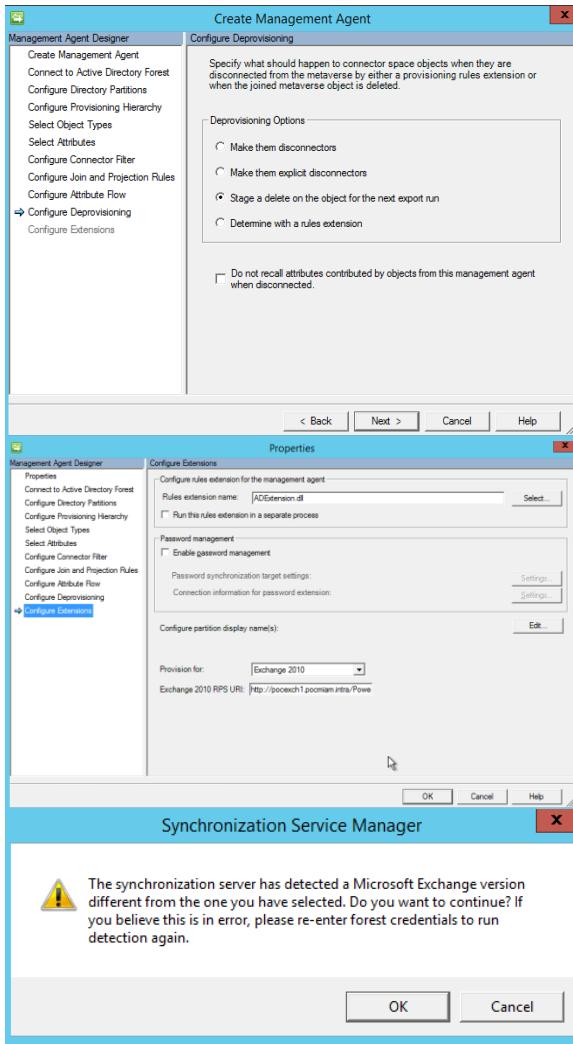
Configure user join and projection rules.



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.*

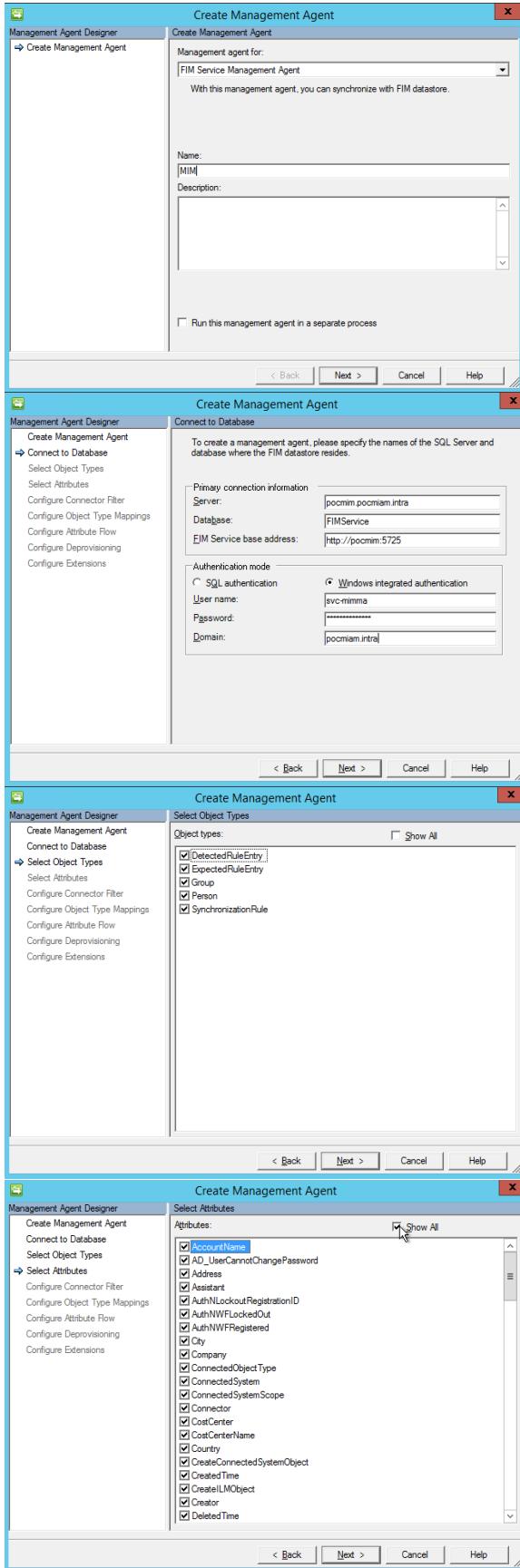
Select Provision for Exchange 2010 (based on your version).

<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.

Built-in Synchronization Account

Resource definitions.

Expiration Time

The date and time when the resource expires. The appropriate Management Policy Rule will delete the resource when the current date and time is later than the date and time specified in this attribute.

Format as M/d/yyyy h:mm tt

Locale

The region and language for which the representation of a resource has been adapted.

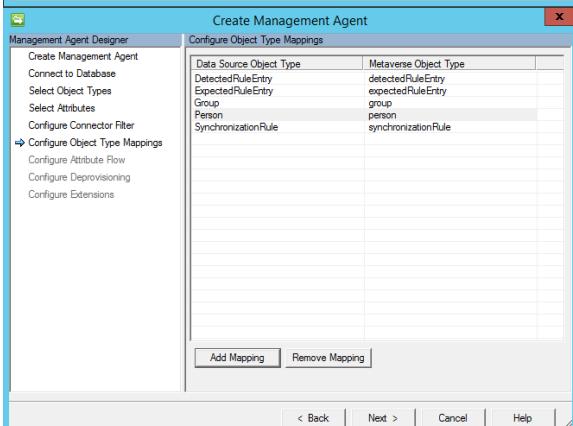
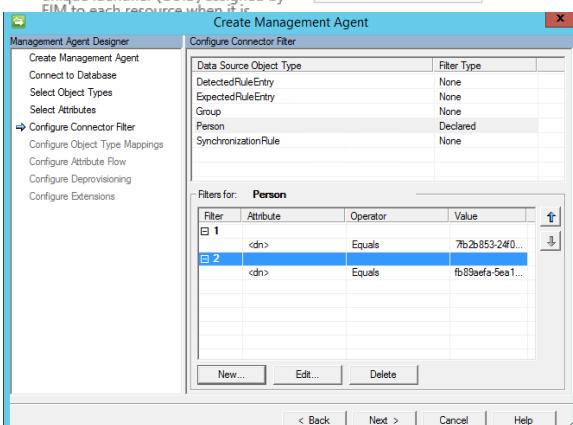
MV Resource ID

The GUID of an entry in the FIM metaverse corresponding to this resource.

fb89aefa-5ea1-47f1-8890-abe7797d6497

Resource ID

The value of the attribute is a globally unique identifier (GUID) assigned by FIM to each resource when it is



Data Source Attribute	Metaverse Attribute	Type	Flow Nulls
Object Type: Person	Object Type: person		
dn	sync-rule-m...		
MVObjectID	<object-id>	Direct	
DetectedRulesList	detectedRulesList	Direct	Allow
Global ID	Global_ID	Direct	
LastName	lastName	Direct	
FirstName	firstName	Direct	
MailNickname	mailNickname	Direct	
DisplayName	displayName	Direct	
EmployeeID	employeeID	Direct	
EmployeeType	employeeType	Direct	
AccountName	accountName	Direct	
Email	email	Direct	
Department	department	Direct	
Company	company	Direct	
JobTitle	jobTitle	Direct	
Manager	manager	Direct	
PostalCode	postalCode	Direct	
Address	postalAddress	Direct	
City	city	Direct	
Country	country	Direct	
MobilePhone	mobilePhone	Direct	
OfficePhone	officePhone	Direct	
Photo	photo	Direct	
EmployeeEndDate	employeeEndDate	Direct	
EmployeeStartDate	employeeStartDate	Direct	

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 *7b2b853-24f0-4498-9534-4e10589723c4*

DN equals to *fb89aefa-5ea1-47f1-8890-abe7797d6497*

Add *Group* and *Person* type mappings.

Configure the following attributes rules for *User* class.

Data Source Attribute	Metaverse Attribute	Type	Row Nulls
Object Type: ExpectedRuleEntry			
Object Type: group			
dn	sync-rule-m...		
MVObjectID	<object-id>	Direct	
DetectedRulesList	detectedRulesList	Direct	Allow
AccountName	accountName	Direct	Allow
DisplayName	displayName	Direct	
Domain	domain	Direct	
Email	email	Direct	Allow
MailNickname	mailNickname	Direct	
Member	member	Direct	Allow
Scope	scope	Direct	Allow
Owner	owner	Direct	
DisplayedOwner	displayedOwner	Direct	
Type	type	Direct	
MembershipAddWorkflow	membership.AddWorkflow	Direct	
MembershipLocked	membership.Locked	Direct	
Description	description	Direct	Allow
ObjectSID	objectSid	Direct	
<dn>	csObjectID	Direct	
ExpectedRulesList	expectedRulesList	Direct	
AccountName	accountName	Direct	
DisplayName	displayName	Direct	
Domain	domain	Direct	
Email	email	Direct	
MailNickname	mailNickname	Direct	
Member	member	Direct	

Configure the following attributes rules for Group class.

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

The screenshot shows the Management Agent Designer interface. On the left, a navigation pane lists various configuration tabs: Properties, Connect to Database, Select Object Types, Select Attributes, Configure Connector Filter, Configure Object Type Mappings, Configure Attribute Flow, Configure Deprovisioning, and Configure Extensions. The 'Configure Deprovisioning' tab is currently selected. The main panel displays two sections: 'Configure Deprovisioning' and 'Properties'. The 'Configure Deprovisioning' section contains a note about what happens to connector space objects when disconnected from the metaverse. It includes a 'Deprovisioning Options' section with four radio button choices: 'Make them disconnectors', 'Make them explicit disconnectors', 'Stage a delete on the object for the next export run' (which is selected), and 'Delete with a rules extension'. A checkbox at the bottom prevents recall of attributes. The 'Properties' section is partially visible below. The right side of the interface shows a large blue progress bar.

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*.

The screenshots show the 'Configure Run Profiles for "HR"' dialog box with the following configurations:

- Full Import:** Step 1: Full Import (Stage Only). Log file: default. Number of Objects: 0. Number of Deletions: 0. Partition: default.
- Export:** Step 1: Export. Log file: default. Number of Objects: 0. Number of Deletions: 0. Partition: default.
- Delta synchronization:** Step 1: Delta Synchronization. Log file: DC=pocmiam,DC=intra. Number of Objects: 0. Number of Deletions: 0. Partition: DC=pocmiam,DC=intra.
- FIFS:** Step 1: FIFS. Log file: default. Number of Objects: 0. Number of Deletions: 0. Partition: default.

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.

The screenshots show the 'Configure Run Profiles for "AD"' dialog box with the following configurations:

- Full Import:** Step 1: Full Import (Stage Only). Log file: default. Number of Objects: 0. Number of Deletions: 0. Partition: DC=pocmiam,DC=intra. Batch Size: 100. Page Size: 500. Timeout (seconds): 120.
- Export:** Step 1: Export. Log file: default. Number of Objects: 0. Number of Deletions: 0. Partition: DC=pocmiam,DC=intra. Batch Size: 100. Page Size: 500. Timeout (seconds): 120.
- Delta synchronization:** Step 1: Delta synchronization. Log file: DC=pocmiam,DC=intra. Number of Objects: 0. Number of Deletions: 0. Partition: DC=pocmiam,DC=intra.
- Delta Import:** Step 1: Delta Import. Log file: DC=pocmiam,DC=intra. Number of Objects: 0. Number of Deletions: 0. Partition: DC=pocmiam,DC=intra. Batch Size: 100. Page Size: 500. Timeout (seconds): 120.
- Full synchronization:** Step 1: Full synchronization. Log file: DC=pocmiam,DC=intra. Number of Objects: 0. Number of Deletions: 0. Partition: DC=pocmiam,DC=intra. Batch Size: 100. Page Size: 500. Timeout (seconds): 120.
- FIFS:** Step 1: FIFS. Log file: default. Number of Objects: 0. Number of Deletions: 0. Partition: default.

The image displays five windows of the 'Configure Run Profiles' dialog for Active Directory (AD) and Microsoft Identity Manager (MIM). Each window shows a list of management agent run profiles with their step details.

- Configure Run Profiles for "AD"** (Top Left):
 - FIFS**: Step 1 - **Delta Synchronization**
 - Step 1** details:

Name	Value
Log file	
Number of Objects	0
Number of Deletions	
Partition	DC=pocmiam,DC=intra
Batch Size	100
Page Size	500
Timeout (seconds)	120
- Configure Run Profiles for "AD"** (Top Right):
 - Step 1** details:

Name	Value
Log file	
Number of Objects	0
Number of Deletions	
Partition	DC=pocmiam,DC=intra
Batch Size	100
Page Size	500
Timeout (seconds)	120
- Configure Run Profiles for "AD"** (Bottom Left):
 - Step 1** details:

Name	Value
Log file	
Number of Objects	0
Number of Deletions	
Partition	DC=pocmiam,DC=intra
Batch Size	100
Page Size	500
Timeout (seconds)	120
- Configure Run Profiles for "AD"** (Bottom Right):
 - Step 1** details:

Name	Value
Log file	
Number of Objects	0
Number of Deletions	
Partition	DC=pocmiam,DC=intra
Batch Size	100
Page Size	500
Timeout (seconds)	120
- Configure Run Profiles for "MIM"** (Bottom Center):
 - Step 1** details:

Name	Value
Log file	
Number of Objects	0
Number of Deletions	
Partition	default
 - Step 2** details:

Name	Value
Log file	
Number of Objects	0
Number of Deletions	
Partition	default

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.

Create Synchronization Rule

General | Scope | Relationship | Inbound Attribute Flow | Summary

Display Name: **HR-IN**

Description:

Dependency: **<Please select an item>**

Data Flow Direction:

- Inbound: Import data into Microsoft Forefront Identity Manager.
- Outbound: Export data to external system.
- Inbound and Outbound: Export and import data to and from an external system.

Apply Rule:

Determines how the synchronization rule is applied to resources of the type specified.

- To specific metaverse resources of this type based on Outbound Synchronization Policy. Outbound Synchronization Policy consists of MPR, set, and workflow.
- To all metaverse resources of this type according to Outbound System Scoping Filter. Outbound System Scoping Filter is defined in the Scope tab.

* Requires input

Synchronization Rule HR-IN

General | Scope | Relationship | Inbound Attribute Flow

Metaverse Resource Type: **Person**

The resource type in the FIM Metaverse that this Synchronization Rule applies to.

External System: **HR**

The external system this Synchronization Rule will operate on.

External System Resource Type: **Person**

The resource type in the external system that this Synchronization Rule applies to.

Outbound System Scoping Filter

Synchronization Rule HR-IN

Add Condition | Delete Condition

MetaverseObject person Attribute	Operator	Value
<Please select an item>	<Please select an item>	

1 items total | Page | 1 of 1 | < > >>

Inbound System Scoping Filter

Add Condition | Delete Condition

person Attribute	Operator	Value
starts with		

1 items total | Page | 1 of 1 | < > >>

* Requires input

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

The screenshot shows the 'Create Synchronization Rule' dialog box. At the top, there are tabs for General, Scope, Relationship, Inbound Attribute Flow, and Summary. The Relationship Criteria tab is active, displaying a condition where 'MetaverseObjectperson/Attr/attribute' is connected to 'ConnectedSystemObjectperson/Attribute'. Below this, there are sections for Create Resource in FIM (with a checked checkbox), Create Resource in External System (unchecked), Enable Deprovisioning (unchecked), and a note about disconnecting from external systems.

The Inbound Attribute Flow tab is also visible, showing a list of mappings between external system attributes and FIM attributes, such as DEPARTMENT=>department, DIVISION=>company, etc. It includes detailed views of flow definitions for Employee End Date and Employee Start Date, which involve concatenating values and using DateTimeFormat functions to convert strings to dates.

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*.

Display Name: HR-OUT

Description:

Dependency: Outbound

Data Flow Direction: Export data to external system.

Apply Rule: To specific metaverse resources of this type based on Outbound Synchronization Policy.

Metaverse Resource Type: person

External System: HR

Outbound System Scoping Filter:

Add Condition	Delete Condition	
MetaverseObject[person/Attribute]	Operator	Value
<input type="checkbox"/> [Reference object is selected]	<input type="checkbox"/> [Reference object is empty]	

Relationship Criteria:

<input type="checkbox"/> MetaverseObject[person/Attribute]	=	ConnectedSystemObject[person/Attribute]
<input type="checkbox"/> Global_ID	=	Global_ID

Create Resource In FIM: If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created. Create resource in FIM

Create Resource In External System: If no resource in the External System satisfies the Relationship Criteria, a new resource will be created. Create resource in external system

Enable Deprovisioning: Disconnect FIM resource from external system resource when this Synchronization Rule is removed.

Workflow Parameters:

<input type="checkbox"/> Name	<input type="button" value="Data type"/>
-------------------------------	--

Outbound Attribute Flow:

Initial Flow Only	Use as Existence Test	Flow (FIM Value => Destination Attribute)
<input type="checkbox"/>	<input type="checkbox"/>	mobile=>Mobile
<input type="checkbox"/>	<input type="checkbox"/>	telephoneNumber=>TelephoneNumber
<input type="checkbox"/>	<input type="checkbox"/>	EmployeeTypeMim=>EDW_EMPLOYEE_TYPE

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

Create Synchronization Rule

General Scope Relationship Workflow Parameters Outbound Attribute Flow Summary More information

Display Name: AD-USER-OUT

Description:

Dependency: A Synchronization Rule that must be applied to a resource before this Synchronization Rule can be applied.

Data Flow Direction: Data Flow Direction indicates the direction of attribute flow for this Synchronization Rule.

Apply Rule: Determines how the synchronization rule is applied to resources of the type specified.

* Requires input.

Next > Finish Cancel

Create Synchronization Rule

General Scope Relationship Workflow Parameters Outbound Attribute Flow Summary

Metaverse Resource Type: person

External System: AD

External System Resource Type: user

Outbound System Scoping Filter

Add Condition Delete Condition

MetaverseObject<person>(Attribute) Operator Value

Inbound System Scoping Filter

Add Condition Delete Condition

user(Attribute) Operator Value

Properties

Management Agent Designer Configure Connector Filter

Data Source Object Type: user (Declared)

Filters for: user

Filter	Attribute	Operator	Value
1	extension/Attribute15	Does not start with	S

Synchronization Rule AD-USER-OUT

General Scope Relationship Workflow Parameters Outbound Attribute Flow

Workflow Parameters

New Delete

Name: <Please select an item>

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.

Create Synchronization Rule

Relationship Criteria

Add Condition Delete Condition

MetaverseObjectperson(Attribute) = ConnectedSystemObjectuser(Attribute)

Global_ID = extensionAttribute15

Create Resource In FIM
If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created.

Create resource in FIM

Create Resource in External System
If no resource in the external system satisfies the Relationship Criteria, a new resource will be created.

Create resource in external system

Enable Deprovisioning
This option applies when this Synchronization Rule is removed.

Disconnect FIM resource from external system resource when this Synchronization Rule is removed.

1 items total Page 1 of 1 < > << >>

< Back Next > Finish Cancel

Outbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Initial Flow Only	Use as Existence Test	Flow (FIM Value => Destination Attribute)
<input type="checkbox"/>	<input type="checkbox"/>	Global_ID => extensionAttribute15
<input type="checkbox"/>	<input type="checkbox"/>	firstName=>givenName
<input type="checkbox"/>	<input type="checkbox"/>	lastName=>s
<input type="checkbox"/>	<input type="checkbox"/>	accountName=@miam.msreport.fr=>userPrincipalName
<input type="checkbox"/>	<input type="checkbox"/>	postalAddress=>streetAddress
<input type="checkbox"/>	<input type="checkbox"/>	postalCode=>postCode
<input type="checkbox"/>	<input type="checkbox"/>	accountName=>sAMAccountName
<input type="checkbox"/>	<input type="checkbox"/>	displayName=>displayName
<input type="checkbox"/>	<input type="checkbox"/>	employeeType=>employeeType
<input type="checkbox"/>	<input type="checkbox"/>	accountName=>mailNickname
<input type="checkbox"/>	<input type="checkbox"/>	Flow (FIM Value => Destination Attribute)
<input type="checkbox"/>	<input type="checkbox"/>	employeeID=extensionAttribute1
<input type="checkbox"/>	<input type="checkbox"/>	"CN="=>accountName,"OU=Users,OU="=>company,"DC=pocmiam,DC=intra"=>dn
<input type="checkbox"/>	<input type="checkbox"/>	city=>l
<input type="checkbox"/>	<input type="checkbox"/>	company=>company
<input type="checkbox"/>	<input type="checkbox"/>	department=>department
<input type="checkbox"/>	<input type="checkbox"/>	jobTitle=>title
<input type="checkbox"/>	<input type="checkbox"/>	manager=>manager
<input type="checkbox"/>	<input type="checkbox"/>	mobilePhone=>mobile
<input type="checkbox"/>	<input type="checkbox"/>	officePhone=>phoneNumber
<input type="checkbox"/>	<input type="checkbox"/>	Type =>extensionAttribute10
<input type="checkbox"/>	<input type="checkbox"/>	Flow (FIM Value => Destination Attribute)
<input type="checkbox"/>	<input type="checkbox"/>	CustomExpression("=>HomeMdb)=homeMDB
<input type="checkbox"/>	<input type="checkbox"/>	MsExchHomeServer=>msExchHomeServerName
<input type="checkbox"/>	<input type="checkbox"/>	CustomExpression(IIF(Eq(country,"United States"),840,IIF(Eq(country,"United Kingdom"),826,250)))=>...
<input type="checkbox"/>	<input type="checkbox"/>	country=>co
<input type="checkbox"/>	<input type="checkbox"/>	CustomExpression(IIF(Eq(country,"United States"),840,IIF(Eq(country,"United Kingdom"),826,250)))=>cou...
<input checked="" type="checkbox"/>	<input type="checkbox"/>	512=>userAccountControl
<input checked="" type="checkbox"/>	<input type="checkbox"/>	"CN="=>accountName,"OU=Users,OU="=>company,"DC=pocmiam,DC=intra"=>dn
<input checked="" type="checkbox"/>	<input type="checkbox"/>	accountName=>sAMAccountName
<input checked="" type="checkbox"/>	<input type="checkbox"/>	accountName=>mailNickname
<input checked="" type="checkbox"/>	<input type="checkbox"/>	accountName=@miam.msreport.fr=>userPrincipalName

Outbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Initial Flow Only	Use as Existence Test	Flow (FIM Value => Destination Attribute)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CustomExpression("=>HomeMdb)=homeMDB
<input checked="" type="checkbox"/>	<input type="checkbox"/>	MsExchHomeServer=>msExchHomeServerName
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Your password =>unicodePwd
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Global_Id =>extensionAttribute15

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

Create Synchronization Rule

General Scope Relationship Inbound Attribute Flow Summary More information

Display Name: AD-USERS-IN

Description:

Dependency: A Synchronization Rule that must be applied to a resource before this Synchronization Rule can be applied.

Data Flow Direction: Inbound Import data into Microsoft Forefront Identity Manager.

Data Flow Direction indicates the direction of attribute flow for this Synchronization Rule.

Apply Rule: Determines how the synchronization rule is applied to resources of the type specified.

To specific metaverse resources of this type based on Outbound Synchronization Policy. Outbound Synchronization Policy consists of MPR set, and workflow.

To all metaverse resources of this type according to Outbound System Scoping Filter. Outbound System Scoping Filter is defined in the Scope tab.

* Requires Input

< Back Next > Finish Cancel

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

Create Synchronization Rule

General Scope Relationship Inbound Attribute Flow Summary More information

Metaverse Resource Type: person

The resource type in the FIM Metaverse that this Synchronization Rule applies to.

External System: AD

The external system this Synchronization Rule will operate on.

External System Resource Type: user

The resource type in the external system that this Synchronization Rule applies to.

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

Outbound System Scoping Filter

Add Condition Delete Condition

MetaverseObject<person>(Attribute)	Operator	Value
<Please select an item>	<Please select an item>	

Outbound System Scoping Filter

Add Condition Delete Condition

MetaverseObject<person>(Attribute)	Operator	Value
<Please select an item>	<Please select an item>	

Inbound System Scoping Filter

Add Condition Delete Condition

user(Attribute)	Operator	Value
<Please select an item>	<Please select an item>	

Properties

Management Agent Designer

- Properties
- Connect to Active Directory Forest
- Configure Directory Partitions
- Configure Provisioning Hierarchy
- Select Object Type
- Select Attribute
- Configure Connector Filter
- Configure Join and Projection Rules
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

Configure Connector Filter

Data Source Object Type	Filter Type
contact	None
container	None
domainDNS	None
group	None
organizationalUnit	None
User	Declared

Filters for: user

Filter	Attribute	Operator	Value
1	extensionAttribute15	Exist	

Create Synchronization Rule

Schedule | Google | Recurring | Inbound Attribute Flow | Summary More information

Relationship Criteria

Add Condition Delete Condition

MetaverseObject<person>(Attribute)	ConnectorSystem<User>(Attribute)
<Please select an item>	<Please select an item>

Create Resource to FIM

If no resource in the FIM Metaverse satisfies the criteria:

- Create resource in FIM

Create Resource in External System

If no resource in the external system satisfies the Relationship Criteria, a new resource will be created:

- Create resource in external system

Enable Deprovisioning

This option is available when this Synchronization Rule is removed from a resource in FIM.

- Disconnect FIM resource from external system resource when this Synchronization Rule is removed.

< Back Next > Finish Cancel

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.

Order	Management Agent	Object Type	Source Attribute(s)	Mapping Type
1	HR	person	FIRST_NAME	SR-Direct
2	MIM	Person	FirstName	Direct
3	AD	user	givenName	SR-Direct

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 has not been 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 other target systems 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

Synchronization Rule AD Distribution Group Sync Rule

General Scope Relationship Workflow Parameters Outbound Attribute Flow Inbound Attribute Flow More info

Display Name: AD Distribution Group Sync Rule
 This is the name used to identify this Synchronization Rule.

Description: Synchronizes Distribution Groups with Active Directory bi-directionally

Dependency: Dependency is a Synchronization Rule. It must be applied before this Synchronization Rule can be applied.

Data Flow Direction: Inbound Import data into Microsoft Forefront Identity Manager. Outbound Export data to external system. Inbound and Outbound Export and Import data to and from an external system.

Apply Rule: To specific metaverse resources of this type based on Outbound Synchronization Policy. Outbound Synchronization Policy consists of MPR, set, and workflow. To all metaverse resources of this type according to Outbound System Scoping Filter. Outbound System Scoping Filter is defined in the Scope tab.

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

Synchronization Rule AD Distribution Group Sync Rule

General Scope Relationship Workflow Parameters Outbound Attribute Flow Inbound Attribute Flow More info

Metaverse Resource Type: group

The resource type in the FIM Metaverse that this Synchronization Rule applies to.

External System: AD

The external system this Synchronization Rule will operate on.

External System Resource Type: group

The resource type in the external system that this Synchronization Rule applies to.

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

Outbound System Scoping Filter

Add Condition Delete Condition

MetaverseObject<group>(Attribute)	Operator	Value
<Please select an item>	<Please select an item>	

Inbound System Scoping Filter

Add Condition Delete Condition

MetaverseObject<group>(Attribute)	Operator	Value
<Please select an item>	<Please select an item>	

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

Synchronization Rule AD Distribution Group Sync Rule

General | Scope | Relationship | Workflow Parameters | Outbound Attribute Flow | Inbound Attribute Flow | More information

Relationship Criteria

Add Condition Delete Condition

MetaverseObject/group/Attribute = ConnectedSystemObject/group/Attribute

objectSid = objectSid

1 items total Page 1 of 1 < < > >

Create Resource in FIM
If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created.

Create resource in FIM

Create Resource in External System
If no resource in the External system satisfies the Relationship Criteria, a new resource will be created.

Create resource in external system

Enable Deprovisioning
This option applies when this Synchronization Rule is removed from an external system.

Disconnect FIM resource from external system resource when this Synchronization Rule is removed.

Synchronization Rule AD Distribution

General | Scope | Relationship | Workflow Parameters | Outbound

Workflow Parameters

New Delete

Name

Synchronization Rule AD Distribution Group Sync Rule

General | Scope | Relationship | Workflow Parameters | Outbound Attribute Flow | Inbound Attribute Flow | More information

Outbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Initial Flow Only Use as Existence Test

Flow (FIM Value => Destination Attribute)

displayedOwner=managedBy

displayName=displayName

member=member

mailNickname=mailNickname

CustomExpression(IIF(Eq(scope,"Global"),2,IIF(Eq(scope,"Universal"),8,IIF(Eq(scope,"DomainLocal"),4,...

CustomExpression("CN=" + displayName + ",OU=Groups,OU=MIM,DC=pocmiam,DC=intra") + dn

displayName=sAMAccountName

CustomExpression(IIF(Eq(scope,"Global"),2,IIF(Eq(scope,"Universal"),8,IIF(Eq(scope,"DomainLocal"),4,...

mailNickname=mailNickname

CustomExpression("CN=" + displayName + ",OU=Groups,OU=MIM,DC=pocmiam,DC=intra") + dn

Flow Definition

Source Destination

Concatenate Value Delete

CustomExpression

IIF(Eq(scope,"Global"),2,IIF(Eq(scope,"Universal"),8,IIF(Eq(scope,"DomainLocal"),4,"")))

Flow Definition

Source Destination

Destination * groupType

The attribute to flow values to.

Allow Null Allow null value to flow to destination.

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,"")))

Create Distribution Group

General Members Owners Summary

Display Name

E-mail Alias

Member Selection

- Manual
Members are manually managed
- Manager-based
Membership is calculated to include a manager, and all people report to them
- Criteria-based
Membership is calculated based on one or more attributes of the members

Description

Outbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Initial Flow Only Use as Existence Test Flow (FIM Value => Destination Attribute)

displayName=>sAMAccountName

Synchronization Rule AD Distribution Group Sync Rule

General Scope Relationship Workflow Parameters Outbound Attribute Flow Inbound Attribute Flow

Inbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Flow (External System Attributes/Values => FIM Attribute)

- CustomExpression(Word(Word(EscapeDNComponent(dn),5,"="),1,"\"))=>domain
- CustomExpression(IIF(Eq(groupType,2),"Global",IIF(Eq(groupType,8),"Universal",IIF(Eq(groupType,4),"D... mail=>email
- managedBy=>displayedOwner
- managedBy=>owner
- member=>member
- "Distribution"=>type
- objectSid=>objectSid
- CustomExpression(IIF(IsPresent(displayName),displayName,sAMAccountName))=>displayName
- CustomExpression(IIF(IsPresent(mailNickname),mailNickname,sAMAccountName))=>mailNickname

Inbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Flow (External System Attributes/Values => FIM Attribute)

- sAMAccountName=>accountName

Inbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Flow (External System Attributes/Values => FIM Attribute)

- sAMAccountName=>accountName

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 used 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 in 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 used 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/heyscriptinggu/y/2004/12/21/how-can-i-tell-whether-a-group-is-a-security-group-or-a-distribution-group/>

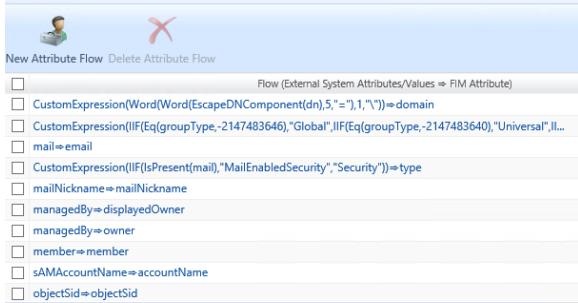
Select *ObjectSID* as relationship criteria.

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"

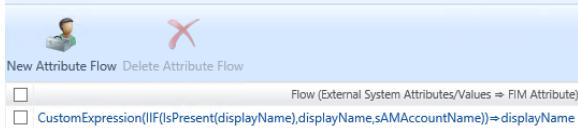
Inbound Attribute Flow



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, sAMAccoun tName)

Inbound Attribute Flow



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.

Sets

New Details Delete

- _All AD Distribution-Groups
- _All AD security groups
- _All HR external users
- _All HR internal users
- _All HR users
- _All terminated users (30 days)
- _All terminated users (365 days)
- _All_AD_Users
- _All_Standard_HR_Users
- _All-Cadre-Dirigeant

All HR external users

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match all of the following conditions:

- Employee Type is External
- Add Statement or Add Sub-condition

All HR users

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match all of the following conditions:

- Global_ID exists
- Add Statement or Add Sub-condition

All HR internal users

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match all of the following conditions:

- Employee Type is Internal
- Add Statement or Add Sub-condition

View Members		
Display Name		
Adalberto ORTIZ		
Adalberto SEXTON		
Adrian SARGEN -External		
Ahmad OSBORNE		
Alan PACHECO		
Alberto VALDEZ		
Andreas CRAIG		
Andres CHANG -External		
Angelo EVERETT		
Asa BARRON		

View Members		
Display Name		
Adalberto ORTIZ		
Adalberto SEXTON		
Ahmad OSBORNE		
Alan PACHECO		
Alberto VALDEZ		
Andreas CRAIG		
Angelo EVERETT		
Asa BARRON		
Basil ALVAREZ		
Benjamin WALTERS		

All terminated users (30 days)

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match **all** of the following conditions:

Employee End Date prior to 30 days ago

Employee End Date after 364 days ago

Add Statement or Add Sub-condition

All terminated users (365 days)

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match **all** of the following conditions:

Employee End Date prior to 365 days ago

Add Statement or Add Sub-condition

View Members

Display Name	Resource
Benjamin WILCOX -External	User
Blaine COBB	User
Cole SKINNER -External	User
Guillaume Bertrando	User
Kris WALKER	User
Lamar HOLMAN -External	User
Logan CHAVEZ -External	User
Wallace GUZMAN	User

All-Cadre-Dirigeant

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match **all** of the following conditions:

Type is Cadre dirigeant

Add Statement or Add Sub-condition

View Members

Display Name	Resource
Bernard BLACKWELL -External	User
Judson HERMAN -External	User
Kraig FOREMAN -External	User

All_Standard_HR_Users

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Select user that match **all** of the following conditions:

Type is not Cadre dirigeant

Add Statement or Add Sub-condition

View Members

Display Name	Resource
Adalberto ORTIZ	User
Adrian SARGEN -External	User
Ahmad OSBORNE	User
Alan PACHECO	User
Andreas CRAIG	User
Angelo EVERETT	User
Asa BARRON	User
Basil ALVAREZ	User
Benjamin WALTERS	User
Bernard COLLINO	User

View Members

Display Name	Resource
Adalberto SEXTON	User
Alberto VALDEZ	User
Andres CHANG -External	User
Benjamin WILCOX -External	User
Bernard BLACKWELL -External	User
Bernie ROBERTS -External	User
Bill WASHINGTON -External	User

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"
```

All AD Distribution-Groups

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Sorry, the filter you are trying to display cannot be rendered with the Forefront corrupted or unsupported by the Filter Builder.

[View Members](#)

Display Name	Type
BRS-AmericasArea-DIST	Group
DIST-GROUP1	Group
DIST-GROUP2	Group
DIST-GROUP3	Group
DIST-GROUP4	Group
DIST-GROUP7	Group
OSS-AMECAA-DIST	Group
OSS-China-DIST	Group
OSS-Continental-DIST	Group
OSS-France-Dist	Group

All AD security groups

General Criteria-based Members Manually-managed Members

Enable criteria-based membership in current set

Sorry, the filter you are trying to display cannot be rendered with the Forefront corrupted or unsupported by the Filter Builder.

[View Members](#)

Display Name	Type
BRS-AmericasArea-SEC	Group
External-Users	Group
Internal-Users	Group
OSS-AMECAA-SEC	Group
OSS-China-SEC	Group
OSS-NorthAmerica-SEC	Group
SER-GROUP1	Group
SER-GROUP2	Group
SER-GROUP3	Group
SER-GROUP4	Group

`xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`

`Dialect="http://schemas.microsoft.com/2006/11/XPatFilterDialect"`

`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/XPatFilterDialect"`

`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 Name: AD-OUT-USERS

Workflow Type: Action

Run On Policy Update: Run on Policy Update

Synchronization Rule Activity:

- This activity manages the application of Synchronization Rules to FIM objects.
- WAL: Add Delay
- 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 resources.

Select

Workflow type: *action*

Select *Synchronization Rule Activity*.

Import Workflow: Import pre-existing Workflow Definition from a XOML file

Add the target resource to Synchronization Rule: AD-USER-OUT

Action Selection:

- Add
- Remove
- Based on Attribute Value

Save Cancel

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.

Import Workflow: Import pre-existing Workflow Definition from a XOML file

Add Activity:

Click on *Finish*.

3.11.2 Create the workflow HR-OUT

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

Workflow Type: Action

Run On Policy Update:

Import Workflow: Import pre-existing Workflow Definition from a XOML file

Select HR-OUT and Add.

Click on Finish.

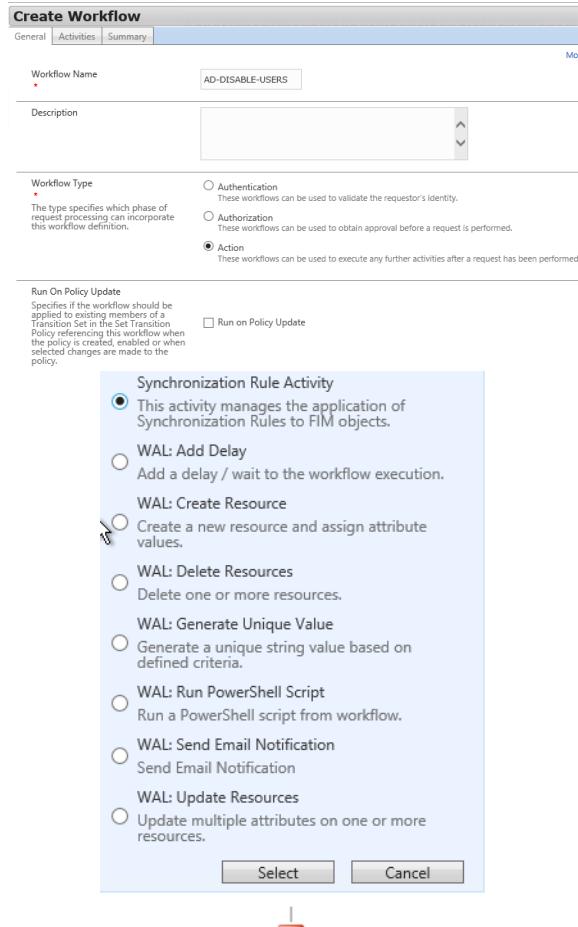
Workflow type: *action*

Select *HR-OUT* and *Add*.

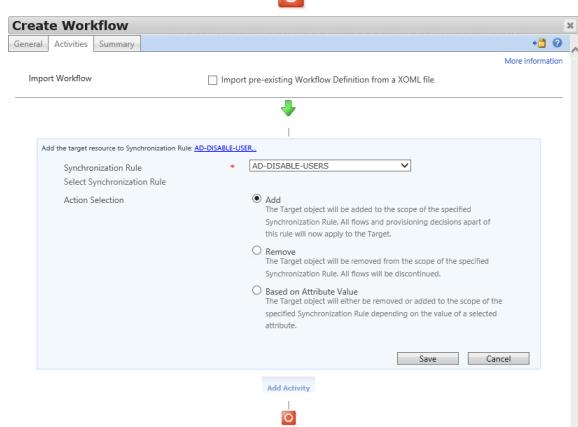
This workflow will allow to generate ERE (*Expected Rule Entry*) for user objects to synchronize mobile phone, office phone and employee type values to HR database.

3.11.3 Create the workflow AD-DISABLE-USERS

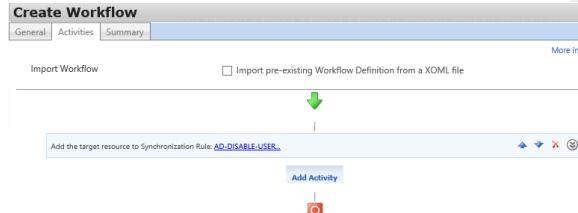
This workflow will allow to start the synchronization rule **AD-DISABLE-USERS** which will disable an Active Directory user account and move it in the OU **Disabled_Users**.



Workflow type: action



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



Click on *Finish*.

3.11.4 Create and configure the Workflow _AD-REMOVE-USERS

_AD-REMOVE-USERS

General Activities

Workflow Name: **_AD-REMOVE-USERS**

Description:

Workflow Type: Action

Run On Policy Update: Run on Policy Update

_AD-REMOVE-USERS

General Activities

Replace Workflow: Replace existing Workflow Definition with a new XOML file

Action Selection:

- Remove the target resource from Synchronization Rule: **AD-DISABLE-USERS**
- Add: The Target object will be added to the scope of the specified Synchronization Rule. All flows and provisioning decisions apart of this rule will now apply to the Target.
- Remove: The Target object will be removed from the scope of the specified Synchronization Rule. All flows will be discontinued.
- Based on Attribute Value: The Target object will either be removed or added to the scope of the specified Synchronization Rule depending on the value of a selected attribute.

Remove the target resource from Synchronization Rule: **AD-USER-OUT**

Remove the target resource from Synchronization Rule: **HS-OUT**

Add Activity

Synchronization Rule AD-USER-OUT

General Scope Relationship Workflow Parameters Outbound Attribute Flow More information

Relationship Criteria

Add Condition Delete Condition

MetaverseObject<person>/Attribute = ConnectedSystemObject<user>/Attribute

Global ID = extensionAttribute15

Create Resource in FIM: If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created. Create resource in FIM.

Create Resource in External System: If no resource in the External system satisfies the Relationship Criteria, a new resource will be created. Create resource in external system.

Enable Deprovisioning: This option applies when this Synchronization Rule is removed from an resource in FIM. Disconnect FIM resource from external system resource when this Synchronization Rule is removed.

Properties

Management Agent Designer

Properties

Configure Deprovisioning

Specify what should happen to connector space objects when they are disconnected from the metaverse by either a provisioning rules extension or when the joined metaverse object is deleted.

Deprovisioning Options

- Make them disconnectors
- Make them explicit disconnectors
- Stage a delete on the object for the next export run
- Determine with a rules extension

Do not recall attributes contributed by objects from this management agent when disconnected.

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

When ERE is removed, the object is mark as disconnect in the AD management Agent.

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.

The screenshot shows two windows from a management interface:

- AD-REMOVE-USERS Workflow:** A workflow titled "AD-REMOVE-USERS" with three sequential activities: "Remove the target resource from Synchronization Rule AD-DISABLE-USER", "Remove the target resource from Synchronization Rule AD-USER-OUT", and "Remove the target resource from Synchronization Rule HR-OUT".
- Synchronization Rule HR-OUT Configuration:** A window titled "Synchronization Rule HR-OUT" showing the "Relationship Criteria" tab. It displays a condition: "MetaverseObject/person/Attribute" equals "ConnectedSystemObject/person/Attribute" with the value "Global_ID".

Below these windows, there is a list of configuration options:

- Create Resource In FIM:** If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created.
- Create Resource in External System:** If no resource in the External system satisfies the Relationship Criteria, a new resource will be created.
- Enable Deprovisioning:** This option applies when this Synchronization Rule is removed from an resource in FIM.

The "Properties" section of the Management Agent Designer shows the "Configure Deprovisioning" tab selected. It includes settings for what happens to connector space objects when disconnected, with the "Stage a delete on the object for the next export run" option selected. There is also a checkbox for "Do not recall attributes contributed by objects from this management agent when disconnected".

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.

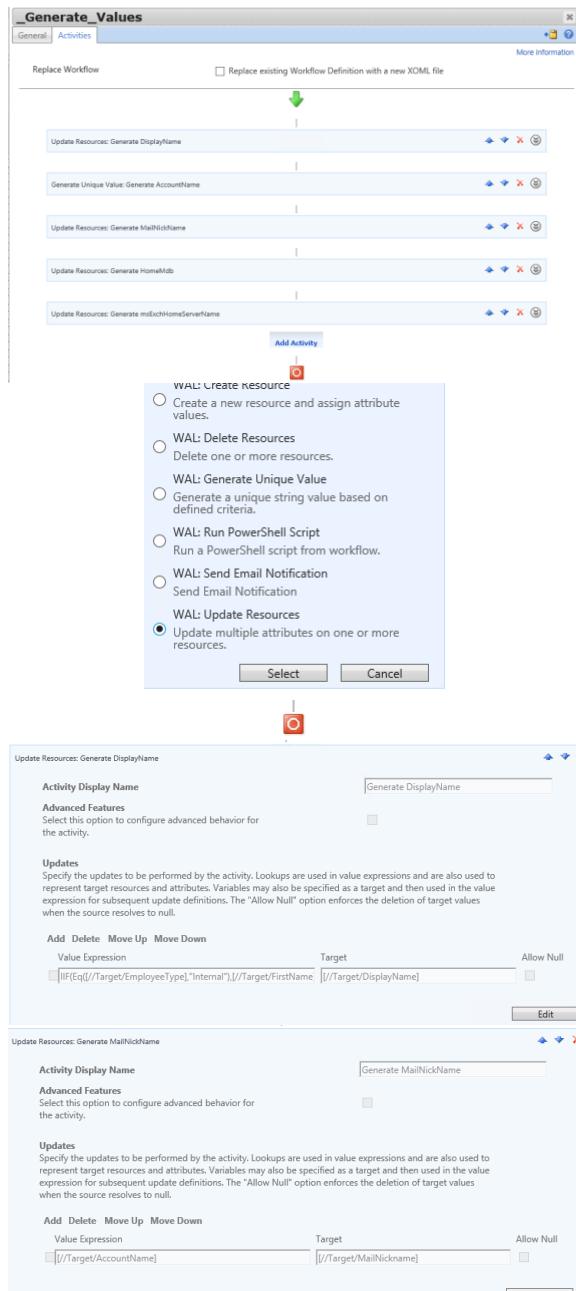
3.11.5 Generate attributes from MIM portal

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:

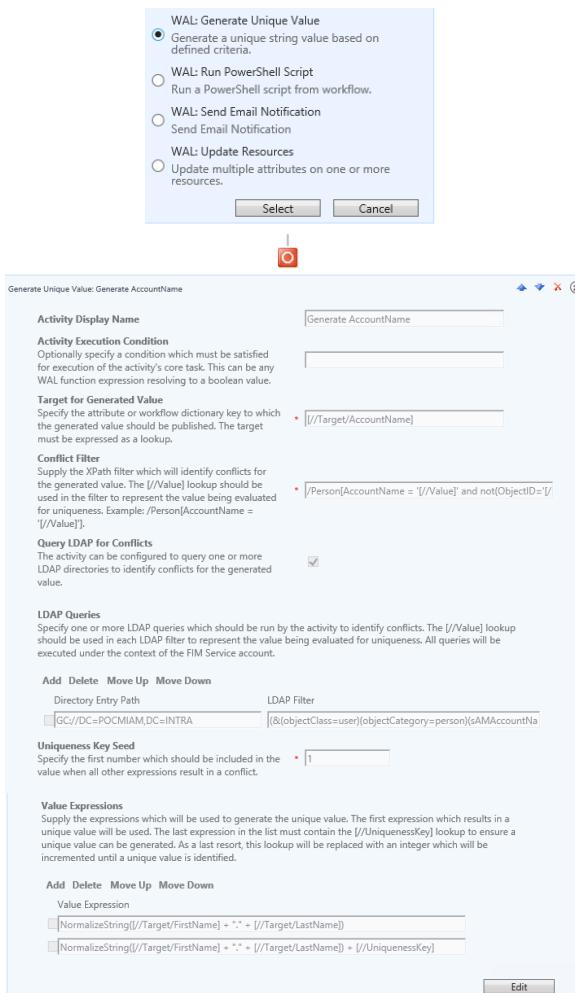
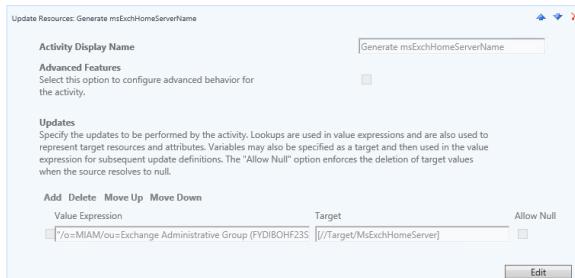
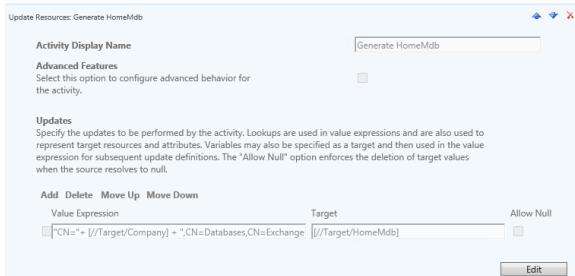
Value expression:

```
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=pocmia
m,DC=intra"
```

To generate value for the attribute
MsExchHomeServer

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

Notes:

In MIM service the attribute has been created with the name **msExchHomeServer**.

In Active Directory, the name of this attribute is **msExchHomeServerName**.

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)(sAMAc
countName=[/Value])(!(Extensionattribute15=[/Tar
get/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

The screenshot shows the configuration for a workflow named "Ask for Approval from Manager". Key settings include:

- Approvers:** /Target/Manager
- Approval Threshold:** 1 Approver(s)
- Duration:** 7 Day(s)
- Escalated Approvers:** /Target/Manager
- Email Templates:**
 - Pending Approval (sent to approvers): Default pending approval email template
 - Pending Approval Escalation (sent to approvers): Default pending approval email template
 - Completed Approval (sent to approvers): Default completed approval email template
 - Rejected Request (sent to requestor): Default rejected request email template
 - Timed Out Request (sent to requestor): Default timed out request email template

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

3.11.7 Create the workflow Notify Manager

The screenshot shows the configuration for a workflow named "Send Email Notification: Notify Manager". Key settings include:

- Activity Display Name:** Notify Manager
- Advanced Features:** Advanced features are selected.
- Activity Execution Condition:** IsPresent(/Target/Manager/Email)
- Email Template:** /EmailTemplate[DisplayName='Manager_Notification']
- To recipients:** /Target/Manager/Email
- 'CC' recipients:** (empty field)
- 'Bcc' recipients:** gmathieu@miam.msreport.fr
- Suppress Exception:** Supresses notification failure from the EmailNotification Activity.

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.

The screenshot shows the configuration for a workflow named "Distribution Group Provisioning to AD". Key settings include:

- Add the target resource to Synchronization Rule:** AD Distribution
- Synchronization Rule:** AD Distribution Group Sync Rule
- Action Selection:**
 - Add: The Target object will be added to the scope of the specified Synchronization Rule. All flows and provisioning decisions apart of this rule will now apply to the Target.
 - Remove: The Target object will be removed from the scope of the specified Synchronization Rule. All flows will be discontinued.
 - Based on Attribute Value: The Target object will either be removed or added to the scope of the specified Synchronization Rule depending on the value of a selected attribute.

The screenshot shows the configuration for a workflow named "Security Group Provisioning to AD". Key settings include:

- Add the target resource to Synchronization Rule:** AD Security Group
- Synchronization Rule:** AD Security Group Sync Rule
- Action Selection:**
 - Add: The Target object will be added to the scope of the specified Synchronization Rule. All flows and provisioning decisions apart of this rule will now apply to the Target.
 - Remove: The Target object will be removed from the scope of the specified Synchronization Rule. All flows will be discontinued.
 - Based on Attribute Value: The Target object will either be removed or added to the scope of the specified Synchronization Rule depending on the value of a selected attribute.

3.11.9 Workflows Result

You must obtain these results.

The screenshot shows a user interface titled "Workflows". At the top, there are three buttons: "New" (gear icon), "Details" (magnifying glass icon), and "Delete" (red X icon). Below the buttons is a list of workflow items, each with a checkbox on the left:

- _AD-DISABLE-USERS
- _AD-OUT-USERS
- _AD-REMOVE-USERS
- _Distribution Group Provisioning to AD
- _Generate_Values
- _HR-OUT
- _Manager_Approval_Classic
- _Notify_Manager
- _Security Group Provisioning to AD

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 --&gt; System.Data.SqlClient.SqlException: Reraised Error 50000, Level 16, State 1,
Procedure DoEvaluateRequestInner, Line 1319, Message: Permission denied:
&lt;ai&gt;&lt;Name&gt;Domain&lt;/Name&gt;&lt;/ai&gt;&lt;ai&gt;&lt;Name&gt;Type&lt;/Name&gt;&lt;/ai&
&gt;&lt;ai&gt;&lt;Name&gt;Global_ID&lt;/Name&gt;&lt;/ai&gt;
```



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

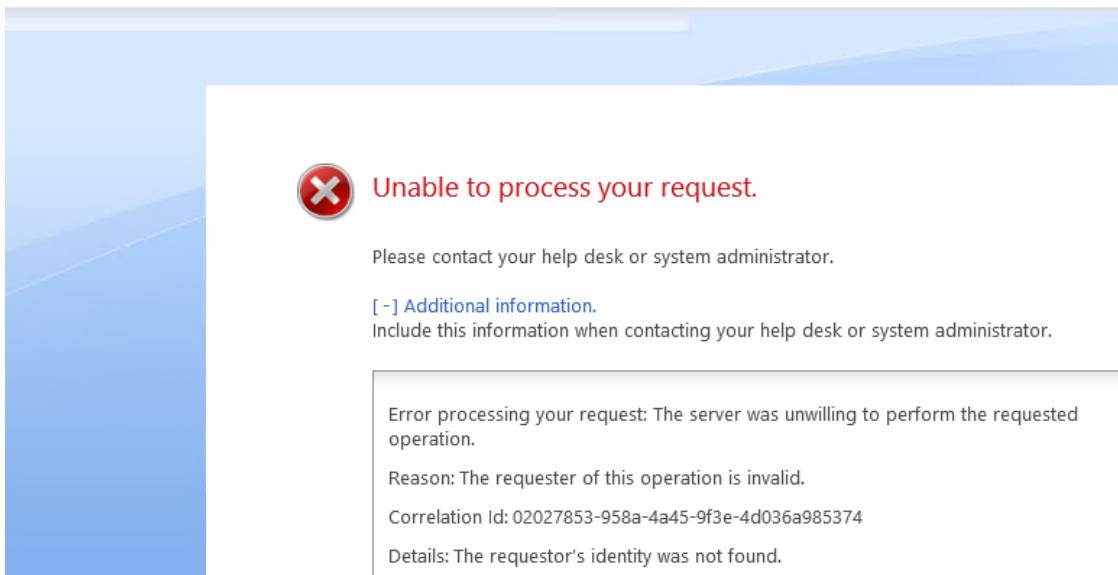
Synchronization: Synchronization account can read group resources it synchronizes

Management Policy Rules						
	Display Name	Action Type	Disabled	Grant Right	Authentication Workflows	Authorization Workflows
<input type="checkbox"/>	Administration: Administrators can control synchronization configuration resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No
<input type="checkbox"/>	Administration: Administrators can update synchronization filter resources	Add, Modify, Remove	No	Yes	No	No
<input type="checkbox"/>	Administration: Administrators control synchronization rule resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account can delete and update expected rule entry resources	Modify, Delete	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account can read group resources it synchronizes	Read	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account can read schema related resources	Read	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account can read synchronization related resources	Read	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account can read users it synchronizes	Read	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account controls detected rule entry resources	Create, Delete, Add, Modify	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account controls group resources it synchronizes	Create, Delete, Add, Modify, Remove	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account controls synchronization configuration resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No
<input type="checkbox"/>	Synchronization: Synchronization account controls users it synchronizes	Create, Delete, Add, Modify, Remove	No	Yes	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:

Microsoft Identity Manager



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

General: Users can read non-administrative configuration resources

General		Requestors and Operations	Target Resources
Display Name	General: Users can read non-administrative configuration resou		
Description	General: Users can read non-administrative configuration resources		
Type	Select the type of this management policy rule.	Request	
Disabled	Indicates if this policy rule is disabled.	<input type="checkbox"/> Policy is disabled	

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

Description: _AD-USERS-OUT

Type:
Select the type of this management policy rule.
Set Transition
Disabled
Indicates if this policy rule is disabled.

Display Name: _AD-USERS-OUT

Type: *Set Transition*.

Transition Set:
* Select the set for which this transition policy is defined.
All AD Users

Transition Type:
Select the type of transition for this policy rule.
Transition In

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*.

Action Workflows

	Display Name	Description	Run On Policy Update
<input type="checkbox"/>	AD-DISABLE-USERS		No
<input checked="" type="checkbox"/>	AD-OUT-USERS		No
<input type="checkbox"/>	AD-REMOVE-USERS		No
<input type="checkbox"/>	Distribution Group Provisioning to AD		No
<input type="checkbox"/>	Generate_Values		No

Selected Resources
AD-OUT-USERS

Select the workflow AD_OUT-USER.

Click on *Submit*.

3.12.5 Create the management policy rule _HR-OUT

_HR-OUT

General	Transition Definition	Policy Workflows
<p>Display Name <input type="text" value="HR-OUT"/></p> <p>Description <input type="text"/></p> <p>Type Select the type of this management policy rule. Set Transition</p> <p>Disabled Indicates if this policy rule is disabled. <input type="checkbox"/> Policy is disabled</p>		

Display Name: *HR-OUT*.

Type: *Set Transition*.

_HR-OUT

General	Transition Definition	Policy Workflows
<p>Transition Set. * <input type="text" value="All AD Users"/></p> <p>Select the set for which this transition policy is defined.</p> <p>Transition Type. Select the type of transition for this policy rule. Transition In</p>		

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

Action Workflows

General	Transition Definition	Policy Workflows
---------	-----------------------	------------------

Action Workflows	
<input type="checkbox"/>	Display Name
<input checked="" type="checkbox"/>	<i>_HR-OUT</i>
<input type="checkbox"/>	<i>_Notify_Manager</i>
<input type="checkbox"/>	<i>_Security Group Provisioning to AD</i>
<input type="checkbox"/>	<i>Expiration Workflow</i> This workflow
<input type="checkbox"/>	<i>Group Expiration Notification Workflow</i>

Select *HR-OUT* workflow.

3.12.6 Create the management policy rule AD-DISABLE-USERS

AD-DISABLE-USERS

General	Transition Definition	Policy Workflows																																
<p>Display Name: <u>AD-DISABLE-USERS</u></p> <p>Description:</p> <p>Type: Select the type of this management policy rule. Set Transition</p> <p>Disabled: <input type="checkbox"/> Policy is disabled. Indicates if this policy rule is disabled.</p>																																		
<p>AD-DISABLE-USERS</p> <table border="1"> <tr> <td>General</td> <td>Transition Definition</td> <td>Policy Workflows</td> </tr> <tr> <td colspan="3"> <p>Transition Set: <u>All terminated users (30 days)</u></p> <p>Select the set for which this transition policy is defined.</p> <p>Transition Type: Transition In</p> </td> </tr> </table>			General	Transition Definition	Policy Workflows	<p>Transition Set: <u>All terminated users (30 days)</u></p> <p>Select the set for which this transition policy is defined.</p> <p>Transition Type: Transition In</p>																												
General	Transition Definition	Policy Workflows																																
<p>Transition Set: <u>All terminated users (30 days)</u></p> <p>Select the set for which this transition policy is defined.</p> <p>Transition Type: Transition In</p>																																		
<p>Create Management Policy Rule</p> <table border="1"> <tr> <td>General</td> <td>Transition Definition</td> <td>Policy Workflows</td> <td>Summary</td> </tr> <tr> <td colspan="4"> <p>Action Workflows</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Display Name</th> <th>Description</th> <th>Run On Policy Update</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td><u>AD-DISABLE-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>AD-OUT-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>AD-REMOVE-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>Generate_Values</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>HR-OUT</u></td> <td>No</td> <td>No</td> </tr> </tbody> </table> <p>Selected Resources: <u>AD-DISABLE-USERS</u></p> </td> </tr> </table>			General	Transition Definition	Policy Workflows	Summary	<p>Action Workflows</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Display Name</th> <th>Description</th> <th>Run On Policy Update</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td><u>AD-DISABLE-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>AD-OUT-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>AD-REMOVE-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>Generate_Values</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>HR-OUT</u></td> <td>No</td> <td>No</td> </tr> </tbody> </table> <p>Selected Resources: <u>AD-DISABLE-USERS</u></p>				<input type="checkbox"/>	Display Name	Description	Run On Policy Update	<input checked="" type="checkbox"/>	<u>AD-DISABLE-USERS</u>	No	No	<input type="checkbox"/>	<u>AD-OUT-USERS</u>	No	No	<input type="checkbox"/>	<u>AD-REMOVE-USERS</u>	No	No	<input type="checkbox"/>	<u>Generate_Values</u>	No	No	<input type="checkbox"/>	<u>HR-OUT</u>	No	No
General	Transition Definition	Policy Workflows	Summary																															
<p>Action Workflows</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Display Name</th> <th>Description</th> <th>Run On Policy Update</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td><u>AD-DISABLE-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>AD-OUT-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>AD-REMOVE-USERS</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>Generate_Values</u></td> <td>No</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td><u>HR-OUT</u></td> <td>No</td> <td>No</td> </tr> </tbody> </table> <p>Selected Resources: <u>AD-DISABLE-USERS</u></p>				<input type="checkbox"/>	Display Name	Description	Run On Policy Update	<input checked="" type="checkbox"/>	<u>AD-DISABLE-USERS</u>	No	No	<input type="checkbox"/>	<u>AD-OUT-USERS</u>	No	No	<input type="checkbox"/>	<u>AD-REMOVE-USERS</u>	No	No	<input type="checkbox"/>	<u>Generate_Values</u>	No	No	<input type="checkbox"/>	<u>HR-OUT</u>	No	No							
<input type="checkbox"/>	Display Name	Description	Run On Policy Update																															
<input checked="" type="checkbox"/>	<u>AD-DISABLE-USERS</u>	No	No																															
<input type="checkbox"/>	<u>AD-OUT-USERS</u>	No	No																															
<input type="checkbox"/>	<u>AD-REMOVE-USERS</u>	No	No																															
<input type="checkbox"/>	<u>Generate_Values</u>	No	No																															
<input type="checkbox"/>	<u>HR-OUT</u>	No	No																															

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

_AD-REMOVE-USERS

General	Transition Definition	Policy Workflows								
<table border="1"> <tr> <td>Display Name</td> <td>_AD-REMOVE-USERS</td> </tr> <tr> <td>Description</td> <td></td> </tr> <tr> <td>Type Select the type of this management policy rule.</td> <td>Set Transition</td> </tr> <tr> <td>Disabled Indicates if this policy rule is disabled.</td> <td><input type="checkbox"/> Policy is disabled</td> </tr> </table>			Display Name	_AD-REMOVE-USERS	Description		Type Select the type of this management policy rule.	Set Transition	Disabled Indicates if this policy rule is disabled.	<input type="checkbox"/> Policy is disabled
Display Name	_AD-REMOVE-USERS									
Description										
Type Select the type of this management policy rule.	Set Transition									
Disabled Indicates if this policy rule is disabled.	<input type="checkbox"/> Policy is disabled									

Display Name: *_AD-REMOVE-USERS*

Type: *Set Transition*.

_AD-REMOVE-USERS

General	Transition Definition	Policy Workflows				
<table border="1"> <tr> <td>Transition Set. * Select the set for which this transition policy is defined.</td> <td>All terminated users (365 days)</td> </tr> <tr> <td>Transition Type. Select the type of transition for this policy rule.</td> <td>Transition In</td> </tr> </table>			Transition Set. * Select the set for which this transition policy is defined.	All terminated users (365 days)	Transition Type. Select the type of transition for this policy rule.	Transition In
Transition Set. * Select the set for which this transition policy is defined.	All terminated users (365 days)					
Transition Type. Select the type of transition for this policy rule.	Transition In					

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

Transition Type: *Transition In*

_AD-REMOVE-USERS

General	Transition Definition	Policy Workflows											
<h4>Action Workflows</h4> <table border="1"> <tr> <td><input type="checkbox"/> _AD-DISABLE-USERS</td> <td>Display Name</td> </tr> <tr> <td><input type="checkbox"/> _AD-OUT-USERS</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> _AD-REMOVE-USERS</td> <td></td> </tr> <tr> <td><input type="checkbox"/> _Distribution Group Provisioning to AD</td> <td></td> </tr> <tr> <td><input type="checkbox"/> _Generate_Values</td> <td></td> </tr> </table> <p>Selected Resources</p> <table border="1"> <tr> <td>AD-REMOVE-USERS</td> </tr> </table>			<input type="checkbox"/> _AD-DISABLE-USERS	Display Name	<input type="checkbox"/> _AD-OUT-USERS		<input checked="" type="checkbox"/> _AD-REMOVE-USERS		<input type="checkbox"/> _Distribution Group Provisioning to AD		<input type="checkbox"/> _Generate_Values		AD-REMOVE-USERS
<input type="checkbox"/> _AD-DISABLE-USERS	Display Name												
<input type="checkbox"/> _AD-OUT-USERS													
<input checked="" type="checkbox"/> _AD-REMOVE-USERS													
<input type="checkbox"/> _Distribution Group Provisioning to AD													
<input type="checkbox"/> _Generate_Values													
AD-REMOVE-USERS													

Select the workflow *_All_REMOVE_USERS*.

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

_Distribution Group Creation and Provisioning to AD													
General Transition Definition Policy Workflows													
Display Name	<input type="text" value="_Distribution Group Creation and Provisioning to AD"/>												
Description	<input type="text" value="Calls an action workflow on Distribution Group creation to associate the group to a provisioning sync rule."/> Select the set for which this transition policy is defined.												
Type	Set Transition												
Disabled	<input type="checkbox"/> Policy is disabled												
_Distribution Group Creation and Provisioning to AD													
General Transition Definition Policy Workflows													
Action Workflows <table border="1"> <thead> <tr> <th>Display Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> _AD-DISABLE-USERS</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/> _AD-OUT-USERS</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/> _AD-REMOVE-USERS</td> <td>No</td> </tr> <tr> <td><input checked="" type="checkbox"/> _Distribution Group Provisioning to AD</td> <td>No</td> </tr> <tr> <td><input type="checkbox"/> _Generate_Values</td> <td>No</td> </tr> </tbody> </table> <p>Selected Resources 12 items total Distribution Group Provisioning to AD</p>		Display Name	Description	<input type="checkbox"/> _AD-DISABLE-USERS	No	<input type="checkbox"/> _AD-OUT-USERS	No	<input type="checkbox"/> _AD-REMOVE-USERS	No	<input checked="" type="checkbox"/> _Distribution Group Provisioning to AD	No	<input type="checkbox"/> _Generate_Values	No
Display Name	Description												
<input type="checkbox"/> _AD-DISABLE-USERS	No												
<input type="checkbox"/> _AD-OUT-USERS	No												
<input type="checkbox"/> _AD-REMOVE-USERS	No												
<input checked="" type="checkbox"/> _Distribution Group Provisioning to AD	No												
<input type="checkbox"/> _Generate_Values	No												

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

_Security Group Creation and Provisioning to AD													
General Transition Definition Policy Workflows													
Display Name	<input type="text" value="_Security Group Creation and Provisioning to AD"/>												
Description	<input type="text" value="Calls an action workflow on Security Group creation to associate the group to a provisioning sync rule."/> Select the set for which this transition policy is defined.												
Type	Set Transition												
Disabled	<input type="checkbox"/> Policy is disabled												
Action Workflows													
General Transition Definition Policy Workflows													
Action Workflows <table border="1"> <thead> <tr> <th>Display Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> _HR-OUT</td> <td></td> </tr> <tr> <td><input type="checkbox"/> _Notify_Manager</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> _Security Group Provisioning to AD</td> <td>This workflow will delete the</td> </tr> <tr> <td><input type="checkbox"/> Expiration Workflow</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Group Expiration Notification Workflow</td> <td></td> </tr> </tbody> </table> <p>Selected Resources 1 item total Security Group Provisioning to AD</p>		Display Name	Description	<input type="checkbox"/> _HR-OUT		<input type="checkbox"/> _Notify_Manager		<input checked="" type="checkbox"/> _Security Group Provisioning to AD	This workflow will delete the	<input type="checkbox"/> Expiration Workflow		<input type="checkbox"/> Group Expiration Notification Workflow	
Display Name	Description												
<input type="checkbox"/> _HR-OUT													
<input type="checkbox"/> _Notify_Manager													
<input checked="" type="checkbox"/> _Security Group Provisioning to AD	This workflow will delete the												
<input type="checkbox"/> Expiration Workflow													
<input type="checkbox"/> Group Expiration Notification Workflow													

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*.

_Generate_values

General Requestors and Operations Target Resources Policy Workflows

Display Name	<input type="text" value="Generate_values"/>
Description	<input type="text"/>
Type	Select the type of this management policy rule.
Request	<input checked="" type="radio"/>
Disabled	<input type="checkbox"/> Policy is disabled Indicates if this policy rule is disabled.

Display Name: *Generate_values*
Type: *Request*

_Generate_values

General Requestors and Operations Target Resources Policy Workflows

Requestors	<input checked="" type="radio"/> Specific Set of Requestors Requestor is defined as the following user set. <input type="text" value="All People"/>
Operation	<input checked="" type="checkbox"/> Create resource <input type="checkbox"/> Add a value to a multivalued attribute <input type="checkbox"/> Delete resource <input type="checkbox"/> Remove a value from a multivalued attribute <input type="checkbox"/> Read resource <input checked="" type="checkbox"/> Modify a single-valued attribute
Permissions	Select if this rule will grant permission to request the operation defined in this rule. Do not select this check box if you want to only define workflows for the operation.

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.

_Generate_values

General Requestors and Operations Target Resources Policy Workflows

Target Resource Definition Before Request	<input type="text" value="All HR users"/>
Target Resource Definition After Request	<input type="text" value="All HR users"/>
Resource Attributes	<input type="radio"/> All Attributes Rule applies to all attributes of the resource <input checked="" type="radio"/> Select specific attributes Rule applies to selected attributes <input type="text" value="Company; Employee Type; First Name; Last Name"/>

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*.

_Generate_values

Action Workflows

<input type="checkbox"/> _Manager_Approval_Classic	Display Name	Manager_Approval_Classic	Description
<input type="checkbox"/> Filter Validation Workflow for Administrators			
<input type="checkbox"/> Filter Validation Workflow for Non-Administrators			
<input type="checkbox"/> Group Validation Workflow			
<input type="checkbox"/> Owner Approval Workflow			
Selected Resources			
8 items total Page 1 of 2 <> >>			
Action Workflows			
<input type="checkbox"/> _AD-DISABLE-USERS	Display Name	_AD-DISABLE-USERS	Description
<input type="checkbox"/> _AD-OUT-USERS			No
<input type="checkbox"/> _AD-REMOVE-USERS			No
<input type="checkbox"/> _Distribution Group Provisioning to AD			No
<input checked="" type="checkbox"/> _Generate_Values			No
Selected Resources			
12 items total Page 1 of 3 <> >>			

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.

Manager_Notification

General	Requestors and Operations	Target Resources	Policy Workflows
Display Name	_Manager_Notification		
Description			
Type	Request		
Select the type of this management policy rule.	<input checked="" type="radio"/>		
Disabled	<input type="checkbox"/> Policy is disabled		
Indicates if this policy rule is disabled.			

Type: Request

Manager_Notification

General	Requestors and Operations	Target Resources	Policy Workflows
Requestors	<input checked="" type="radio"/> Specific Set of Requestors Requestor is defined as the following user set. <input type="text"/> All HR users		
	<input type="radio"/> Relative to Resource Select the attribute of resource that defines valid requestors. <input type="text"/>		
Operation	<input type="checkbox"/> Create resource <input type="checkbox"/> Add a value to a multivalued attribute <input type="checkbox"/> Delete resource <input type="checkbox"/> Remove a value from a multivalued attribute <input type="checkbox"/> Read resource <input checked="" type="checkbox"/> Modify a single-valued attribute		
Permissions	Select if this rule will grant permission to request the operation defined in this rule. Do not select this check box if you want to only define workflows for the operation. <input type="checkbox"/> Grants permission		

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.

Manager_Notification

General	Requestors and Operations	Target Resources	Policy Workflows
Target Resource Definition Before Request	<input type="radio"/> Define the set the target resource must belong to before the request is processed. This applies only to Read, Modify and Delete operation types. <input type="text"/> All Standard HR Users		
Target Resource Definition After Request	<input type="radio"/> Define the set the target resource must belong to after the request is processed. This applies only to Modify and Create operation types. <input type="text"/> All Standard HR Users		
Resource Attributes	<input type="radio"/> All Attributes Rule applies to all attributes of the resource <input checked="" type="radio"/> Select specific attributes Rule applies to selected attributes <input type="text"/> Employee Type: Mobile Phone: Office Phone: Photo		

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.

Action Workflows

<input type="checkbox"/> _Manager_Approval_Classic	Display Name	Description
<input type="checkbox"/> Filter Validation Workflow for Administrators		
<input type="checkbox"/> Filter Validation Workflow for Non-Administrators		
<input type="checkbox"/> Group Validation Workflow		
<input type="checkbox"/> Owner Approval Workflow		

Selected Resources 8 items total Page 1 of 2 < > >>

Action Workflows

<input type="checkbox"/> _Manager_Approval_Classic	Display Name	Description	Run On Policy Update
<input type="checkbox"/> _HR-OUT			No
<input checked="" type="checkbox"/> Notify_Manager			No
<input type="checkbox"/> Security Group Provisioning to AD			No
<input type="checkbox"/> Expiration Workflow		This workflow will delete the resource to which it is applied.	No
<input type="checkbox"/> Group Expiration Notification Workflow			No

Selected Resources 12 items total Page 2 of 3 < < > >>

Select the action workflow named Notify_Manager

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

_Manager_Approval_Classique

General Requestors and Operations Target Resources Policy Workflows

Display Name: _Manager_Approval_Classique

Description:

Type: Request

Select the type of this management policy rule.

Request

Disabled: Policy is disabled

Indicates if this policy rule is disabled.

Type: Request

_Manager_Approval_Classique

General Requestors and Operations Target Resources Policy Workflows

Requestors:

- Specific Set of Requestors: Requestor is defined as the following user set: All HR users
- Relative to Resource: Select the attribute of resource that defines valid requestors.

Operations:

Define what operation types this rule applies to:

- Create resource
- Add a value to a multivalued attribute
- Delete resource
- Remove a value from a multivalued attribute
- Read resource
- Modify a single-valued attribute

Permissions:

Select the rule will grant permission to request to operate defined in this rule. Do not select this check box if you want to only define workflows for the operation.

Requestor must be *All_HR_users*.

_Manager_Approval_Classique

General Requestors and Operations Target Resources Policy Workflows

Target Resource Definition Before Request:

Define the set the target resource must belong to before the request is processed. This applies only to Read, Modify and Delete operation types.

All-Cadre-Dirigeant

Target Resource Definition After Request:

Define the set the target resource must belong to after the request is processed. This applies only to Modify and Create operation types.

All-Cadre-Dirigeant

Resource Attributes:

Select the target resource attributes for this rule.

All Attributes: Rule applies to all attributes of the resource

Select specific attributes: Rule applies to selected attributes

Mobile Phone; Office Phone; Employee Type; Photo

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.

Authorization Workflows

General Requestors and Operations Target Resources Policy Workflows

Authentication Workflows

Display Name: Description

>Password Reset AuthN Workflow: This workflow is a system workflow that is required for any registration for Self-service Password Reset. Removing this workflow will break the self-service password reset feature.

Selected Resources

Authorization Workflows

Display Name
<input checked="" type="checkbox"/> _Manager_Approval_Classic
<input type="checkbox"/> Filter Validation Workflow for Administrators
<input type="checkbox"/> Filter Validation Workflow for Non-Administrators
<input type="checkbox"/> Group Validation Workflow
<input type="checkbox"/> Owner Approval Workflow

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

3.12.13 Allow a manager to read attributes of his reports

Create Management Policy Rule

General | Requestors and Operations | Target Resources | Policy Workflows | Summary

Display Name	User management: Manager can read attributes of his reports
Description	<input type="text"/>
Type	<input checked="" type="radio"/> Request Policy is evaluated and applied against incoming requests. <input type="radio"/> Set Transition Policy is applied based on changes in Set membership and independent of the request.
Disabled	<input type="checkbox"/> Policy is disabled
Requestors	<input type="radio"/> Specific Set of Requestors Requestor is defined as the following user set. <input checked="" type="radio"/> Relative to Resource Select the attribute of resource that defines valid requestors. <input type="text"/> Manager
Operation	<input type="checkbox"/> Create resource <input type="checkbox"/> Add a value to a multivalued attribute <input type="checkbox"/> Delete resource <input type="checkbox"/> Remove a value from a multivalued attribute <input checked="" type="checkbox"/> Read resource <input type="checkbox"/> Modify a single-valued attribute
Permissions	Select if this rule will grant permission to request the operation defined in this rule. Do not select this check box if you want to only define workflows for the operation.
Target Resource Definition Before Request	Define the set the target resource must belong to before the request is processed. This applies only to Read, Modify and Delete operation types. <input type="text"/> All HR users
Resource Attributes	<input type="radio"/> All Attributes Rule applies to all attributes of the resource <input checked="" type="radio"/> Select specific attributes Rule applies to selected attributes <input type="text"/> Last Name;First Name;E-mail; E-mail Alias;Display Name;Employee ID;

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

The screenshots show the configuration of a management policy rule:

- General Tab:**
 - Display Name: User management: Manager can edit attributes of his reports
 - Description: (empty)
 - Type:
 - Request: Policy is evaluated and applied against incoming requests.
 - Set Transition: Policy is applied based on changes in Set membership and independent of the request.
 - Disabled: (checkbox unchecked)
- Requestors and Operations Tab:**
 - Requestors:
 - Specific Set of Requestors: Requestor is defined as the following user set. (empty)
 - Relative to Resource: Select the attribute of resource that defines valid requestors. Manager
 - Operation:
 - Define what operation types this rule applies to:
 - Create resource
 - Add a value to a multivalued attribute
 - Delete resource
 - Remove a value from a multivalued attribute
 - Read resource
 - Modify a single-valued attribute
 - Permissions:
 - Select if this rule will grant permission to request the operation defined in this rule. Do not select this check box if you want to only define workflows for the operation.
 - Grants permission
- Target Resources Tab:**
 - Target Resource Definition Before Request:
 - Define the set the target resource must belong to before the request is processed. This applies only to Read, Modify and Delete operation types.
 - All HR users
 - Target Resource Definition After Request:
 - Define the set the target resource must belong to after the request is processed. This applies only to Modify and Create operation types.
 - All HR users
 - Resource Attributes:
 - Select the target resource attributes for this rule.
 - All Attributes: Rule applies to all attributes of the resource
 - Select specific attributes: Rule applies to selected attributes
 - Employee Type, Mobile Phone, Office Phone, Photo

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.

User management: Users can read attributes of their own

General Requestors and Operations Target Resources

Display Name	<input type="text" value="User management: Users can read attributes of their own"/>
Description	<input type="text" value="User management: Users can read attributes of their own"/>
Type Select the type of this management policy rule.	Request
Disabled Indicates if this policy rule is disabled.	<input type="checkbox"/> Policy is disabled

Uncheck the box *Disabled*.

User management: Users can read attributes of their own

General Requestors and Operations Target Resources

Requestors Define who this rule applies to.	<input type="radio"/> Specific Set of Requestors Requestor is defined as the following user set. <input type="text"/>
	<input checked="" type="radio"/> Relative to Resource Select the attribute of resource that defines valid requestors. <input type="text" value="Resource ID"/>
Operation Define what operation types this rule applies to.	<input type="checkbox"/> Create resource <input type="checkbox"/> Add a value to a multivalued attribute <input type="checkbox"/> Delete resource <input type="checkbox"/> Remove a value from a multivalued attribute <input checked="" type="checkbox"/> Read resource <input type="checkbox"/> Modify a single-valued attribute

Let all default settings.

User management: Users can read attributes of their own

General Requestors and Operations Target Resources

Target Resource Definition Before Request Define the set the target resource must belong to before the request is processed. This applies only to Read, Modify and Delete operation types.	<input type="text" value="All Active People"/>
Resource Attributes Select the target resource attributes for this rule.	<input type="radio"/> All Attributes Rule applies to all attributes of the resource <input checked="" type="radio"/> Select specific attributes Rule applies to selected attributes <input type="text" value="Employee ID; Employee Start Date; Employee Type; Photo; Global ID"/>

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*).

The screenshot shows the 'User management: Users can modify attributes of their own' configuration page. Under the 'General' tab, the 'Display Name' is set to 'User management: Users can modify attributes of their own'. The 'Type' is set to 'Request'. The 'Disabled' checkbox is unchecked, indicating the policy rule is enabled.

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

Type: *Request*

The screenshot shows the 'Requestors and Operations' tab of the configuration page. In the 'Requestors' section, the 'Relative to Resource' option is selected, and the 'Resource ID' field contains 'ResourceID'. In the 'Operation' section, the 'Modify a single-valued attribute' checkbox is checked. In the 'Permissions' section, the 'Grants permission' checkbox is checked.

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

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

The screenshot shows the 'Target Resources' tab of the configuration page. It includes sections for 'Target Resource Definition Before Request' (set to 'All HR users') and 'Target Resource Definition After Request' (set to 'All HR users'). In the 'Resource Attributes' section, the 'Select specific attributes' option is selected, and the list contains 'Mobile Phone; Office Phone; Photo'.

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

The screenshot shows the 'General' tab of the configuration page. It includes fields for Display Name ('User management: Users can read selected attributes of other'), Description ('User management: Users can read selected attributes of other Users'), Type ('Request'), and Disabled ('Policy is disabled').

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

We have renamed existing management policy rule.

Type: Request

The screenshot shows the 'Requestors and Operations' tab. Under 'Requestors', it's set to 'Specific Set of Requestors' with 'All Active People' selected. Under 'Operation', 'Read resource' is checked. Under 'Permissions', 'Grants permission' is checked.

Let default settings.

The screenshot shows the 'Target Resources' tab. Under 'Target Resource Definition Before Request', 'All People' is selected. Under 'Resource Attributes', 'Select specific attributes' is chosen, showing options like 'Employee ID', 'Employee Start Date', 'Employee Type', 'Office Phone', and 'Photo'.

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

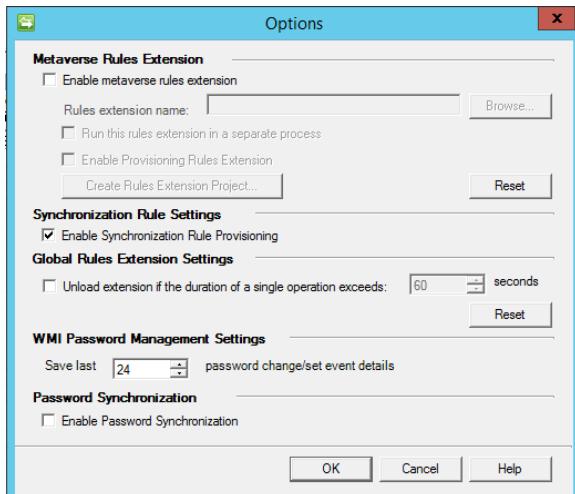
Global_ID; Employee Id; Employee Type; Address; Postal Code; City; Country; Mobile Phone; Office Phone; Photo; Employee End Date; Employee Start date; Type; Domain

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.

<p>Manager can create his report</p> <p>General Requestors and Operations Target Resources Policy Workflows</p> <p>Display Name <input type="text" value="Manager can create his report"/></p> <p>Description <input type="text"/></p> <p>Type <input checked="" type="radio"/> Request Select the type of this management policy rule.</p> <p>Disabled <input type="checkbox"/> Policy is disabled Indicates if this policy rule is disabled.</p>	<p>Manager can create his report</p> <p>General Requestors and Operations Target Resources Policy Workflows</p> <p>Requestors <input checked="" type="radio"/> Specific Set of Requestors Requestor is defined as the following user set: <input type="text"/></p> <p><input checked="" type="radio"/> Relative to Resource Select the attribute of resource that defines valid requestors. <input type="text" value="Manager"/></p> <p>Operation <input checked="" type="checkbox"/> Create resource <input type="checkbox"/> Add a value to a multivalued attribute <input type="checkbox"/> Delete resource <input type="checkbox"/> Remove a value from a multivalued attribute <input type="checkbox"/> Read resource <input type="checkbox"/> Modify a single-valued attribute</p> <p>Permissions <input checked="" type="checkbox"/> Grants permission Select if this rule will grant permission to request the operation defined in this rule. Do not select this check box if you want to only define workflows for the operation.</p>
<p>Manager can create his report</p> <p>General Requestors and Operations Target Resources Policy Workflows</p> <p>Target Resource Definition After Request <input checked="" type="radio"/> Define the set the target resource must belong to after the request is processed. This applies only to Modify and Create operation types. <input type="text" value="All HR users"/></p> <p>Resource Attributes <input checked="" type="radio"/> All Attributes Rule applies to all attributes of the resource <input type="radio"/> Select specific attributes Rule applies to selected attributes <input type="text"/></p>	

3.13 CONFIGURE PROVISIONNING



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

Check the box *Enable Synchronization Rules Provisionning*.

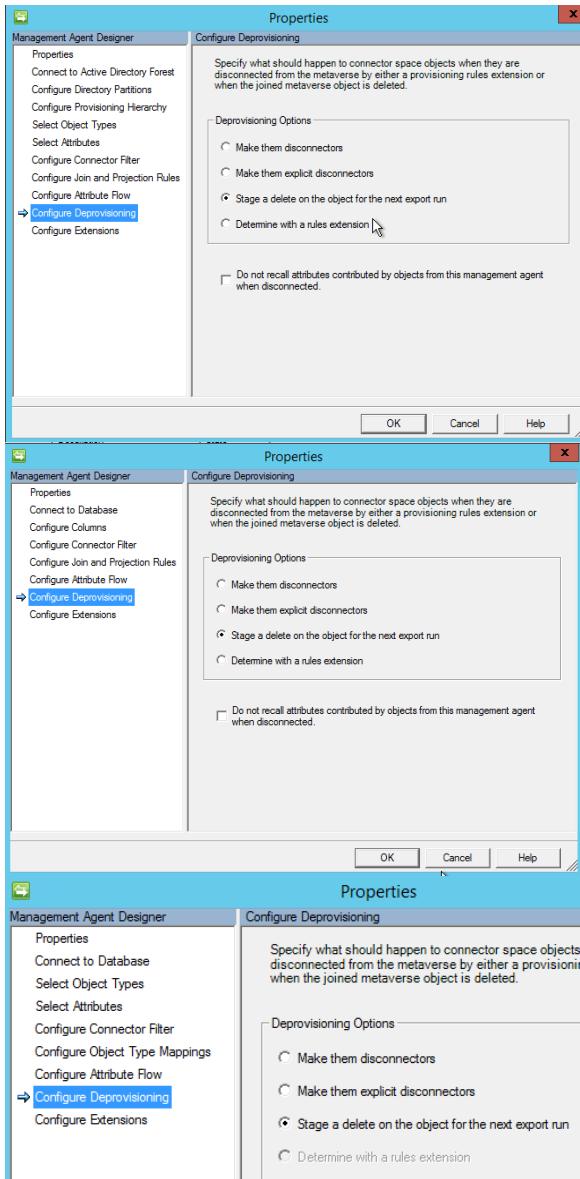
3.14 CONFIGURE DEPROVISIONNING FOR USER

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 deleted 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 Deprovisioning* 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.

The screenshot shows three windows of the Synchronization Service Manager:

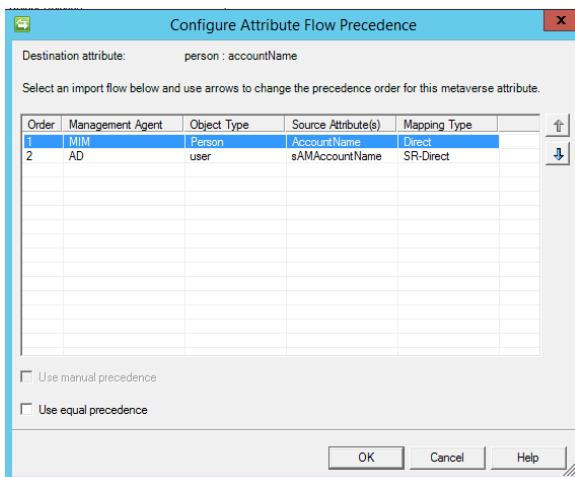
- Metaverse Search:** Shows a table with columns Attribute, Operator, and Value. A dropdown menu "Scope by Object Type" is set to "synchronizationRule".
- Search Results:** Shows a table titled "Retrieved 5 of 5 matching records" with a single row "displayName".
- Metaverse Designer:** Shows the "Object types" tab with "person" selected. It lists attributes like "Name", "city", "company", etc. On the right, under "Actions", there is a section for "Configure Attribute Rules Precedence".
- Configure Attribute Flow Precedence:** A dialog box showing the precedence for the "person : email" attribute. It lists two entries: "1 AD" and "2 MIM". The "AD" entry has "user" as the object type, "mail" as the source attribute, and "SR-Direct" as the mapping type. The "MIM" entry has "Person" as the object type, "Email" as the source attribute, and "Direct" as the mapping type. There are checkboxes for "Use manual precedence" and "Use equal precedence".

All the synchronization rules must appear.

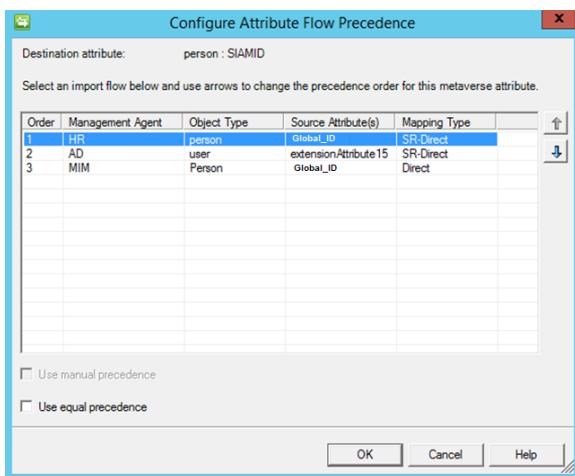
Configure rules precedence for the user class.

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

Active Directory is authoritative for attribute **Email**.

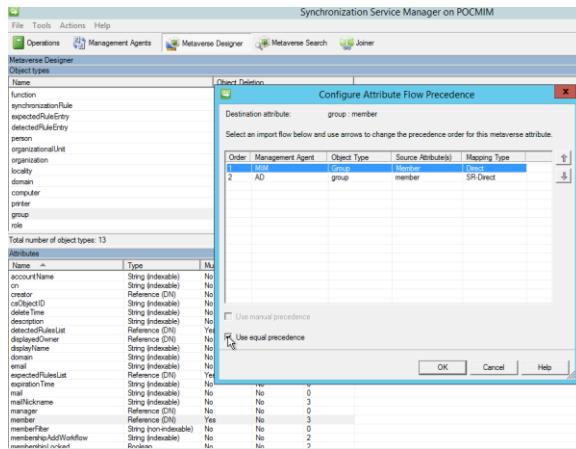


MIM portal is authoritative for the attribute *displayName* and *accountName*.



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/>

The screenshot shows the Microsoft Identity Manager Administration interface. On the left, there's a navigation sidebar with links like Home, Distribution Groups (DGs), Security Groups (SGs), Users, Management Policy Rules, Requests & Approvals, and Privileged Access. The main content area is titled "Resource Control Display Configuration". It shows a table with three items: "Configuration for User Creation", "Configuration for User Editing", and "Configuration for User Viewing". Each item has columns for "Display Name", "Target Resource Type" (Person), and checkboxes for "Applies to Create", "Applies to Edit", and "Applies to View". Below this table, there's a configuration form for "Configuration for User Creation" with fields for "Display Name" (set to "Configuration for User"), "Target Resource Type" (set to "Person"), "Configuration Data" (a dropdown menu with options like "Click here to view the value of this attribute", "Browse...", and "Clear"), and checkboxes for "Applies to Create", "Applies to Edit", and "Applies to View".

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.wapshore.com/misymiis/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't 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>

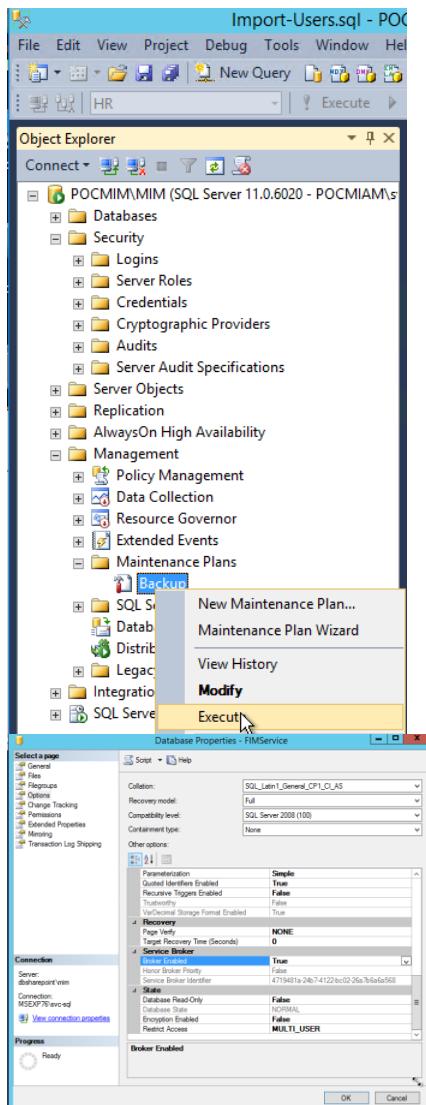
Enter the following information in the RCDC.

```
<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](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 broker 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()

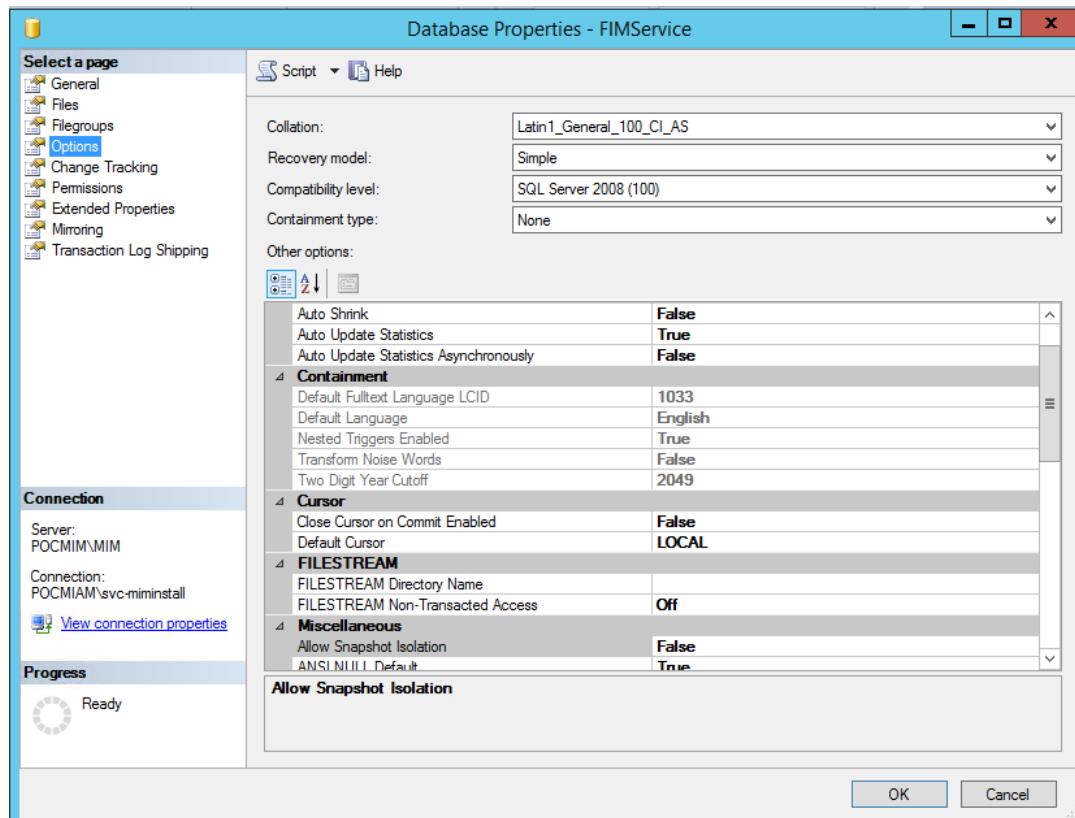
```

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**.

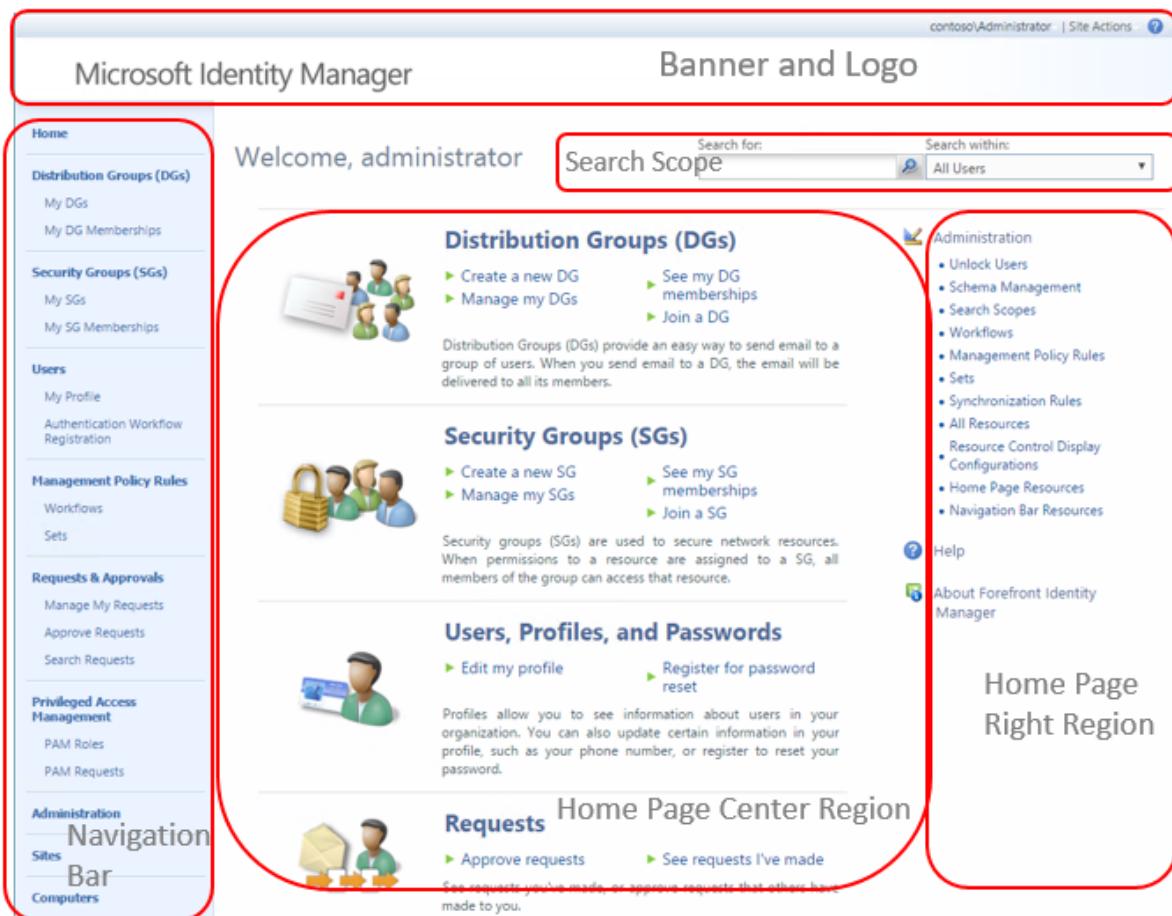


Create also a task which will save the database then remove the log (maintenance plans).

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/auth/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:	Advanced Search
	Display Name	Description	Region	Parent Order	Order	Navigation Url
<input type="checkbox"/>	About Forefront Identity Manager		3	3	0	javascript:iLM2AboutWindow()
<input type="checkbox"/>	Administration		3	1	0	~/IdentityManagement/aspx/configuration/configurationSettings.aspx
<input type="checkbox"/>	All Resources		2	1	10	~/IdentityManagement/aspx/customized/AllCustomizedObjectTypes.aspx
<input type="checkbox"/>	Approve requests		1	4	1	~/IdentityManagement/aspx/requests/MyApprovals.aspx
<input type="checkbox"/>	Create a new DG		1	1	1	javascript:PopupPage("~/IdentityManagement/aspx/groups/CreateDistributionList.aspx");
<input type="checkbox"/>	Create a new SG		1	2	1	javascript:PopupPage("~/IdentityManagement/aspx/groups/CreateSecurityGroup.aspx");
	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.				
<input type="checkbox"/>	Distribution Groups (DGs)		1	1	0	~/IdentityManagement/aspx/groups/AllDLs.aspx
<input type="checkbox"/>	Domain Configurations		4	1	50	~/IdentityManagement/aspx/customized/CustomizedObjects.aspx?type=DomainConfiguration&display=Domain+Configurations
<input type="checkbox"/>	Edit my profile		1	3	1	javascript:PopupPage("~/IdentityManagement/aspx/users/EditPerson.aspx");
<input type="checkbox"/>	Email Templates		4	1	70	~/IdentityManagement/aspx/customized/CustomizedObjects.aspx?type=EmailTemplate&display=Email+Templates
<input type="checkbox"/>	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.

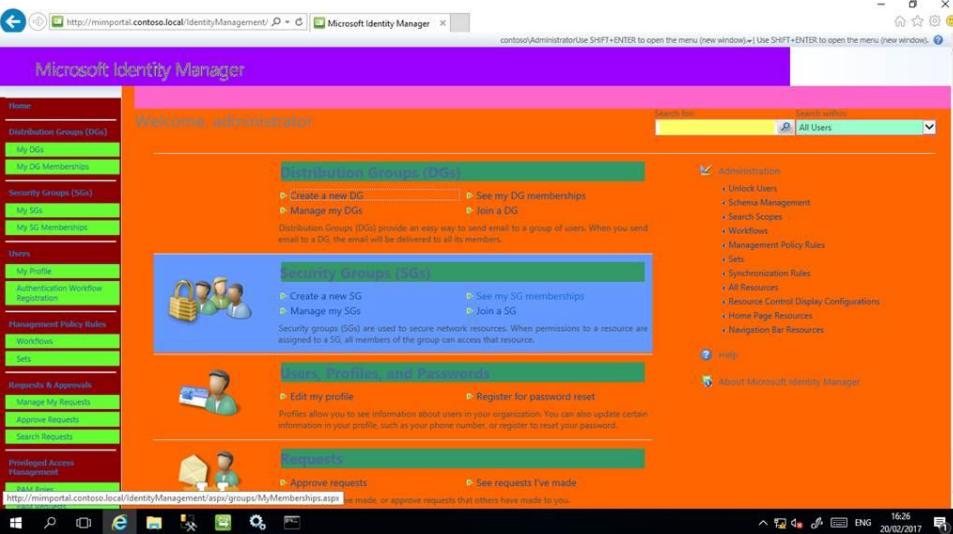
More details are available in this article [Understanding Configuring and Customizing the FIM Portal](#)

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	 <p>The screenshot shows the Microsoft Identity Manager Home page. The left navigation bar includes links for Distribution Groups (DGs), Security Groups (SGs), Users, Management Policy Rules, Requests & Approvals, Privileged Access Management, and Administration. The main content area features sections for Distribution Groups (DGs), Security Groups (SGs), Users, Profiles, and Passwords, and Requests. Each section contains icons and links for various actions like creating new groups, managing memberships, or viewing profiles.</p>
Customized CSS template	 <p>The screenshot shows the same Microsoft Identity Manager Home page but with a different CSS theme. The entire interface has a purple header and footer, and the main content area has a purple background. The navigation bar and sidebar links are highlighted in green. The overall aesthetic is more vibrant and modern compared to the default theme.</p>

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.

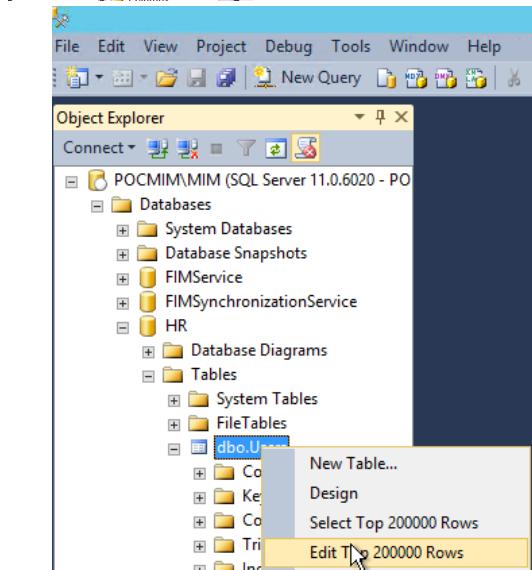
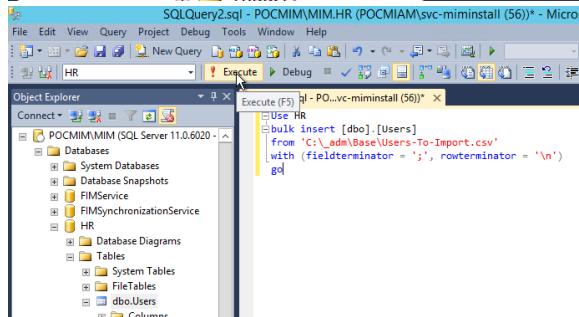
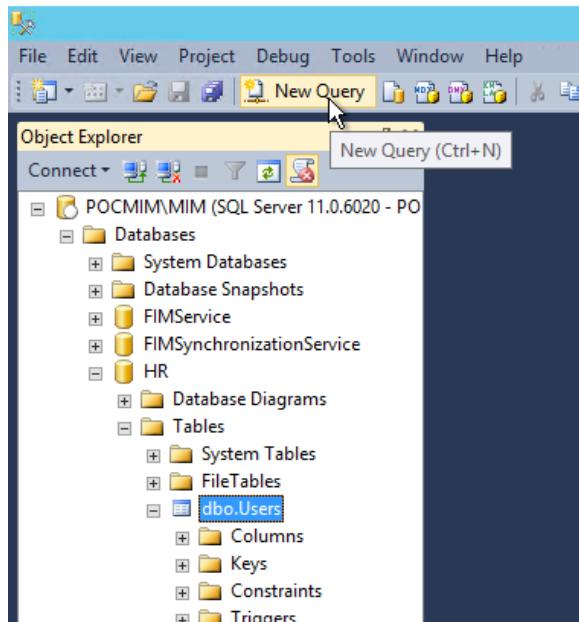
4.1.2 Step by step

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.

```
C:\Windows\system32\cmd.exe
C:\_adm\Synchronization>script C:\_adm\Synchronization\PIFS-HR.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running HR_Execute("PIFS")...
Run completed with result: success
C:\_adm\Synchronization>Pause
Press any key to continue . . .
```

Profile Name: FIFS User Name: POCMIM\svc-miminstall

Step Type:	Full Synchronization
Step 1	
Synchronization Statistics	
Inbound Synchronization	
Projections	1
Joins	0
Filtered Disconnectors	142
Disconnectors	0
Connectors with Flow Updates	1
Connectors without Flow Updates	13
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization MIM	
Export Attribute Flow	1
Provisioning Adds	1

Synchronization Service Manager on POCMIM

File Tools Actions Help

Operations Management Agents Metaverse Designer Metaverse Search Joiner

Management Agents

Name	Type	Description	State
AD	Active Directory Domain Services		Idle
MIM	FIM Service Management Agent		Idle

Total number of management agents: 3

Profile Name: Full Import User Name: POCMIM\svc-miminstall

Step Type: Full Import (Stage Only) Partition: default Start Time: 2/2/2017 8:14:24 AM End Time: 2/2/2017 8:14:25 AM Status: completed-discovery-errors

Synchronization Statistics		Connection Status
Staging	156	success
Unchanged	156	
Adds	0	
Updates	0	
Renames	0	
Purges	0	

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](#)

Optional task (only in case of error):

If MIM display the error [duplicate object](#), you have imported the same user [multiple times](#).

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'](#)

[Click on the Save button.](#)

You must add again the user in the HR SQL Server database.

[End of optional task.](#)

The screenshot shows the Metaverse Service Manager interface with a search results table and a command-line window.

Metaverse Search

Scope by Object Type: person

Attribute Operator Value

Retrieved 14 of 14 matching records

Search Results
displayName
Merlin CANINE

Metaverse Object Properties

Unique identifier (GUID): {851D9C7E-04E7-6111-8004-00003A0A0B83}

Display Name: person

Object type: person

Attributes | Connectors |

Attribute Name	Value	Contributing MA	Type	Last Modified
domainSelection	1	HR	string	1/30/2017 3:55:17 PM
city	London	HR	string	1/30/2017 3:55:17 PM
company	OSS - AMECA	HR	string	1/30/2017 3:55:17 PM
country	United Kingdom	HR	string	1/30/2017 3:55:17 PM
department	Customer Support & Benefits	HR	string	1/30/2017 3:55:17 PM
employeeID	HRS00000000265000000014	HR	string	1/30/2017 3:55:17 PM
employeeStartDate	2010-01-01T00:00:00.000Z	HR	string	1/30/2017 3:55:17 PM
employeesType	Internal	HR	string	1/30/2017 3:55:17 PM
firstName	Merlin	HR	string	1/30/2017 3:55:17 PM
jobTitle	Manager	HR	string	1/30/2017 3:55:17 PM
lastName	CALDERON	HR	string	1/30/2017 3:55:17 PM
mobilePhone	+44 (0)7482 0110	HR	string	1/30/2017 3:55:17 PM
mobilePhone	+44 (0)7482 0110	HR	string	1/30/2017 3:55:17 PM
postAddress	One Southbank Row	HR	string	1/30/2017 3:55:17 PM
postCode	WC1B 5HA	HR	string	1/30/2017 3:55:17 PM
manager	Merlin CANINE		reference	1/30/2017 3:55:17 PM

C:\Windows\system32\cmd.exe

```
C:\>_adm\Syncrhonization>script C:\_adm\Syncrhonization\PIPS-HR.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running HR.Execute("PIFS")...
Run completed with result: success

C:\>_adm\Syncrhonization>Pause
Press any key to continue . . .

C:\>_adm\Syncrhonization>script C:\_adm\Syncrhonization\Export-MIM.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running MIM.Execute("Export")...
Run completed with result: success

C:\>_adm\Syncrhonization>Pause
Press any key to continue . . .
```

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.

The screenshot shows the Microsoft Identity Manager interface. At the top, there's a navigation bar with icons for Back, Forward, Stop, and Refresh, followed by the URL <https://pocmim.pocmiam.intra/IdentityManagement/default.aspx>. Below the URL is a menu bar with File, Edit, View, Favorites, Tools, and Help. The main title "Microsoft Identity Manager" is displayed prominently. On the left, a sidebar has "Home" selected. Under "Distribution Groups (DGs)", there are links for "My DGs" and "My DG Memberships". Under "Security Groups (SGs)", there are links for "My SGs", "Users", and "Memberships". The "Users" link is highlighted with a red box. At the bottom of the sidebar, there's a "My Profile" link. The main content area features a large "Welcome, svc-mimininstall" message, a "Distribution Groups" section with a "Create a new" button and a user icon, and a "Security Groups" section with a "Create a new" button and a group of users icon.

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

Microsoft Identity Manager

Home

Distribution Groups (DGS)

My DGS

My DG Memberships

Users

New Details Delete Domain

New Details Delete Domain

Find the users you want using the Search above.

Search for:

Search for: Advanced Search

Search for: All Users

Display Name Domain Account Name Job Title Office Location Office Phone E-mail

Adrian SARGEN - External pocimain Adrian.SARGEN Manager (+1) 301 987 4000 Adrian.SARGEN@miam.msrcreport.fr

Bernard COLINO pocimain Bernard.COLINO Manager +44 (0)20 7404 0111 Bernard.COLINO@miam.msrcreport.fr

Blake MAY pocimain Blake.MAY Manager +33 (0)1 57 74 84 28 Blake.MAY@miam.msrcreport.fr

Bull - Synchroization Account

Eusebio DECKER pocimain Eusebio.DECKER Manager (+1) 301 987 4000 Eusebio.DECKER@miam.msrcreport.fr

Guillame Bertrand pocimain Guillame.Bertrand Manager IT +33 (0)1 30 05 75 08 Guillame.Bertrand@miam.msrcreport.fr

Jerold RAMOS pocimain jerold.RAMOS Manager +33 (0)1 37 74 84 28 Jerold.RAMOS@miam.msrcreport.fr

Martin CAINE pocimain Martin.CAINE Director of OSS - AMEECA +33 (0)1 37 74 84 28 Martin.CAINE@miam.msrcreport.fr

Mike CALDRON pocimain Mike.CALDRON Manager +44 (0)20 7404 0110 Mike.CALDRON@miam.msrcreport.fr

NexENTOS pocimain NexoENTOS Manager +33 (0)1 57 73 84 28 NexoENTOS@miam.msrcreport.fr

Rick VANCER pocimain Rick.VANCER Manager +33 (0)1 57 73 84 28 Rick.VANCER@miam.msrcreport.fr

sv-mininstall pocimain sv-mininstall Manager

Tuan HUUF pocimain Tuan.HUUF Manager +33 (0)1 57 75 84 28 Tuan.HUUF@miam.msrcreport.fr

Walter DANIEL pocimain Walter.DANIEL Manager +33 (0)1 30 05 75 08 Walter.DANIEL@miam.msrcreport.fr

Willis BAILEY pocimain Willis.BAILEY Manager +33 (0)1 30 05 75 08 Willis.BAILEY@miam.msrcreport.fr

Click on Search button.

You can see the new user.

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

Microsoft Identity Manager

Search Requests

Request Title Date Submitted Status Originator

- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:52 AM Completed Built-in Synchronization Account M
- Update to mv-data AD Request 1/30/2017 8:15:44 AM Completed Built-in Synchronization Account M
- Update to mv-data AD Request 1/30/2017 8:15:44 AM Completed Built-in Synchronization Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:23 AM Completed Built-in Synchronization Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:23 AM Completed Built-in Synchronization Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:23 AM Completed Built-in Synchronization Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:23 AM Completed Built-in Synchronization Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:23 AM Completed Built-in Synchronization Account M
- Create ExpectedRuleEntry-AD-USER-CUT Expected Rule Entry 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M
- Update to Person 'Milford CALDERON' Request 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M
- Update to Person 'Milford CALDERON' Request 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M
- Update to Person 'Milford CALDERON' Request 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M
- Update to Person 'Milford CALDERON' Request 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M
- Update to mv-data Metaverse configuration object Request 1/30/2017 8:15:24 AM Completed Forefront Identity Manager Service Account M

Synchronization Service Manager on POCMIM

Operations Management Agents Metaverse Designer Metaverse Search Joiner

Metaverse Search Scope by Object Type: person Collation: default

Retrieved 14 of 14 matching records

Search Results displayName

Attribute	Value	Contributing MA	Type	Last Modified
displayName	Milford CALDERON		string	1/30/2017 8:15:17 PM
city	London	HR	string	1/30/2017 8:15:17 PM
company	██████████	HR	string	1/30/2017 8:15:17 PM
country	United Kingdom	HR	string	1/30/2017 8:15:17 PM
department	Compensation & Benefits	HR	string	1/30/2017 8:15:17 PM
displayName	Milford CALDERON	MM	string	1/30/2017 8:15:17 PM
domainSelection	1	HR	string	1/30/2017 8:15:17 PM
employeeID	00000000000000000000000000000004	HR	string	1/30/2017 8:15:17 PM
employeeStartDate	2010/01/01 00:00:00	HR	string	1/30/2017 8:15:17 PM
employeeType	internal	HR	string	1/30/2017 8:15:17 PM
EmployeeTypeMin	internal	MM	string	1/30/2017 8:15:17 PM
employeeTypeMax	internal	MM	string	1/30/2017 8:15:17 PM
firstName	Milford	HR	string	1/30/2017 8:15:17 PM
HomeMDB	CH-██	MM	string	1/30/2017 8:15:17 PM
JobTitle	Manager	HR	string	1/30/2017 8:15:17 PM
lastName	CALDERON	HR	string	1/30/2017 8:15:17 PM
mailNickname	Milford CALDERON	MM	string	1/30/2017 8:15:17 PM
manager	Martin CALIE	reference	string	1/30/2017 8:15:17 PM

Synchronization Service Manager on POCMIM

File Tools Actions Help

Operations Management Agents Metaverse Designer Metaverse Search Joiner

Management Agent Operations

Name	Profile Name	Status	Start Time	End Time
AD	Export	success	1/30/2017 4:19:24 PM	1/30/2017 4:19:40 PM
MIM	FIFS	success	1/30/2017 4:19:24 PM	1/30/2017 4:19:40 PM
MIM	Export	success	1/30/2017 4:03:21 PM	1/30/2017 4:03:23 PM
HR	FIFS	success	1/30/2017 3:55:16 PM	1/30/2017 3:55:18 PM
HR	Full Import	success	1/30/2017 3:52:56 PM	1/30/2017 3:52:57 PM
AD	FIFS	success	1/30/2017 3:52:54 PM	1/30/2017 3:52:55 PM
HR	Export	success	1/30/2017 3:52:52 PM	1/30/2017 3:52:53 PM
AD	Export	success	1/30/2017 3:52:52 PM	1/30/2017 3:52:53 PM
MIM	FIFS	success	1/30/2017 3:52:41 PM	1/30/2017 3:52:52 PM
MIM	Export	success	1/30/2017 3:52:40 PM	1/30/2017 3:52:41 PM
HR	FIFS	success	1/30/2017 3:52:37 PM	1/30/2017 3:52:40 PM
HR	Full Import	success	1/30/2017 3:47:20 PM	1/30/2017 3:47:21 PM

File Edit View Favorites Tools Help

Outlook Web App

+ new mail search Mail and People INBOX CONVERSATIONS BY DATE all unread to me flagged

Inbox Drafts Sent Items Deleted Items Junk Email Notes

There are no items to show in this view.

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\StartFinSynchronization.bat](#).

This will perform all the synchronization steps without manual action.

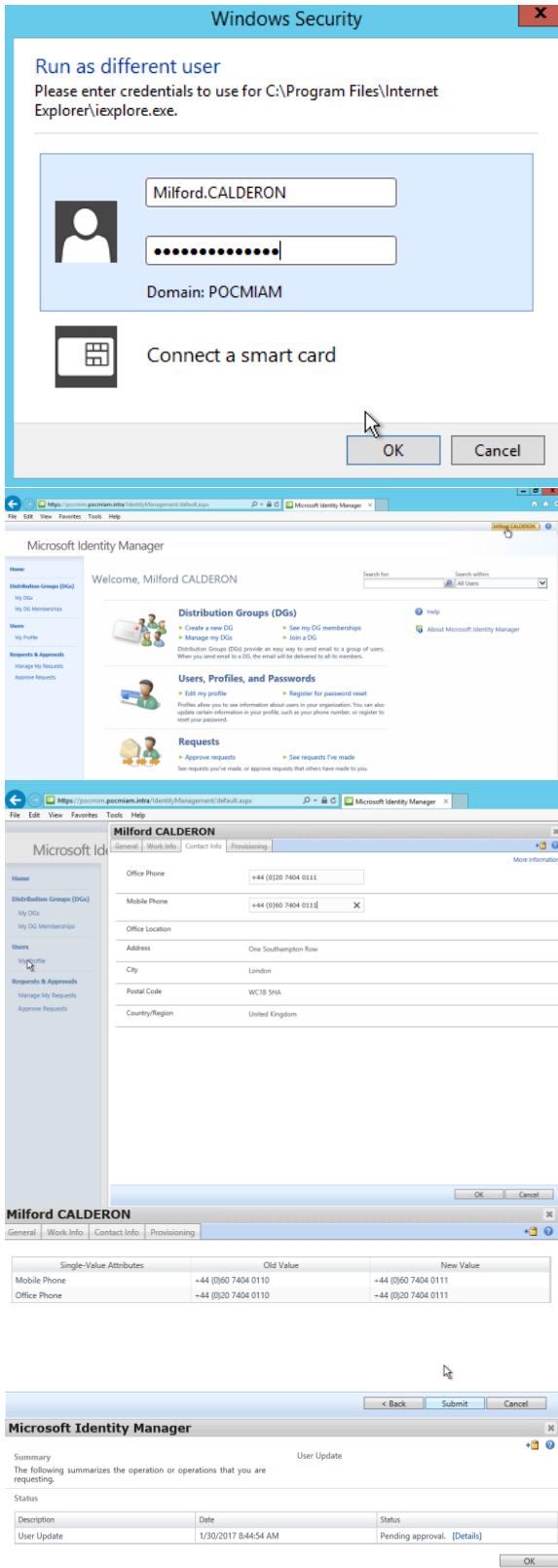
Go to the MIM portal again:

<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.

Milford CALDERON[General](#) | [Work Info](#) | [Contact Info](#) | [Provisioning](#)

Employee Start Date	12/31/2009 4:00:00 PM Format as M/d/yyyy h:mm tt
Employee End Date	
Employee Type	Internal
Employee ID	S000000002E000000014
Manager	Merlin CAINE
Company	ENTITY1
Department	Compensation & Benefits
Job Title	Manager
Rank	Cadre dirigeant

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)

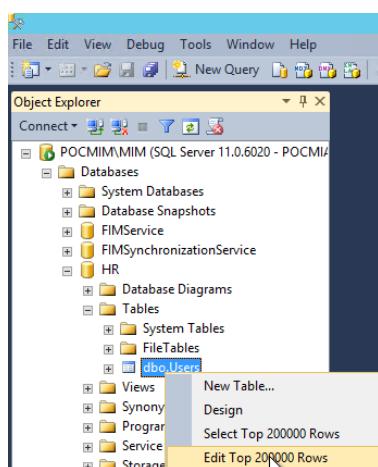
Test 4: user is removed in MIM portal and Active Directory.

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*.



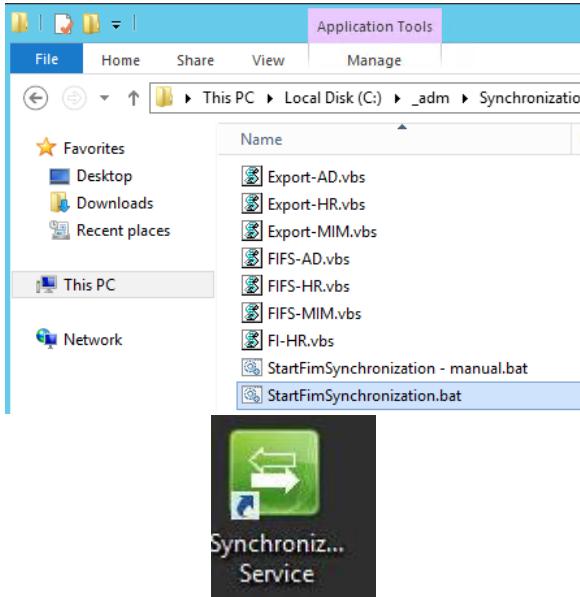
Edit the Users SQL Server table.

Use the user you provision previously. In this example: *S000000002E000000014*.

Set the *Employee End Date* to the value 03/03/2016 (**US format**).



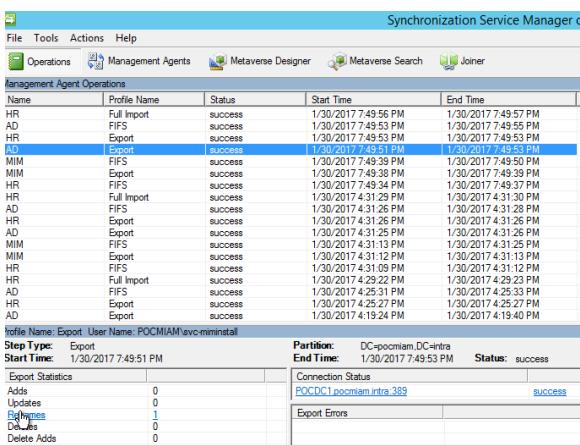
Go the next line and save the change.



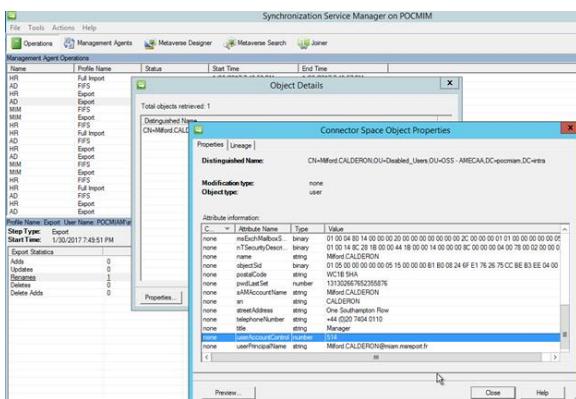
Start the synchronization cycle:

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 2 times 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 screenshot shows the Synchronization Service Manager interface. At the top, there's a menu bar with File, Tools, Actions, Help. Below it are tabs for Operations, Management Agents, Metaverse Designer, Metaverse Search, and Joiner. A table titled 'Management Agent Operations' lists various steps: HR Full Import, AD FIFS, HR Export, AD Export, MIM FIFS, MIM Export, HR FIFS, HR Full Import, AD FIFS, HR Export, AD Export, and MIM FIFS. Each row includes columns for Name, Profile Name, Status, Start Time, and End Time. An 'Object Details' panel on the right shows 'Total objects retrieved: 1' with 'Distinguished Name: S000000002E000000014'. Below this is a 'Users' table listing several users with their details like Display Name, Domain, Account Name, Job Title, Office Location, Office Phone, and E-mail.

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

This screenshot shows a Windows File Explorer window with the path C:_adm\Synchronization\StartFimSynchronization.bat selected. The window displays several files: Export-AD.vbs, Export-HR.vbs, Export-MIM.vbs, FIFS-AD.vbs, FIFS-HR.vbs, FIFS-MIM.vbs, FI-HR.vbs, and StartFimSynchronization - manual.bat.

This screenshot shows the Microsoft Identity Manager portal at https://*yourdomain*.microsoftonline.com/IdentityManagement.aspx#users. It displays a list of users under the 'Users' section, including names like Adrian SARGEN, Bernad COLINO, Blake MAY, Euzebio DECKER, Guillaume.BERTRANDO, Jerold RAMOS, Merlin CARNE, Noel KENTOS, Rick VANCER, Tuan HUFF, Walter DANIEL, Willis BAILEY, and Winfred KRAMER.

Delete a standard user (not a manager or a top level user) in Active Directory

Start the synchronisation script 2 times and check result.

The user is recreated in Active Directory (new SID).

(End of test 3)

Delete a standard user (not a manager or a top level user) in HR database.

Start the synchronisation script 3 times and check result.

The user is not deleted in Active Directory and MIM 2016 portal but is disconnect from HR management agent.

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.

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)

David WUIBAILLE

General Work Info Contact Info Provisioning   

More information

Expected Rules List
This resource has been added to these Synchronization Rules and will be manifested to external systems according to the Synchronization Rule definitions.

Display Name	Expected Rule Entry Action	Synchronization Rule Status
AD-USER-OUT	Add	Applied
HR-OUT	Add	Not Applied

(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.

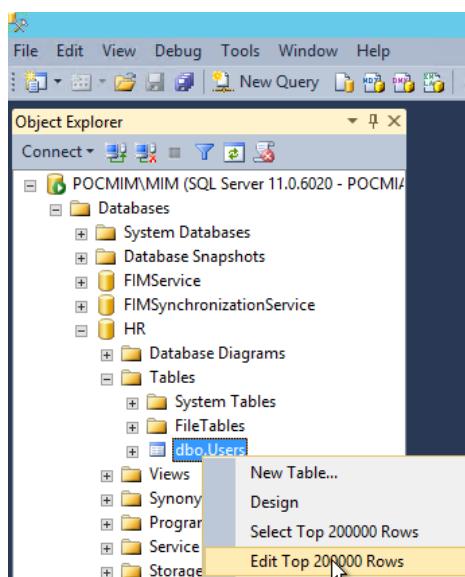
Exchange 2013 will update email address based on *Exchange Recipient Address Policies*.

4.3.2 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.

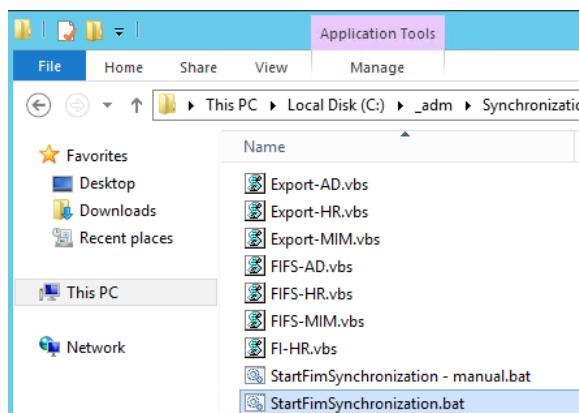
Start SQL Server Management Studio.

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.

Melanie.MATHIEUDO Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
General	Addressees	Account	Profile	Tolerances
				Connections

Multi-valued String Editor

Attribute: proxyAddresses

Value to add:

Add

Values:

smtp:Melanie.BERTRAND@miam.msreport.fr
SMTP:Melanie.MATHIEUDO@miam.msreport.fr

Remove

Users

Display Name	Domain	Account Name	Job Title	Office Location	Office Phone	E-mail
Adrian SARGEN - External	pscomam	Adrian.SARGEN	Manager	(+33) 301 987 4000		Adrian.SARGEN@miam.msreport.fr
Bernard COLLINO	pscomam	Bernard.COLLINO	Manager	+44 (0)20 7404 0111		Bernard.COLLINO@miam.msreport.fr
Blake MAY	pscomam	Blake.MAY	Manager	+33 (0)1 57 75 84 26		Blake.MAY@miam.msreport.fr
Built-in Synchronization Account						
Guillaume Bertrand	pscomam	Guillaume.Bertrand	Manager IT	(+33) 301 987 4000	+33 (0)1 30 85 75 00	Guillaume.Bertrand@miam.msreport.fr
Ierold RAMOS	pscomam	Ierold.RAMOS	Manager	+33 (0)1 57 75 84 28	+33 (0)1 57 75 84 28	Ierold.RAMOS@miam.msreport.fr
Melanie MATHIEUDO - External	pscomam	Melanie.MATHIEUDO	Executive Assistant IT	+33 (0)1 30 85 75 00		Melanie.MATHIEUDO@miam.msreport.fr

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.

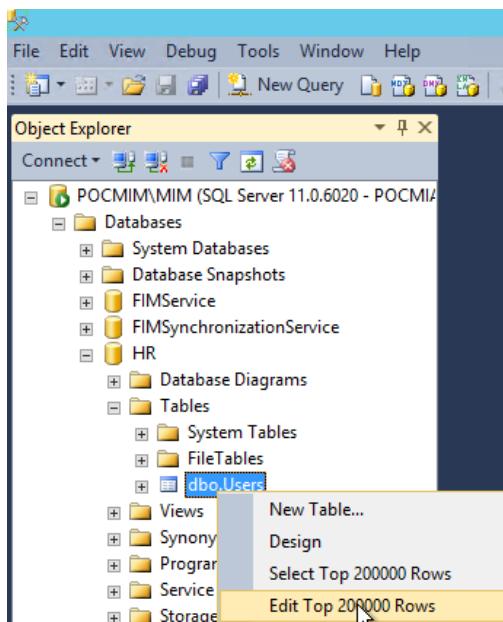
The user is moved automatically in the OU corresponding to his new HR entity.

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*.



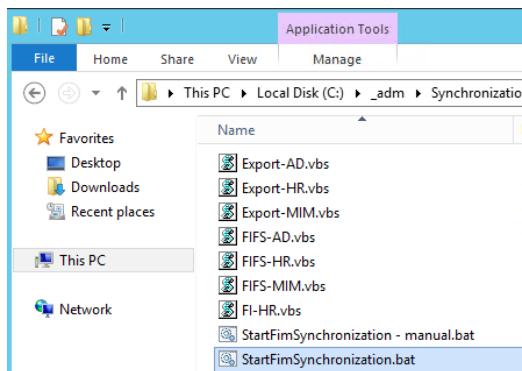
Edit the *Users* SQL Server table.

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

Notes: 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 EMPLOYEE TYPE 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

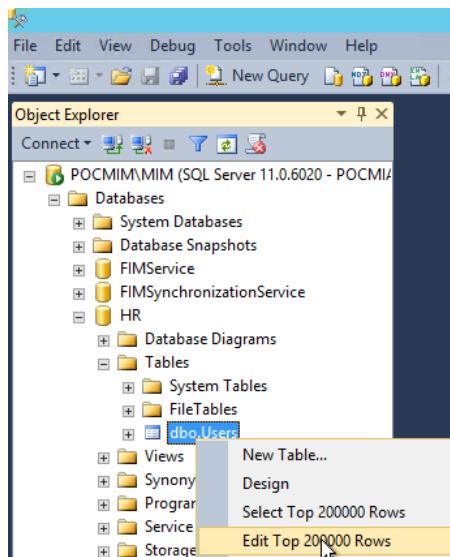
The user is added to the group *External-Users* and is removed from the group *Internal-Users*.

4.6.2 Step by step

Log on POCMIM (RDP) with the service account *pocmiam\svc-miminstall*.

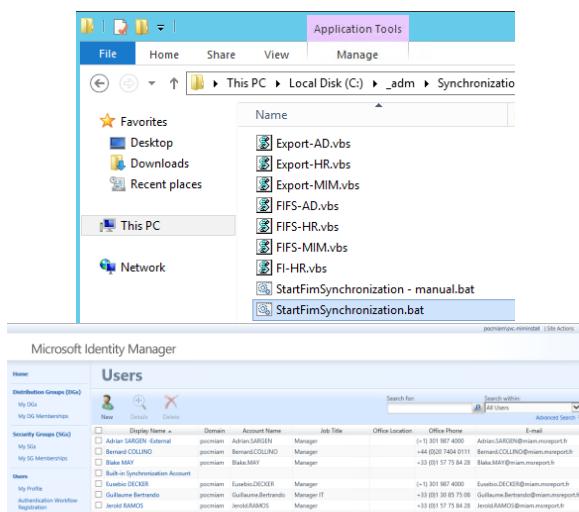
Start SQL Server Management Studio.

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*).



Display Name	Domain	Account Name	Job Title	Office Location	E-mail
S000000002E000000014	poscimam	Adrian.GARLEN	Manager	(+33) 15 79 85 4000	Adrian.GARLEN@msreport.fr
	poscimam	Balazs.COLCINO	Manager	(+33) 15 79 85 4011	Balazs.COLCINO@msreport.fr
	poscimam	Balazs.MAT	Manager	+33 (0) 15 79 85 28	Balazs.MAT@msreport.fr
	poscimam	Emile.DECCKER	Manager	(+33) 15 79 85 4000	Emile.DECCKER@msreport.fr
	poscimam	Guillaume.BARTHES	Manager IT	(+33) 15 79 85 4000	Guillaume.BARTHES@msreport.fr
	poscimam	Jordi.RAMOS	Manager	+33 (0) 15 79 85 28	Jordi.RAMOS@msreport.fr
	poscimam	Melanie.MATHIEU	Executive Assistant NEWIT	+33 (0) 30 85 75 00	Melanie.MATHIEU@msreport.fr

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*.

Search Requests

Request Title	Date Submitted	Status	Originator	Operation
Update to mv-data: 'Metaverse configuration object' Request	1/30/2017 1:49:41 PM	Completed	Built-in Synchronization Account	Modify
Update to mv-data: 'AD' Request	1/30/2017 1:49:43 PM	Completed	Built-in Synchronization Account	Modify
Update to mv-data: 'HR' Request	1/30/2017 1:49:45 PM	Completed	Built-in Synchronization Account	Modify
Update to Person: Mélanie MATHIEUDO Request	1/30/2017 1:49:51 PM	Completed	Forefront Identity Manager Service Account	Modify

Synchronization Service Manager on P

File Tools Actions Help

Operations Management Agents Metaverse Designer Metaverse Search Joiner

Management Agent Operations

Name	Profile Name	Status	Start Time	End Time
HR	FIFS	success	1/30/2017 9:49:51 PM	1/30/2017 9:49:52 PM
AD	FIFS	success	1/30/2017 9:49:49 PM	1/30/2017 9:49:50 PM
HR	Export	success	1/30/2017 9:49:48 PM	1/30/2017 9:49:48 PM
AD	Export	success	1/30/2017 9:49:46 PM	1/30/2017 9:49:48 PM
MIM	FIFS	success	1/30/2017 9:49:32 PM	1/30/2017 9:49:46 PM
MIM	Export	success	1/30/2017 9:49:32 PM	1/30/2017 9:49:46 PM
HR	FIFS	success	1/30/2017 9:49:31 PM	1/30/2017 9:49:46 PM
HR	Full Import	success	1/30/2017 9:49:31 PM	1/30/2017 9:49:46 PM
AD	FIFS	success	1/30/2017 9:49:31 PM	1/30/2017 9:49:46 PM
HR	Export	success	1/30/2017 9:49:31 PM	1/30/2017 9:49:46 PM
AD	Export	success	1/30/2017 9:49:31 PM	1/30/2017 9:49:46 PM
MIM	FIFS	success	1/30/2017 9:49:31 PM	1/30/2017 9:49:46 PM

Profile Name: Export User Name: POCHIAMI/avc-mininstall

Step Type: Export Start Time: 1/30/2017 9:49:46 PM

Export Statistics

Action	Count
Updates	0
Renames	1
Deletes	0
Delete Adds	0

Object Details

Connector Space Object

Distinguished Name: CN=Mélanie.MATHIEUDO.OU=Users,O

Modification type: none
Object type: user

Attribute information:

Changes	Attribute Name	Type	Value
none	accountExpires	number	9223372036854775807
none	c	string	FR
none	cn	string	Mélanie.MATHIEUDO
none	co	string	FRANCE
none	company	string	ENTITÉ
none	countryCode	number	250
none	department	string	NEWIT
none	displayname	string	Mélanie MATHIEUDO -External

Melanie.MATHIEUDO Properties

Published Certificates Member Of Password Replication Dial-in Object

Security Environment Sessions Remote control

Remote Desktop Services Profile COM+ Attribute Editor

General Address Account Profile Telephones Organization

Melanie.MATHIEUDO

First name: Mélanie Initials:

Last name: MATHIEUDO

Display name: Mélanie MATHIEUDO -External

External-Users

General Members Owners

Select user that match **all** of the following conditions:

Employee Type is External
Add Statement or Add Sub-condition

The **Display Name** attribute is updated to Active Directory.

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

View Members

Display Name

Adrian SARGEN -External
Mélanie MATHIEUDO -External

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.

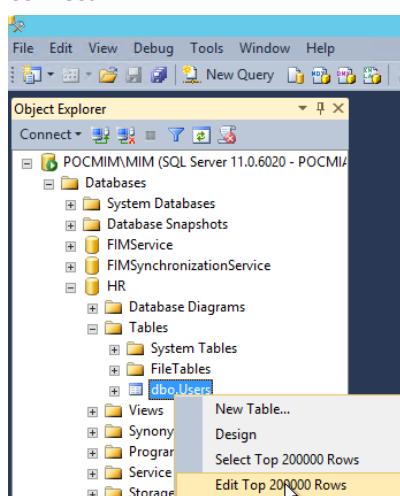
Test 4: the change performed from the Active Directory is replaced by the value defined in HR database.

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.

```
C:\Windows\system32\cmd.exe
C:\_adm\Synchronization>script C:\_adm\Synchronization\FIFS-HR.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running HR.Execute("FIFS")...
Run completed with result: success

C:\_adm\Synchronization>script C:\_adm\Synchronization\Export-MIM.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

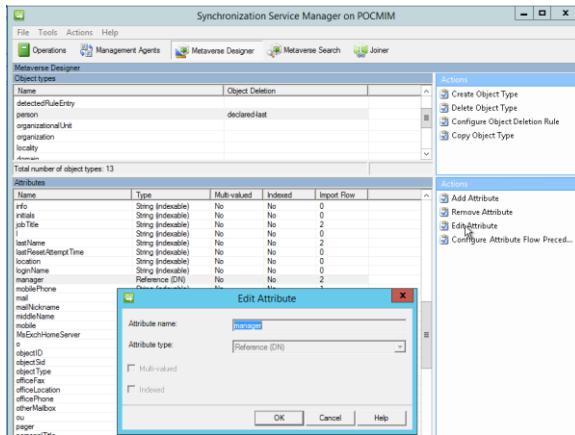
Running MIM.Execute("Export")...
Run completed with result: success

C:\_adm\Synchronization>script C:\_adm\Synchronization\FIFS-MIM.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running MIM.Execute("FIFS")...
```

Start all synchronization steps:

C:_adm\Synchronization\StartFimSynchronization.bat



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.

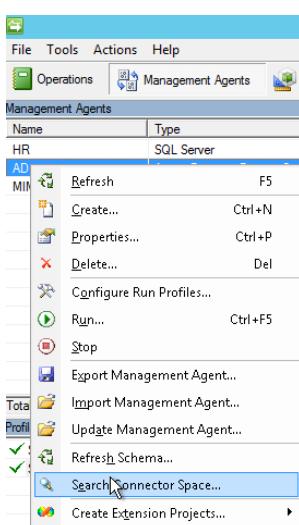
HR Export: no change

AD Full Import: check that the change has been applied in the AD Connector space.

MIM Full Synchronization

AD Full Synchronization

HR Full import



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.

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 *Disconnecter* (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.

Microsoft Identity Manager



Outbound Attribute Flow

New Attribute Flow Delete Attribute Flow

Initial Flow Only	Use as Existence Test	Flow (FIM)
<input type="checkbox"/>	<input type="checkbox"/>	employeeID=>extensionAttribute1 "CN="+accountName+",OU=Users,OU=
<input type="checkbox"/>	<input type="checkbox"/>	city=>l
<input type="checkbox"/>	<input type="checkbox"/>	company=>company
<input type="checkbox"/>	<input type="checkbox"/>	department=>department
<input type="checkbox"/>	<input type="checkbox"/>	jobTitle=>title
<input type="checkbox"/>	<input type="checkbox"/>	manager=>manager

Flow Definition

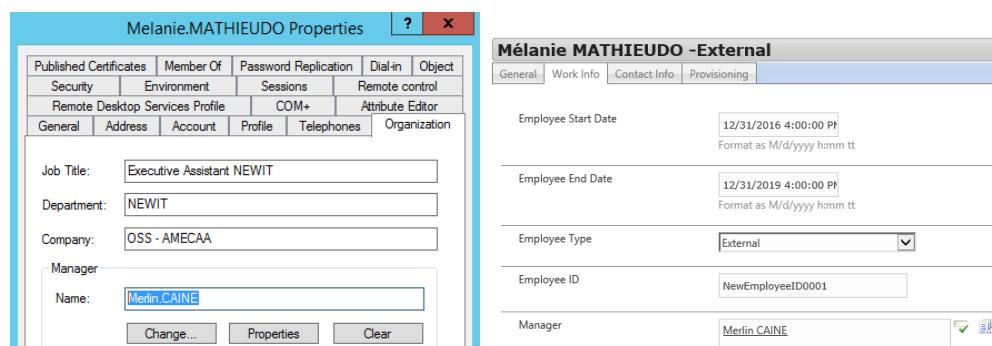
Source Destination

Destination: manager

The attribute to flow values to.

Allow Null Allow null value to flow to destination.

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



Melanie.MATHIEUDO Properties

Job Title: Executive Assistant NEWIT

Department: NEWIT

Company: OSS - AMECAA

Manager:

Name: Merlin.CAINE

Mélanie MATHIEUDO -External

Employee Start Date: 12/31/2016 4:00:00 PM

Employee End Date: 12/31/2019 4:00:00 PM

Employee Type: External

Employee ID: NewEmployeeID0001

Manager: Merlin.CAINE

Mélanie MATHIEUDO -External

General	Work Info	Contact Info	Provisioning	
Employee Start Date	12/31/2016 4:00:00 PM Format as M/d/yyyy h:mm tt			
Employee End Date	12/31/2019 4:00:00 PM Format as M/d/yyyy h:mm tt			
Employee Type	External	<input checked="" type="checkbox"/>		
Employee ID	NewEmployeeID0001			
Manager	Merlin CAINE	<input checked="" type="checkbox"/> 		

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

Change the Manager value.

Mélanie MATHIEUDO -External

General	Work Info	Contact Info	Provisioning	
Employee Start Date	12/31/2016 4:00:00 PM Format as M/d/yyyy h:mm tt			
Employee End Date	12/31/2019 4:00:00 PM Format as M/d/yyyy h:mm tt			
Employee Type	External	<input checked="" type="checkbox"/>		
Employee ID	NewEmployeeID0001			
Manager	Noel KENTOS	<input checked="" type="checkbox"/> 		

Define another user and then click on submit.

```
C:\Windows\system32\cmd.exe
C:\_adm\Synchronization>cscript C:\_adm\Synchronization\FIFS-HR.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running HR.Execute("FIFS")...
Run completed with result: success

C:\_adm\Synchronization>cscript C:\_adm\Synchronization\Export-MIM.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running MIM.Execute("Export")...
Run completed with result: success

C:\_adm\Synchronization>script C:\_adm\Synchronization\FIFS-MIM.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Running MIM.Execute("FIFS")...
```

Start twice the synchronization script:

C:_adm\Synchronization\StartFimSynchronization.bat

Profile Name: FIFS User Name: POCMIA\svc-miminstall	
✓ Step 2	Step Type: Full Synchronization
✓ Step 1	Start Time: 1/31/2017 7:44:27 AM
Synchronization Statistics	
Inbound Synchronization	
Projections	0
Joins	0
Filtered Disconnectors	142
Disconnectors	0
Connectors with Flow Updates	0
Connectors without Flow Updates	14
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization MIM	
Export Attribute Flow	1

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

Synchronization Service Manager on POCMIA

File Tools Actions Help

Operations Management Agents Metaverse Designer Metaverse Search Joiner

Metaverse Designer

Object types

Name	Type	Multi-valued	Indexed	Import Flow
detectedRuleEntry	Object	No	No	0
person	Object	No	No	2
organizationalUnit	Object	No	No	0
organization	Object	No	No	0
location	Object	No	No	0
domain	Object	No	No	0

Total number of object types: 13

Attributes

Name	Type	Multi-valued	Indexed	Import Flow
loginName	String (Indexable)	No	No	0
manager	Reference (DN)	No	No	2

Configure Attribute Flow Precedence

Destination attribute: person -> manager

Select an import flow below and use arrows to change the precedence order for this metaverse attribute.

Order	Management Agent	Object Type	Source Attribute(s)	Mapping Type
1	MIM	Person	Manager	Direct
2	MIM	Person	Manager	Direct

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 EMPLOYEE TYPE (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*, *TelephoneNumber* 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

The screenshot shows the MIM Synchronization console interface. The top menu bar includes File, Tools, Actions, and Help. Below the menu is a toolbar with icons for Operations, Management Agents, Metaverse Designer, and Metaverse Search. The main area is titled 'Metaverse Designer' and 'Object types'. It lists various object types such as function, synchronizationRule, expectedRuleEntry, detectedRuleEntry, person, organizationUnit, organization, locality, domain, computer, printer, group, and a summary row stating 'total number of object types: 13'. Below this is a table titled 'Attributes' with columns for Name, Type, Multi-valued, Indexed, and Import Flow. The 'mobile' attribute is highlighted with a blue background, showing its details: Type is String (indexable), Multi-valued is No, Indexed is No, and Import Flow is 1. Other attributes listed include manager, middleName, mobilePhone, mobilePhone, and MsExchHomeServer.

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.

The screenshot shows two user profile edit forms for 'Mélanie MATHIEUDO'. Both forms have tabs for General, Work Info, Contact Info, and Provisioning. The first form shows 'Office Phone' as '+33666540000' and 'Mobile Phone' as '+33666540000'. The second form shows 'Employee Start Date' as '12/31/2016 4:00:00 PM' and 'Employee End Date' as '12/31/2019 4:00:00 PM'. Both forms also have an 'Employee Type' dropdown set to 'External'. At the bottom of each form, there is a note: 'If you change the value from Active Directory, the change is replaced by the value of MIM portal / HR database.'

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.

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*, *StreetAddress*, *I* and *C_Co*, *CountryCode* attributes).

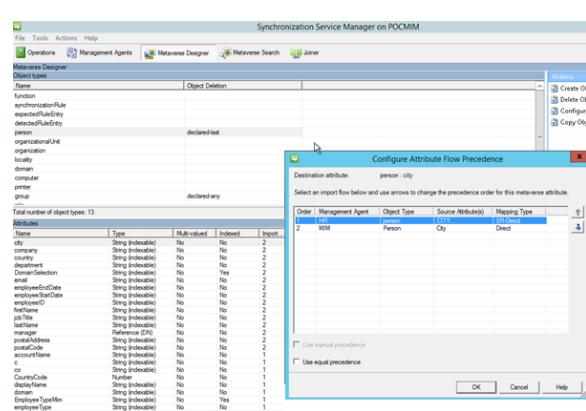
Success criteria:

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. Start synchronization twice for each test.

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:

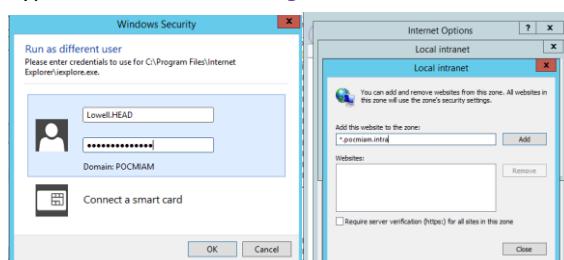
- One standard user (*Type*) is equal to *Cadre* and his manager.
- One standard user (*Type*) is equal to *Cadre Dirigeant* and his manager.

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*.

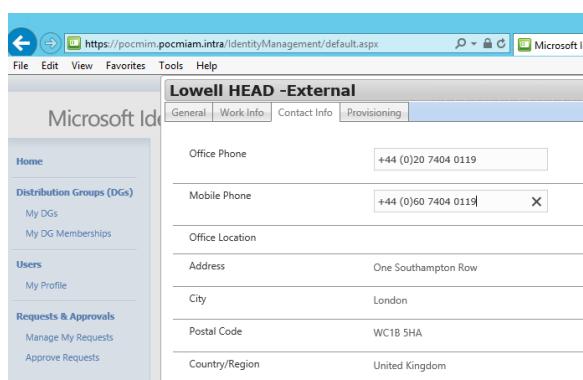
Type of Lowell HEAD is “*Agent de maitrise*”.



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).

Alan PACHECO
Alan.PACHECO@miam.msreport.fr
Executive Assistant Financial controlling, Financial controlling

Licences de produits

Emplacement *
France

Produit	Statut
Enterprise Mobility + Security E5	Activé
249 licences disponibles sur 250	
Microsoft Cloud App Security	Désactivé
Azure Information Protection Premium P2	Désactivé
Azure Information Protection (plan 1)	Désactivé
Azure Rights Management	Désactivé
Intune A - Direct	Désactivé
Azure Active Directory Premium P2	Désactivé
Azure Multi-Factor Authentication	Désactivé
Azure Active Directory Premium (plan 1)	Activé



Compte professionnel ou scolaire

Alan.PACHECO@miam.msreport.fr

 Maintenir la connexion

Se connecter **Précédent**

Connect to *Alan.PACHECO*

Votre compte n'est pas accessible ?



Informations supplémentaires requises

Votre administrateur exige que vous ajoutiez des informations de sécurité supplémentaires pour vous aider à récupérer votre compte.

Suivant

[Se déconnecter et se connecter avec un autre compte](#)

[Plus d'informations](#)

ne perdez pas l'accès à votre compte !

Pour nous assurer que vous pouvez réinitialiser votre mot de passe, nous devons collecter quelques informations qui nous permettront de vérifier votre identité. Ces informations ne seront pas utilisées pour vous envoyer du courrier indésirable, mais seulement pour sécuriser davantage votre compte. [Vous devrez configurer au moins 1 des options ci-dessous.](#)

Telephone (bureau) est défini(e) sur +1 3019874010. Ces informations sont gérées par votre administrateur.

Authentification est défini(e) sur +1 6019874010. Vérifier

Adresse électronique d'authentification n'est pas configuré(e). [Configurer maintenant](#)

les informations semblent correctes annuler

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.

Microsoft Azure

ne perdez pas l'accès à votre compte !

Pour nous assurer que vous pouvez réinitialiser votre mot de passe, nous devons collecter quelques informations sur nous permettant de vérifier votre identité. Ces informations ne seront pas utilisées pour vous envoyer du courrier indésirable, mais seulement pour sécuriser davantage votre compte. [Vous devrez configurer au moins 1 des options ci-dessous.](#)

✓ Téléphone (bureau) est défini(e) sur +1 3019874010. Ces informations sont gérées par votre administrateur.

⚠ Téléphone d'authentification est défini(e) sur +1 6019874010. [Vérifier](#)

● Adresse électronique d'authentification n'est pas configuré(e). [Configurer maintenant](#)

[les informations semblent correctes](#) annuler

Microsoft Azure

ne perdez pas l'accès à votre compte !

Vérifiez votre numéro de téléphone d'authentification ci-dessous.

Téléphone d'authentification

France (+33)

0666548993

[m'envoyer un SMS](#) [m'appeler](#)

Nous appelons votre numéro de téléphone. Répondez pour pouvoir continuer. 

[précédent](#)

Microsoft Azure

ne perdez pas l'accès à votre compte !

Merci ! Nous utiliserons les informations ci-dessous pour récupérer votre compte si vous oubliez votre mot de passe.

✓ Téléphone (bureau) est défini(e) sur +1 3019874010. Ces informations sont gérées par votre administrateur

✓ Téléphone d'authentification est défini(e) sur +33 0666548993. [Changer](#)

⚠ Adresse électronique d'authentification n'est pas configuré(e). [Configurer maintenant](#)

[terminer](#) annuler

Microsoft Azure

ne perdez pas l'accès à votre compte !

Veuillez vérifier votre adresse e-mail d'authentification ci-dessous. N'utilisez pas votre propre adresse.

Adresse électronique d'authentification

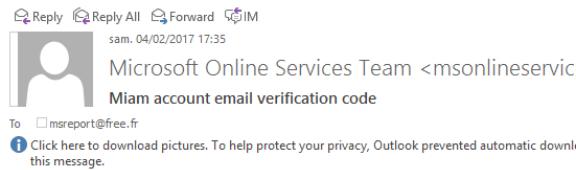
msreport@free.fr

[m'envoyer un courrier électronique](#)

[précédent](#)

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).



Verify your email address

Thanks for verifying your Alan.PACHECO@miam.msreport.fr account!

Your code is: **305262**

Sincerely,

Microsoft Azure

ne perdez pas l'accès à votre compte !

Veuillez vérifier votre adresse e-mail d'authentification ci-dessous. N'utilisez pas votre principe.

Adresse électronique d'authentification

Nous avons envoyé à votre adresse un courrier électronique contenant un code de vérification.

Microsoft Azure

ne perdez pas l'accès à votre compte !

Merci ! Nous utiliserons les informations ci-dessous pour récupérer votre compte si vous oubliez votre mot de passe.

- Téléphone (bureau) est défini(e) sur +1 3019874010. Ces informations sont gérées par votre administrateur.
- Téléphone d'authentification est défini(e) sur +33 0666548993. [Changer](#)
- Adresse électronique d'authentification est défini(e) sur msreport@free.fr. [Changer](#)

User can view his setting from Azure Active Directory portal, review its applications, download his software and manage his settings.

<https://portal.office.com/account/#settings>

(End of test 3)

Microsoft

Retournez sur votre compte

Qui êtes-vous ?

Pour récupérer votre compte, commencez par saisir votre ID d'utilisateur puis les lettres situées dans l'image ou la bande-son ci-dessous

* Identifiant utilisateur :

Exemple : utilisateur@contoso.onmicrosoft.com ou utilisateur@contoso.com



Saisissez les caractères de l'image ou les mots du fichier audio.

Suivant Annuler

Microsoft

Retournez sur votre compte

Pour quelle raison ne parvez-vous pas à vous connecter ?

- J'ai oublié mon mot de passe
- Ne vous inquiétez pas. Nous allons vous aider à réinitialiser votre mot de passe à l'aide des informations de sécurité que vous nous avez fournies.
- Je connais mon mot de passe, mais je ne parviens pas à me connecter

Suivant Annuler

Retournez sur votre compte

étape de vérification 1 > choisir un nouveau mot de passe

Choisissez la méthode de contact à utiliser pour la vérification :

- Envoyer un courrier électronique sur mon adresse de messagerie secondaire
 - Envoyer un SMS à mon téléphone mobile
 - Appeler mon numéro de téléphone mobile
 - Appeler mon numéro de téléphone de bureau
- Suivant

Quel numéro de téléphone voulez-vous utiliser pour la vérification ?

- Appelez-moi au *****93
- Appelez-moi au *****10

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

Retournez sur votre compte

étape de vérification 1 > choisir un nouveau mot de passe

Choisissez la méthode de contact à utiliser pour la vérification :

Envoyer un courrier électronique sur mon adresse de messagerie secondaire

Envoyer un SMS à mon téléphone mobile

Appeler mon numéro de téléphone mobile

Appeler mon numéro de téléphone de bureau

Pour protéger votre compte, nous vous demandons de bien vouloir entrer votre numéro de téléphone mobile complet (******93) ci-dessous. Vous allez ensuite recevoir un appel. Veuillez y répondre pour poursuivre.

0666548993 X

Appeler

Précédent

Retournez sur votre compte

étape de vérification 1 ✓ > choisir un nouveau mot de passe

* Saisissez le nouveau mot de passe :

*****•••••

Enter your new password.

* Confirmez le nouveau mot de passe :

*****•••••

Terminer **Annuler**



Retournez sur votre compte

✓ Votre mot de passe a été réinitialisé

Try connect to

<https://pocmim.pocmiam.intra/identitymanagemen>

t from the computer POCMIM to check that the

Active Directory user account password has also changed.